MEHMET MURAT, HUYUT

Ph.D. Thesis

PRU 2022

T.C. PÎRÎ REİS UNIVERSITY
INSTITUTE FOR GRADUATE STUDIES

A MODEL AND AN APPLICATION FOR INFORMATION TECHNOLOGY GOVERNANCE, RISK AND COMPLIANCE, AND IMPLEMENTATION IN A BANK

PhD. THESIS

MEHMET MURAT HUYUT

2022

T.C. PÎRÎ REİS UNIVERSITY
INSTITUTE FOR GRADUATE STUDIES

A MODEL AND AN APPLICATION FOR INFORMATION TECHNOLOGY GOVERNANCE, RISK AND COMPLIANCE, AND IMPLEMENTATION IN A BANK

PhD. THESIS

by

MEHMET MURAT HUYUT

MBA. Business Administration, Yıldız Technical University, 2012

B.Sc. Computer Engineering, Yıldız Technical University, 2009

Graduate Program in Business Administration

Thesis Advisor: Prof. Dr. Batuhan KOCAOĞLU

2022

APPROVAL of the INSTITUTE for GRADUATE STUDIES

PRU, Graduate Studies Institute's Doctoral student “188113003” and “Mehmet Murat Huyut” prepared his thesis titled

“A MODEL AND AN APPLICATION FOR INFORMATION TECHNOLOGY GOVERNANCE, RISK AND COMPLIANCE AND IMPLEMENTATION IN A BANK” by fulfilling all the necessary conditions determined by the relevant regulations and successfully presented it to the jury whose signatures are below.

Approval of the Institute for Graduate Studies

(Title and Name)
Director

(Title and Name)
Head of Department

Advisor Examining Committee Members

Prof. Dr. Batuhan KOCAOĞLU
(Thesis Supervisor)

Assoc. Asst. Prof. Dr. Aykut ARSLAN

Asst. Prof. Dr. Orhan Özgür AYBAR

Assoc. Prof. Dr. Farid HUSEYNOV

Assoc. Prof. Dr. Berk KUCUKALTAN

Date of Approval:

DEDICATION

I dedicate this thesis to my dear wife; Ünzile Huyut and my dear daughter; Ayşe Hümeyra Huyut, who live with them as a gift to me.

Also, the help of all my family members, friends, colleagues was precious, I also dedicate all of them.

Mehmet Murat HUYUT

ACKNOWLEDGMENT

I wish to thank my dear supervisor Prof. Dr. Batuhan KOCAOĞLU for his assistance, kindness, and support during the whole period of my thesis preparation. I also thank Assoc. Prof. Dr. Aykut ARSLAN, Asst. Prof. Dr. Orhan Özgür AYBAR for their advice, and valuable insights throughout this monitoring period.

Also, to prepare this thesis the governing body of the sample bank gives their precious time to involve time-consuming survey, without their support this work could not have been completed. I would like to thank all the chief executives, group heads, vice presidents, and managers to involve in the IT GRC model creation process.

Finally, I am greatly thankful to my wife, daughter, and my family for their constant support, and encouragement. Their energy, and patience made it possible to finish the whole process. This required too much effort but, “So verily, with every hardship there is ease. Verily, with every hardship, there is ease” (Ash Sharh, 5-6).

ABSTRACT

A MODEL AND AN APPLICATION FOR INFORMATION TECHNOLOGY GOVERNANCE, RISK AND COMPLIANCE, AND IMPLEMENTATION IN A BANK

Continuous developments in information and related technologies increase the importance of effective governance in IT (Information Technology) day by day. One of the important approaches developed is the GRC (Governance Risk and Compliance) approach, where governance, risk, and compliance are evaluated together instead of considering IT governance alone. Although GRC is an enterprise-wide model, IT GRC models are also developed as a subset, and it is aimed to manage IT processes more effectively & efficiently. IT governance includes the alignment of business strategies, and IT strategies, associating IT goals with corporate goals, determining IT goals in line with business goals, and continuous monitoring in order to ensure effective management and executive oversight. On the other hand, IT risk management includes developing response strategies against the positive/negative risks that the IT-based operating processes of the enterprises may encounter, observing the increasing or decreasing impacts of the risks, and continuous improvement processes according to their realization possibilities. Considering that IT risks include the risks arising from cyber threats for businesses working on information technologies, the importance of effective management, and surveillance of IT risks will be understood. IT compliance processes may increase in importance for businesses operating in sectors that require intense legislation, and if they are not managed effectively, they may be subject to heavy penalties by the legislator/regulatory boards against legislative incompatibilities. Internal audit and control activities, as well as external audits, and audits by the authority themselves, can become processes that can be easily carried out by the enterprise operating an effective GRC model.

Within the scope of this thesis, it is aimed to create an IT GRC model to define which IT processes need to be evolved, and the maturity levels get higher. As this model can be used in all businesses, an exemplary application has been made especially in the banking sector, which is subject to strict regulations, and continuously audited. In the compliance dimension, it is aimed to complete the IT GRC process by including the most up-to-date legislation provisions, which are obligatory for Turkish banks to comply with in IT processes, into the model. In Turkey, BRSA (Banking Regulation and Supervision Authority) offers Cobit (Control Objectives for Information and Related Technologies) as a reference resource in

applied regulation to use in information technology process management. ISACA's (Information Systems Audit and Control Association) latest best practice "Cobit 2019" serves a tailored governance model, but its design guide suggests a method that is not suitable for a collaborative approach. This thesis suggests a model for implementing the Cobit 2019 collaboratively by the enterprise's governing body. As a result of the proposed collaboratively quantitative research, based on Cobit 2019, targeting the entire IT governance team of the sample bank, the model, which includes the results of 10 design factors, and prioritized processes, was designed. For the first time in the academic field, a tailored GRC model has been created with the help of the Cobit 2019 design guide. IT risks and all 10-design factor inputs were collected by the sample bank's IT governing body.

BRSA's IT-related legislations were renewed in 2021, and its latest edition is named "Bank IT Systems and Electronic Banking Services". This regulation implementation has become mandatory for sector. In order to find the legislative equivalents or relations of Cobit's 1202 practice, the relationship between BRSA's 214 legislation clauses was revealed by the latent semantic analysis methodology, and the data set created with a 1202 * 214 matrix, and transposition, reporting dashboards were created with the help of the Power BI v.2.87 application. Results show that the 5 most important (or that need to be addressed first) processes of the sample bank according to the determined model;

- DSS 05, ("Deliver, Service and Support") "Managed Security Services"
- DSS 04, "Managed Continuity"
- APO 12, ("Align, Plan and Organize") "Managed Risk"
- APO 13, "Managed Security"
- EDM 03, ("Evaluate, Direct and Monitor") "Ensured Risk Optimization"

When these processes are evaluated together, it is seen that the bank needs to have more mature processes basis on best practices, and taking into account legislative requirements in order to increase the level of maturity in its processes for security and continuity management. In addition to these 2 main processes, it has been concluded that IT risks need to be managed more mature at both governance and organizational levels. Best practices and legislative provisions in line with the proposal is modeled from the LSA (Latent Semantic Analysis) based data set, and made available to the bank.

According to the processes determined according to the lowest importance level, the bank; operates mature processes in IT strategy and innovation management, budget and cost management, resource optimization, portfolio/program/project management, service level agreements management, and it has not been seen that it is compulsory to apply new practices. At this stage, it is recommended that the enterprise first make situational analyzes in order to increase the maturity levels of these processes, identify the areas open to improvement and carry out remedial studies to increase the maturity levels of these areas. While carrying out these studies, the process can be accelerated by using the Power BI dashboards created within the scope of the thesis. These processes' regulation gaps can be found, with the help of the application and then Cobit actions can be defined to align with best practice.

As a result, with this model and application, it is easier for banks to comply with regulation and international best practices. With the created relatedness matrix, the businesses can both examine the points that it is subject to regulation in all domains whose priority order is determined within the scope of the model, and determine which practices/actions it should implement based on the regulation. This method, which can be used in the entire banking sector, will also benefit the academy for further studies on finding the relationship between regulation and good practices.

Keywords: Cobit, IT GRC, LSA, IT Governance

ÖZET

BİLGİ TEKNOLOJİLERİ YÖNETİŞİMİ, RISK VE UYUM MODEL ÖNERİSİ VE BIR BANKADA UYGULAMASI

Bilgi ve ilgili teknolojilerindeki hız kesmeyen gelişmeler bu alanın etkin yönetişiminim önemini her geçen gün artırmaktadır. BT (Bilgi Teknolojileri) yönetişimini tek başına ele almak yerine geliştirilen en önemli yaklaşımlardan birisi yönetişim, risk ve uyumun bir arada değerlendirildiği GRC (Governance, Risk ve Compliance, Yönetişim-Risk ve Uyum) yaklaşımıdır. GRC kurum genelinde uygulanan bir model olmakla birlikte bir alt küme olarak BT GRC modelleri de geliştirilmekte ve BT süreçlerinin daha etkin bir şekilde yönetilmesi hedeflenmektedir. BT yönetişimi, etkin bir yönetim gözetimi sağlayabilmek adına işletme stratejileri ile BT stratejilerini eş düzeyleme, BT hedeflerini kurumsal hedefler ile ilişkilendirme, işletme hedeflerine uyumlu BT hedefleri tespit etme ve sürekli izleme faaliyetlerini kapsamaktadır. BT risk yönetimi ise işletmelerin BT temelli işleyen süreçlerinin karşılaşabileceği olumlu/olumsuz risklerine karşı cevap stratejileri geliştirmeyi, risklerin artan veya azalan etkilerini gözlemeyi, gerçekleşme olasılıklarına göre sürekli iyileştirme süreçlerini içermektedir. Bilgi teknolojileri temelli çalışan işletmeler için BT riskleri, siber tehditlerden kaynaklanan riskleri de içerdiği düşünülürse BT risklerinin etkin yönetimi ve gözetiminin önemi anlaşılacaktır. BT mevzuat uyum süreçleri ise yoğun mevzuat gereksinimi gösteren sektörlerde faaliyet gösteren işletmeler için önemi artabilen, etkin yönetilmez ise mevzuat uyumsuzlukları karşısında kanun koyucu/mevzuat otoritesi tarafından ağır cezalara çarptırılabilecektir. Gerek iç denetim ve kontrol faaliyetleri gerekse dış denetim ve düzenleyicinin bizatihi yaptığı denetimler işletmenin etkin bir GRC modeli işletmesi ile rahatlıkla yürütülebilecek süreçler haline gelebilmektedir.

Tez kapsamında, BT süreçlerinden geliştirilmesi ve olgunluk seviyesinin yükseltilmesi gereken süreçleri belirlemek için bir BT GRC modeli oluşturulması amaçlanmaktadır. Bu model tüm işletmelerde kullanılabildiği için özellikle sıkı düzenlemelere tabi olan ve sürekli denetlenen bankacılık sektöründe örnek bir uygulama yapılmıştır. Uyum boyutunda, Türk bankalarının BT süreçlerinde uyması zorunlu olan en güncel mevzuat hükümlerinin modele dahil edilerek BT GRC sürecinin tamamlanması hedeflenmiştir. Türkiye'de BDDK (Bankacılık Düzenleme ve Denetleme Kurumu), bilgi teknolojileri süreç yönetiminde kullanılmak üzere Cobit'i (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri) mevzuatta referans kaynak olarak sunmaktadır. ISACA'nın (Information Systems Audit and Control

Association) en güncel iyi uygulamalar bütünü “Cobit 2019”, terzi dikimi bir yönetişim modeli kurulumu amacıyla oluşurulmuştur, ancak Cobit tasarım kılavuzu, işbirlikçi bir yaklaşım için uygun olmayan bir yöntem önermektedir. Tez kapsamında, Cobit 2019'un işletmenin yönetim organları tarafından işbirliği içinde uygulanması için bir model önermektedir. Örnek bankanın BT yönetişim ekibini hedef alan, Cobit 2019 temelli, ortaklaşa yapılan bir nicel araştırma sonucunda, 10 tasarım faktörü ve önceliklendirilmiş süreçlerin sonuçlarını içeren bir model tasarlanmıştır. Akademik alanda ilk kez Cobit 2019 tasarım kılavuzu yardımıyla terzi dikimi özel bir IT GRC modeli oluşturulmuştur.

BDDK'nın 2021 yılında yenilenen BT ile ilgili mevzuatı “Banka Bilişim Sistemleri ve Elektronik Bankacılık Hizmetleri” yayımlanmıştır. Bu yönetmelik sektör için zorunlu hale gelmiştir. Cobit'in 1202 uygulamasının yasal karşılıklarını veya ilişkilerini bulmak için BDDK'nın 214 mevzuat hükümleri arasındaki ilişki latent semantik analiz metodolojisi ile ortaya konulmuş ve 1202*214 matrisi aracılığıyla oluşturulan bu veri seti ile Power BI v.2.87 uygulamasının yardımıyla raporlama gösterge tabloları oluşturulmuştur. Sonuçlar, belirlenen modele göre örnek bankanın en önemli (veya önce ele alınması gereken) 5 sürecinin;

- DSS 05, Yönetilen Güvenlik Hizmetleri (Managed Security Services)
- DSS 04, Yönetilen Süreklilik (Managed Continuity)
- APO 12, Yönetilen Risk (Managed Risk)
- APO 13, Yönetilen Güvenlik (Managed Security)
- EDM 03, Garanti Edilmiş Risk Optimizasyonu (Ensured Risk Optimization)

Bu süreçler bir arada değerlendirildiğinde bankanın güvenlik ve süreklilik yönetimine yönelik işletilen süreçlerinde olgunluk seviyesini artırabilmek üzere iyi uygulamalar baz alınarak ve mevzuat gereksinimleri gözetilerek çalışmalar gerçekleştirmesi önerilmektedir. Bu 2 ana sürece ek olarak BT risklerini hem yönetişim hem de organizasyon seviyesinde etkin yönetimine önem vermesi gerektiği sonuçlarına ulaşılmıştır. Önerimize uygun pratikler ve mevzuat hükümleri de LSA temelli veri setinden modellenerek bankanın kullanımına sunulmuştur.

En düşük önem seviyesine göre belirlenen süreçlere göre banka; BT strateji ve inovasyon yönetiminde, bütçe ve maliyet yönetiminde, kaynak optimizasyonunda, portföy/program ve proje yönetiminde ve servis seviye anlaşmaları süreçleri yönetiminde olgun süreçler

işletmektedir ve yeni pratikler uygulamak zorunluluğu görülmemiştir. Bu süreçler için mevzuat uyumsuz alanları bulunabilir ve en iyi uygulama ile uyum sağlamak için Cobit eylemleri tanımlanabilir. Bu sürecin yardımıyla regülasyon boşlukları bulunabilir ve ardından en iyi uygulama ile uyum sağlamak için Cobit aksiyonları tanımlanabilir.

Sonuç olarak bu model ve uygulama ile Bankaların regülasyona ve uluslararası iyi uygulamalara uyum konusunda kolaylık sağlanmıştır. Oluşturulan ilişki matrisi ile işletme gerek model kapsamında öncelik sırası belirlenmiş tüm domainlerde regülasyona tabi olduğu noktaları inceleyebilir, gerekse regülasyondan yola çıkarak hangi pratikleri/aksiyonları uygulaması gerektiğini belirleyebilir. Tüm bankacılık sektöründe kullanılabilir olan bu yöntem, regülasyon ve iyi uygulamalar arasında ilişki bulma yolunda akademi için de sonraki çalışmalar için fayda sağlayacaktır.

Anahtar Kelimeler: Cobit, IT GRC, LSA, BT Yönetişimi

TABLE OF CONTENTS

DEDICATION iv
ACKNOWLEDGMENT v
ABSTRACT vi
ÖZET ix
TABLE OF CONTENTS xii
LIST OF FIGURES xv
LIST OF TABLES xvii
LIST OF SYMBOLS xix
LIST OF ACRONYMS AND ABBREVIATIONS xix
1. INTRODUCTION 1
1.1. Definition of the Problem 2
1.2. Motivation 5
1.3. Research Objective 6
2. LITERATURE REVIEW 9
2.1. Corporate Governance, Governance, Risk, and Compliance 9
2.2. IT Governance (Enterprise Governance of IT) 11
2.3. IT Governance Frameworks 14
2.4. IT risk 21
2.4.1. IT Risk Frameworks 24
2.4.1.1. Cobit "Control Objectives for Information and Related Technology" 24
2.4.1.2. FAIR ("Factor Analysis of Information Risk") 26
2.4.1.3. FRAAP ("Facilitated Risk Analysis Process") 28
2.4.1.4. ISO 31000 Standard 28
2.4.1.5. OCTAVE ("Operationally Critical Threat, Asset and Vulnerability Evaluation") 29
2.4.1.6. RMF ("Risk Management Framework") 31
2.4.2. Risk Mitigation Techniques 32
2.5. IT compliance 34
2.5.1. "Turkish Banking Regulation and Supervision Agency (BRSA)" 37
2.5.2. "Regulation on Information Systems Audit to be Made in Banks by Independent Audit Institutions" 37
2.5.2.1. Application controls 38
2.5.2.2. IT General Controls 40
2.5.3. "Communiqué on Principles to be Considered in Information Systems Management in Banks" 42

2.5.4. “Information Systems and Electronics of Banks Regulation on Banking Services” 44
2.6. GRC and IT GRC 49
2.6.1. IT GRC 54
2.6.2. GRC Frameworks 58
2.6.2.1. OCEG (“Open Compliance and Ethics Group”) 58
2.6.2.1.1. Learn 60
2.6.2.1.2. Align 61
2.6.2.1.3. Perform 62
2.6.2.1.4. Review 63
2.6.2.2. OCEG IT GRC 64
2.6.2.3. Amazon GRC Model 67
2.6.2.4. KPMG’s GRC TOM; A pragmatic and holistic approach 70
2.6.2.5. PwC- GRC Enablement Model 75
2.6.2.6. Cobit 5 77
2.6.2.7. Cobit 2019 80
2.7. Literature Review Results 82
2.8. Literature Review Results in Turkish Journals and Thesis 89
2.9. Literate Review Final Evaluation 91
3. RESEARCH METHODOLOGY 93
3.1. Designing the Research 93
3.1.1. Design Factors and Research Results 95
3.1.1.1. Enterprise strategy (DF 1) 97
3.1.1.2. Enterprise goals (DF 2) 103
3.1.1.3. Risk Profile and Importance of Each Generic IT Risk Category (DF 3) 110
3.1.1.4. I&T Related Issues (DF 4) 114
3.1.1.5. Threat Landscape (DF 5) 120
3.1.1.6. Compliance Requirements (DF 6) 121
3.1.1.7. Role of IT (DF 7) 123
3.1.1.8. Sourcing Model for IT (DF 8) 125
3.1.1.9. IT Implementation Methods (DF 9) 126
3.1.1.10. Technology Adoption Strategy (DF 10) 128
3.1.2. All Design Factors (Final Evaluation) 130
3.2. Latent Semantic Analysis 139
3.2.1. Compliance Map with Latent Semantic Analysis 144

3.2.2. Mapping Cobit Activities to BRSA's IS and Electronic Banking Regulation 148
3.2.3. Creating an Application 153
3.2.3.1. Cobit to Regulation Review 153
3.2.3.2. Regulation to Cobit Review 158
4. CONCLUSION 165
4.1. Recommendations 172
4.2. Suggestions for Future Research 173
5. REFERENCES 175
6. CURRICULUM VITAE 189
7. PUBLICATIONS/PRESENTATIONS ON THE THESIS 190
APPENDIX A 191
APPENDIX B 196
APPENDIX C 197
APPENDIX D 199
APPENDIX E 201
APPENDIX F 202
APPENDIX G 204
APPENDIX H 205
APPENDIX I 206
APPENDIX J 207
APPENDIX K 208
APPENDIX L 209
APPENDIX M 210
APPENDIX N 217

LIST OF FIGURES

Figure 2.1 Corporate governance key elements....11
Figure 2.2. ISACA Cobit 4.1. IT governance domains....14
Figure 2.3. Cobit framework historical timeline....16
Figure 2.4. IT governance main domains....16
Figure 2.5. IT risks categories....23
Figure 2.6. IT risk in the risk hierarchy....24
Figure 2.7. ISACA's risk IT framework....25
Figure 2.8. The Fair model....27
Figure 2.9. Implementing an effective risk management system....27
Figure 2.10. ISO 31000 the risk management process....29
Figure 2.11. Octave Allegro risk management process....31
Figure 2.12. NIST's 6 steps for Risk Management Framework....31
Figure 2.13. Risk mitigation techniques....33
Figure 2.14. Audited main areas of IS by independent audit institutions....38
Figure 2.15. Information technology controls by IIA....39
Figure 2.16. Application and general control relatedness by ISACA....39
Figure 2.17. IT general controls defined by BRSA....40
Figure 2.18. IT general controls....40
Figure 2.19. General control's main processes....41
Figure 2.20. BRSA's defined I&T control target....41
Figure 2.21. Risk management and establishment of controls regarding information systems....46
Figure 2.22. Electronic banking services....46
Figure 2.23. Frame of reference for integrated GRC....50
Figure 2.24. The business case for Integrated GRC....52
Figure 2.25. Universal GRC outcomes....53
Figure 2.26. "GRC and IT GRC in the business and IT context"....55
Figure 2.27. Process model for IT GRC....56
Figure 2.28. Business process model for IT GRC, modeled with ArchiMate....57
Figure 2.29. OCEG's GRC capability model....59
Figure 2.30. OCEG capability model "learn" domain details....60
Figure 2.31. OCEG capability model "align" domain details....61
Figure 2.32. OCEG capability model "perform" domain details....62
Figure 2.33. OCEG capability model "review" domain details....63
Figure 2.34. OCEG's IT Roadmap for GRC....65
Figure 2.35. "Scaling a governance, risk, and compliance program"....67
Figure 2.36. Amazon's GRC model "governance" domain....68
Figure 2.37. Amazon's GRC model "risk management" domain....68
Figure 2.38. Amazon's GRC model "compliance" domain....69
Figure 2.39. KPMG's integrated governance, risk, and compliance target operating model (TOM)....70
Figure 2.40. KPMG's 8 steps and their details for the continuous GRC....71
Figure 2.41. KPMG GRC operational model domains.....72
Figure 2.42. KPMG's enterprise GRC lifecycle....73
Figure 2.43. KPMG's GRC scan (gap analysis sample)....74
Figure 2.44. KPMG's technology assessment diagnostic model....74
Figure 2.45. PwC's GRC enablement model and processes....75

Figure 2.46. PwC, GRC management methodology 76
Figure 2.47. PwC's IT GRC implementation method 76
Figure 2.48. Cobit's domains and main purposes 77
Figure 2.49. Cobit 5 principles 78
Figure 2.50. Cobit 5 processes 80
Figure 2.51. Cobit 2019 framework 81
Figure 2.52. Literature review methodology created by Racz et al. 84
Figure 2.53. GRC-related software tools Gartner magic quadrant 90
Figure 2.54. CONIG® (Converged Information Governance) by TAC 90
Figure 2.55. Literature structure that worked in the thesis 92
Figure 3.1. Research process 93
Figure 3.2. Tailored IT governance risk and compliance mechanism by Cobit 2019 design guide 94
Figure 3.3. Cobit 2019 design factors 96
Figure 3.4. Design factor 1, sample bank's strategy archetype 100
Figure 3.5. DF1 results for Cobit domains 101
Figure 3.6. DF 2, sample bank's enterprise goals results 106
Figure 3.7. Bank's design factor 2 results for Cobit domains 107
Figure 3.8. Bank's design factor 3 results for Cobit domains 112
Figure 3.9. The initial design for governance and management objectives importance 119
Figure 3.10. DF 5, IT threat landscape results 120
Figure 3. 11. DF 6, compliance requirements result 122
Figure 3.12. DF 7, the role of IT results 124
Figure 3.13. DF 8, IT sourcing model results 125
Figure 3.14. DF 9, IT implementation methods results 127
Figure 3.15. DF 10, technology adoption strategy results 129
Figure 3.16. All design factors governance and management objectives importance (Highest scored processes are enclosed in red boxes) 133
Figure 3.17. Cobit total DF's canvas result for "Evaluate Direct & Monitor" (EDM) and "Align, Plan and Organize" (APO) domains 134
Figure 3.18. Cobit total DF's canvas result for Build, "Acquire and Implement" (BAI), "Deliver Service and Support" (DSS) and "Monitor Evaluate and Assess" (MEA) domains 135
Figure 3.19. DSS 05 IT-related goals and its metrics 136
Figure 3.20. DSS 05's subprocesses and RACI chart 137
Figure 3.21. Final IT GRC model for the sample bank based on Cobit 2019 138
Figure 3.22. LSA method 141
Figure 3.23. LSA method flowchart 144
Figure 3.24. Cobit 2019 to ITIL v4 relatedness map 146
Figure 3.25. Cobit-ISO 27001 maps with ArchiMate 147
Figure 3.26. Cobit DSS02-ISO 33072 map with ArchiMate 147
Figure 3.27. Map's purpose; Cobit to regulation and regulation to Cobit 148
Figure 3.28. Power BI data model to create two dashboards 153
Figure 3.29. Cobit DSS05.01 subprocesses practices and activities 162
Figure 3.30. Cobit processes, practices, and action selection and regulation relatedness dashboard 164
Figure 3.31. Regulation section, part and article selection, and Cobit relatedness dashboard 164

LIST OF TABLES

Table 2.1. "Worldwide IT spending forecast by Gartner" (billions of USD) 12
Table 2.2. Common IT governance mechanisms 14
Table 2.3. IT governance disclosure framework 17
Table 2.4. IT value delivery items 18
Table 2.5. IT risk management items 18
Table 2.6. IT performance measurement items 19
Table 2.7. IT-related governance frameworks 20
Table 2.8. Preliminary provisions 44
Table 2.9. Risk management 45
Table 2.10. IS regulation on banking services-related articles 47
Table 2.11. Electronic banking services 48
Table 2.12. Electronic banking services regulation-related articles 48
Table 2.13. Cobit 2019 versus Cobit 5 82
Table 2.14. GRC-related papers search results from Journals 83
Table 2.15. GRC literature review observations two-decade comparisons. 86
Table 3.1. Participant's roles and counts for the survey 97
Table 3.2. DF 1, enterprise strategy design factor details 98
Table 3.3. DF 1 inputs, calculation methods and outputs 98
Table 3.4. DF 1, Enterprise strategy governance/management objective importance results 102
Table 3.5. DF 2, enterprise goals design factor details 104
Table 3.6. Design factor 2 inputs, calculation methods and outputs 104
Table 3.7. DF 2, Enterprise goals governance/management objective importance results 108
Table 3.8. Design factor 3 inputs, calculation methods and, outputs 110
Table 3.9. DF 3, Cobit 2019 generic risk categories and bank's impact and likelihood results 111
Table 3.10. DF 3, IT risk profile governance/management objective importance results 113
Table 3.11. DF 4, I&T related issues design factor 114
Table 3.12. Design factor 4 inputs, calculation methods, and outputs 114
Table 3.13. DF 4, I&T related issues, and bank's responses 116
Table 3.14. DF 4, I&T related issues governance/management objective importance results 118
Table 3.15. DF 5, threat landscape design factor 120
Table 3.16. Design factor 5 inputs, calculation methods, and outputs 120
Table 3.17. DF 6, compliance requirements design factor 121
Table 3. 18. Design factor 6 inputs, calculation methods, and outputs 122
Table 3.19. DF 7, the role of IT design factor details 123
Table 3.20. Design factor 7 inputs, calculation methods, and outputs 123
Table 3.21. DF 8, sourcing model for IT design factor details 125
Table 3.22. Design factor 8 inputs, calculation methods, and outputs 125
Table 3.23. DF 9, IT implementation methods design factor details 126
Table 3.24. Design factor 9 inputs, calculation methods, and outputs 127
Table 3.25. DF 10, technology adoption strategy design factor details 128
Table 3.26. Design factor 10 inputs, calculation methods, and outputs 129
Table 3.27. DSS 05.01 action list 137

Table 3.28. Cobit-NIST cyber security framework map....145
Table 3.29. Sample domain, process, and practices for Cobit....149
Table 3.30. Cobit actions and practices in relation....150
Table 3.31. Translated regulation's main parts and its articles....151
Table 3.32. Coded regulation articles' clauses....151
Table 3.33. Regulation articles and Cobit actions relatedness map sample....152
Table 3.34. DSS 05.01 processes actions' relatedness between regulation articles....154
Table 3.35. Data confidentiality related articles relatedness map....159
Table 3.36. Most relevant Cobit actions with data confidentiality articles....160
Table 3.37. Data confidentiality articles related actions by calculating mean values....162
Table 3.38. Protect against malware-related articles by calculating mean values....163

LIST OF SYMBOLS

$: United States Currency-Dollar
€: European Union Currency-Euro
₺: Turkey Currency-Turkish Lira

LIST OF ACRONYMS AND ABBREVIATIONS

APO: Align, Plan and Organize
ATM: Automated Teller Machine
AS: Australian Standard
BAI: Build, Acquire and Implement
BDDK: Bankacılık Düzenleme ve Denetleme Kurumu
BRSA: Banking Regulation and Supervision Agency
BT: Bilişim/Bilgi Teknolojileri
CEO: Chief Executive Officer
CERT/CC: Coordination Center of the Computer Emergency Response Teams
CFO: Chief Financial Officer
CIO: Chief Information Officer
CMMI: Capability Maturity Model Integration
CTO: Chief Technology Officer
COBIT: Control Objectives for Information and Related Technologies
DF: Design Factor
DevOps: Development Operations
DevSecOps: Development Security Operations
DSS: Deliver, Service and Support
EDM: Evaluate, Direct and Monitor
EG: Enterprise Goal
EU: European Union
FAIR: Factor Analysis of Information Risk
FRAAP: Facilitated Risk Analysis Process
GDPR: General Data Protection Regulation-EU GDPR
GRC: Governance, Risk and Compliance
HIPAA: Health Insurance Portability and Accountability Act
IS: Information Systems
IIA: The Institute of Internal Auditors
ISO: International Organization for Standardization
IT: Information Technology
ITGI: Information Technology Governance Institute
IT GAM: IT Governance Arrangements Matrix
IT GRC: Information Technology Governance, Risk and Compliance
ITIL: Information Technology Infrastructure Library
IS: Information Systems
I&T: Information and Technology

PCI-DSS: Payment Card Industry Data Security Standard
PwC: PricewaterhouseCoopers
RACI: Responsible, accountable, consulted, and informed
RISKCAT: Risk Category
RMF: Risk Management Framework
U.S.: United States
USD: United States Dollar
ISACA: Information Systems Audit and Control Association
ISO: International Organization for Standardization
LSA: Latent Semantic Analysis
MoR: Management of Risk
MMULT: Multiplication of two matrices
NIST: National Institute of Standards and Technology
OCEG: The Open Compliance and Ethics Group
OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation
SEI: Software Engineering Institute
SOX: The Sarbanes–Oxley Act
SVD: Singular Value Decomposition
TOM: KPMG Target Operating Model
TOGAF: The Open Group Architecture Framework
USD: United States Dollar
UML: Unified Modeling Language
YÖK: Yüksek Öğretim Kurumu

1. INTRODUCTION

In this fast-changing world, businesses have harsh conditions to survive. In every sector, there are many rivals to race against, and being a successful business is too hard (Kukharuk, 2021). Especially in some sectors risks and compliances are changing fast and it is more difficult to be compliant.

For businesses competition are inevitable; to adapt business through the changes in technology and environment, enterprises have to follow the developments and innovation closely in too many areas (Rozanova, 2021). To achieve the alignment of businesses to IT (Information Technologies) there are some frameworks and approaches (ISACA, 2012). One of them is through a Governance Risk and Compliance (GRC) system/framework and its related technologies. GRC systems have entered businesses' life as an integrator of main three areas. With help of a GRC framework, businesses can integrate their processes to their risk, compliance requirements, and internal or external control environment. Moreover, corporate governance and other aspects affect the business life span (Mayer et al., 2015).

This thesis, it is intended to create an IT GRC (Information Technology Governance Risk and Compliance) framework for the Turkish Banking Sector as a sophisticated and highly regulated area. There are many reasons to create a framework, but to summarize, the increasing importance of the alignment between IT and business (Hirschheim and Sabherwal, 2001, Sarno et al., 2013, Weiss and Thorogood 2011), the criticality in the management of IT risks, (Svatá and Fleischmann, 2011) and the rapid changes in legislation can be listed as the correct and appropriate actions of the enterprise. Cobit-based tailored IT GRC framework offers a model for a bank to able to relate its IT-related risk and compliance requirements.

The thesis started with a literature review, on corporate governance, IT governance, risk, and compliance term definitions, and its standalone management frameworks had given. Second, GRC frameworks are mentioned in detail. The thesis continues with the main part as GRC and IT GRC framework sample and Cobit 2019. In the final section, created IT GRC model was explained and implemented in the sample bank. In the final phase latent semantic analysis (LSA) based regulation to Cobit integration analysis was made to create the proposed IT GRC model's compliance dimension to the newest IT-related regulation. LSA is a natural processing language algorithm especially used in paragraph-based relation definition. With the help of this analysis, each regulation articles' relation with Cobit actions

or each Cobit actions' regulation relatedness was found by 1202*224 relatedness matrices and the thesis was finalized with recommendations and conclusion.

1.1. Definition of the Problem

For businesses, technology plays a critical role, and its importance is getting higher. Technology is a complicated area for anybody, also for executive management and related parties. Governing information technologies is crucial, without aligning the strategy between businesses and IT, corporations would have difficulties surviving (Hirschheim and Sabherwal, 2001).

The increasing use of information technologies by businesses has led to both positive and negative developments. In addition to the corporate processes they manage, businesses have had to ensure that information technology processes are one of the natural processes of the business (Tvrdíková, 2016). The management of information technology processes as well as their main business, the definition of their relationship with business processes, and even the ongoing and non-information-based processes are carried out with the help of information technologies or completely with information technologies (Sharma, 2020).

Businesses that use information technologies adequately and effectively have experienced competitive advantages in their sectors, created new products or services, used new technologies or technology-based marketplaces to ensure customer interaction, and achieved many positive or negative developments. Positive aspects can be given as examples such as saving time or effort and/or gaining cost advantages by automating long time or labor-intensive processes of the enterprise (Saeidi et al., 2019). The use of information-based technologies and the use of new technologies in relevant business areas by taking research and development activities to higher levels have also set examples that benefit the business, the sector, customers, and all relevant stakeholders. In addition to all these positive developments, businesses' dependence on these technologies has increased, the costs of using technologies have affected businesses, and businesses that cannot manage new technology-related risks or that cannot synchronize their technology-based newly developing processes with business processes have also been exposed to negative effects (Rothrock et al., 2018). Businesses that cannot adapt to the innovations brought by technology have also lost their competitive advantage (Ciffolilli and Muscio, 2018).

One of the sectors where information technologies can be used intensively in the finance sector. With innovations such as the digitalization of money, the widespread use of payment

systems, and the availability of financial services through all alternative channels 24/7, financial institutions have become one of the sectors where digitalization and technology use are most intense (Agarwal and Zhang, 2020). The increasing use of technology has accelerated the change and development of financial enterprises but has revealed the necessity of managing the increasing technology risks. Although all these technologies have improved the customer experience positively, especially in an area such as the banking sector, they have produced new areas of weakness that must be managed by customers and all parties related to the bank. To ensure the governance of these vulnerabilities and all information technology-related processes in a harmonious manner, GRC frameworks have been produced, IT governance processes that foresee hand-leveling IT and business processes specific to information technologies, IT risk management methodologies and regulations by regulatory institutions, and national/ international non-governmental organizations. international good practices are established (Chergui and Chakir, 2020).

Within the scope of this thesis, GRC, IT GRC models, and all their dimensions (governance, risk, and compliance), which aimed to carry out all these dimensions in a whole and harmony in the field of information technologies. These dimensions have been compiled separately in terms of governance, risk, and compliance, and literature studies have been carried out, on these fields, but they are not observed to be studied together in the examined literature and are not discussed as a whole. Academic studies in the field of GRC and IT GRC were not conducted in the field in the past 20 years long, and developed in 10-year periods were not studied comparatively. By making the final evaluation of the literature study, a holistic study was put forward that could fill the gap that was evaluated in the field.

As a result of the examination of IT GRC models, tailored IT GRC models in literature have been proposed, especially in the banking sector where IT risks are intensely encountered and IT governance has high importance (Joseph et al., 1999). The fact that the selected sector was guided by the regulatory authorities in this area, and that it uses an IT governance best practice like Cobit, has been effective in the selection of this sector and a best practice; Cobit. It was published with Cobit 2019 with the claim of creating a tailored IT GRC model compared to its previous versions. By finding the weaknesses or improvement aspects of this proposed model, a tailored IT GRC model is proposed for a business with a collaborative approach. Cobit 2019 designed model created by an aspect of an IT governor and it is not an effective way to show businesses' collaborative thoughts. Reinforcing this weakness of

Cobit with a collaborative approach to the involvement of the entire IT governing body is needed. Another aspect is Cobit 2019 design model's regulation dimension. Cobit is not able to integrate the regulation into the IT GRC model. Although Cobit stated that the relevant IT regulation should be included in the model, how this would be done was not mentioned (ISACA, 2018). Only tailored GRC is proposed as an input to the model and regulation density is included as a design factor. A regulation relationship cannot be established with Cobit's actions. Practitioners do not have a method other than subjective methods to establish the relationship between their regulations and Cobit.

In the IT area some institutes created best practices to govern and manage effective risk or compliance management in IT, but these are not sector-specific and their compliance relatedness is too little or any (De Haes and Grembergen, 2006; Kaneand and Alavi, 2007). According to every country's regulations, control objectives, and control practices importance levels are changing. Although some best practices are mapped with other best practices to easily apply, its map with countries' special regulations is not defined, or a sector-based best practice is never created. Best practices to other standards are mapped with each other but this mapping is generally a top-down approach, they do not math every practice (Chew and Gottschalk 2009). They only analyze the objectives of the related domain and match them together. The method to create relation mapping is generally on a manual basis or a UML (Unified Modelling Language) based mapping such as Archimate. It is a modeling tool described by Kitsios et al.; as "a modeling language that The Open Group developed. ArchiMate is an open and independent architecture modeling language. It includes business processes, information flows, organizational structures, information systems, and technical infrastructure" (Kitsios et al., 2022). These methods create the subjective basis and relationship matrices for good practices, but since the applied methods are created with the views of the mapping parties, they can be biased and erroneous. The maps made are at the basic level and cannot go down to the level of actions or practices. Mapping at the basic domain level cannot be used effectively by practitioners or IT governors. Although it is guiding, finding relevant relationships at the process or practice level can be carried out depending on the expertise of the practitioner.

Common GRC models are stabilized, and control objectives are fixed but, they cannot be tailored for a sector or business. All main areas and domains are settled and the importance level for a subdomain generally stays the same. Because of these reasons different needs of

a specific sector cannot be met. Best practices have general objectives and practices but to create a more effective and tailored governance system used frameworks should be more specific.

1.2. Motivation

The motivation behind the thesis varies but mainly about the difficulties of governing an IT organization in a highly regulated sector, like the banking sector, its difficulty level gets harder (Ramesh, 2021). In Turkey BRSA (Banking Regulation and Supervision Authority) creates new regulations or brings updates every year, trying to be compliant gets too much effort from the organizations. At the same time, new IT risks emerging fast, and response plan creation is continuous. Security breaches or newly invented techniques are generally tried in the finance and banking sector (Hellwig, 2009).

Although the banking sector's IT-related issues are complex, many banks turn this into an advantage for their growth. Greuning et al. explain this complexity and its challenge as; "The changing environment in which banks find themselves presents major opportunities for banks but also entails complex, variable risks that challenge traditional approaches to bank management. Consequently, banks must quickly gain financial risk management capabilities to survive in a market-oriented environment, withstand competition by foreign banks, and support private sector-led economic growth." (Greuning, 2022) Banks need to manage their risks continuously they have to mitigate their risk in any area such as financial risk (credit risk, market risk, interest rate risk, currency forex risk, hedging risk, etc.) and non-financial risk (strategic, operational, political, legal, cyber and technology, etc.) (Brooks et al., 2000; Kolesova and Girzheva, 2018; Campanella et al., 2017) Because of these reasons managing risks in a GRC framework simplifies the process (Trim and Lee, 2016) especially managing IT risks in an IT GRC umbrella framework is beneficial too (Mayer et al., 2015).

Hackers generally targeted banks and use known and unknown attack types to get information or money. Some are not only getting information or stealing money from banks, but they also try denial of service attacks to give harm to the finance system for reputation or various reasons. Their behaviors are changing, their tools are changing and getting more powerful, and even the threat landscape is always changing (Jeun & Won, 2012). Therefore, these rapidly changing external and internal factors need to be managed in a harmony. IT GRC helps to govern this in a corporation, especially in a bank. The thesis, it is aimed to create a tailored GRC model to help banks' governing body to evaluate, direct and monitor

IT-related activities. It is based on Cobit 2019 due to the regulatory direction of compliance in Turkey's banking sector. The proposed model needed to be a collaborative approach that solves the problem mentioned in the problem definition. It also covers the compliance issues with strong participation in the compliance dimension. An objective way is needed to align specific (county or sector-specific) regulations or a best practice to another best practice. After creating the IT GRC model, its regulation relatedness is defined with an application to simply adapt actions to comply with. Using methodology would be a scientific objective way to create relatedness of regulation to a best practice. The state of the art of this thesis proposes to bridge the gap between an IT GRC model and regulation with a scientific objective approach with the help of a natural language algorithm "latent semantic analysis".

1.3. Research Objective

The thesis aim is to create a tailored IT GRC model. Especially in governing risk and compliance dimensions creating an IT GRC model is complicated (Marchant & Wallach, 2015). The finance and banking sector are highly regulated and, in this sector, businesses are using high technology in their processes. It is hard to be compliant in this volatile financial environment (Edwards & Wolfe 2004). Moreover, risk management is another important domain in this sector. To govern all aspects of a bank it is needed to align all IT-related regulations and create a model which can be implemented in a quantitative survey and a best practice-based tailored model.

Cobit is a known best practice used to govern IT by ISACA (Information Systems Audit and Control Association) (ISACA, 2012). In Turkey, Cobit is widely used to mature information technology processes, especially in the banking sector (Topçu & Metin, 2011). In 2011 BRSA created a communiqué to announce the mandatory use of Cobit. In 2020 BRSA announced its own created detailed IT regulation. By creating Cobit 2019, ISACA updated the Cobit and suggests a tailored IT governance system (ISACA, 2019). ISACA created 4 books to define their proposed tailored GRC system. In this thesis, Cobit 2019 design guide was used to create an IT GRC model to comply with BRSA's regulatory obligations. Cobit design guide offers 11 design factors to evaluate by an IT governor and create a tailored GRC model. In this thesis based on selected 10 design factors, a survey was created for a collaboratively creating tailored GRC model. After the creation of the survey, it was implemented on the sample bank's governing body's 52 participants. Cobit 2019 does not include a regulatory dimension, it only stated to include related regulations with an only the

IT governor's aspect, and the regulation dimension offered model creation is not effective. The proposed collaborative approach suggests a survey, which consists of Cobit 2019's 10 design factors' results and constructs the tailored GRC model. After creating the GRC model, Cobit core's whole 40 processes were used to define the importance or maturity levels to implement on the sample bank. This model can be implemented in any sector not only in banks but also in small businesses or else. Without local regulations, evaluating only the best practices' actions is not enough (Zaring, 2006; Albu, C, Albu, N., and Alexander, 2014). Every year independent auditors or banking internal inspectors/auditors audit the regulation needs (BRSA, 2015). Their basis comes from local or global regulations. Sometimes if a bank has a foreign owner or a major stakeholder, its regulation needs to expand. Every country has its banking regulations and its needs are always changing (Barth, Caprio, and Levine, 2013). Following these changes is very hard without using a GRC system (OCEG, 2021).

In Turkey, BRSA creates IT-related regulations. In 2020, BRSA announced a new regulation to obey titled; "Information Systems and Electronics of Banks Regulation on Banking Services" (BRSA, 2019). This regulation creates detailed rules for every IT process. BRSA addressed Cobit 4.1 to comply with but in 2019 "Communiqué on Principles to Be Considered in Information Systems Management in Banks" was repealed (BRSA, 2019). With the new regulation, banks should create new governance, risk, and compliance management mechanisms to govern. Banks need to design new committees to govern their IT. New compliance requirements show the importance of IT GRC (OCEG, 2021). All these changes make it necessary to adapt quickly to all the updates on the regulation side and require an IT GRC model that can address all the risks that the business is in, and can address all threats and legal requirements originating from information technology processes. There is also a need to address the requirements in the dimension of regulation by determining the relationship within international best practices with a dynamic method. The relationship matrix created in this thesis is aimed to establish a dynamic bridge between Cobit and the latest BRSA's IT regulation. This proposed relation creation method is adaptable to find the relation between any best practices or best practices to a specific regulation.

Current methods of creating relationship matrices show a top-down approach based on expert opinions. After the academic literature reviews, it was seen that the approaches were generally subjective and relationship definitions were made at a high level. No study or

method has been encountered that aims to find the relations between each other in the most detailed practices or actions of regulation or international best practices. Natural language processing methods were not used as an objective method to find the relations of all practices with each other with a bottom-up approach. Semantic analysis methods made it possible to understand text content and relate to a specific topic or another text (Rieger, 2021).

Latent semantic analysis is used in this thesis to map selected regulation's actions and Cobit 2019's practices. LSA is a natural language processing method that is useful in paragraph-based meaning exposure. (Landauer, 2007). Created relation map is a 224*1202 matrix to show the relatedness of selected BRSA regulation to Cobit or Cobit to regulation's articles. By creating these two ways, GRC participants can evaluate, direct or monitor Cobit or regulation-based investigations. After creating relatedness matrices Power BI's Power Query was used to create 2 dashboards to have an application. With the help of these applications, IT process owners, auditors, inspectors, compliance controllers/officers, business process owners (affected by the related IT processes), IT governing body members, and executive senior management in charge of IT can view all the regulation items for the selected area or process, based on the relevant regulation, at any time. They can access all Cobit practices and actions with the highest associated. Similarly, if desired, all the mentioned parties make it possible to find the relevant articles in the legislation of any process selected from Cobit and to compare the legal provisions and Cobit practices and actions against these articles. A ranking is made by considering the maturity or importance levels of the 40 Cobit processes obtained with the created IT GRC model. With this ranking, the processes or domains that the selected bank should consider and the expectations of the regulatory authority for these areas or the recommendations in international good practice can be reported quickly.

2. LITERATURE REVIEW

2.1. Corporate Governance, Governance, Risk, and Compliance

Corporate governance is an old term, and has various meanings but in general defined as a system. This system is based on regulations, rules, related policies, and procedures that regulate, and control the company's activities (Gillan and Starks, 1998). Obtaining strategic inputs, determining performance targets, establishing important appointments, and oversight of management can be counted as the four most important items of corporate governance. The element in each item is the quality of decision-making, so all controls are focused on board structures, composition, and processes. Most of these studies (Forbes and Milliken, 1999; Denis, 2001; Daily, Dalton and Cannella, 2003; Noonan and Watson, 2007; Frankforter, Davis, Vollrath and Hill, 2007) have been studied in detail. In addition, studies involving the effects of organizational performance on corporate governance (Mueller, 2006; Kiel and Nicholson, 2006; Brennan, 2006; Choi, Park and Yoo, 2007; Raja and Kumar, 2007; Kroll, Walters, and Wright, 2008) is located. If corporate governance is considered a tool that enables investors to truly reclaim the amount of capital they have placed in the investment, it becomes necessary for the banking sector to establish a structure that will secure the rights of all stakeholders, especially its customers, in the face of the possibility of realization of the risks it is exposed to due to its activities (Kiel and Nicholson, 2002; Kleffner, Lee, and McGannon, 2003).

Risk management is the desire to eliminate the factors that will prevent or delay the achievement of the target in all kinds of activities to be carried out within an ethical framework, which will reward the capital owner, and the investor due to the bank's earning an acceptable level of profit, by managing the risk of loss or economic loss for any reason (Pforsich, Peterson, Kramer and Just, 2006)

The main problem with the organization and corporate governance is to mitigate the risk within the business. Agency problems arise between shareholders (principal) and managers, and executives (agents) in countries that are developed with diffused ownership of firms; the same issues arise between small and large shareholders in consolidated ownership developing countries (Shleifer and Vishny, 1997). Also, La Porta described this term as "a set of mechanisms through which outside investors protect themselves against expropriation by the insiders" (La Porta et al. 2000). Agency theory is explained by "the relationship between the managers (agents) and the shareholders (principals)" (Donaldson and Davis, 1991). In Jensen and Meckling's article, the agency theory is applied to the modern

company, and the potential for conflict of interest between shareholders and controllers is revealed. (Jensen, Meckling, 1976) The work of Jensen and Meckling formed the basis of many theoretical and empirical studies. After this period, the problems that arise when the decision-making authority in the companies is in the hands of the managers who do not own the company shares, and the solutions related to them, economics, business, law, etc. have been the subject of investigation in different areas (Fama, 1980). In the 1970s and 1980s, research focused mainly on the corporate governance of American companies, and from the early 1990s, corporate governance practices in Japan, Germany, and England began to be the subject of research. (Denis and McConnell, 2003) In recent years, it is seen that corporate governance has gained importance in both developed and developing countries all over the world.

Although legislation and regulations differ for all countries, corporate governance aims to mitigate the problem of agency. It gives agencies less legal rights than common laws (La Porta et al., 1998). Corporate governance mechanisms can be categorized as internal, that is structural, or external like market-based. Internal corporate governance structures are formed by structural, and firm-specific facts; while externals are influenced by legislation, and laws at the country level imposed by governing authorities or the board of capital markets (Dennis and McConnell, 2003).

Enron and WorldCom scandals in 2001 shocked the World. They were the major drivers of corporate governance, enactment of the Sarbanes–Oxley (SOX) Act in 2002 by the US government created to legislate/regulate a set of good corporate governance, best practices, and standards/mechanisms (Ailon, 2011). Nearly all countries published their acts, legislations, or modified their principles of corporate governance in the year of 2000s. Turkey also released a corporate governance code, named “Corporate Governance Communiqué” (January 2014) corporate governance principles (Corporate Governance Communiqué Annex I, aka “Kurumsal Yönetim Tebliği”, 2000).

“Institute on Governance” defines governance as “governance determines who has power, who makes decisions, how other players make their voice heard, and how an account is rendered.”. “Institute on Governance” created five principles depicted in Figure 2.1 that gives key elements of corporate governance.

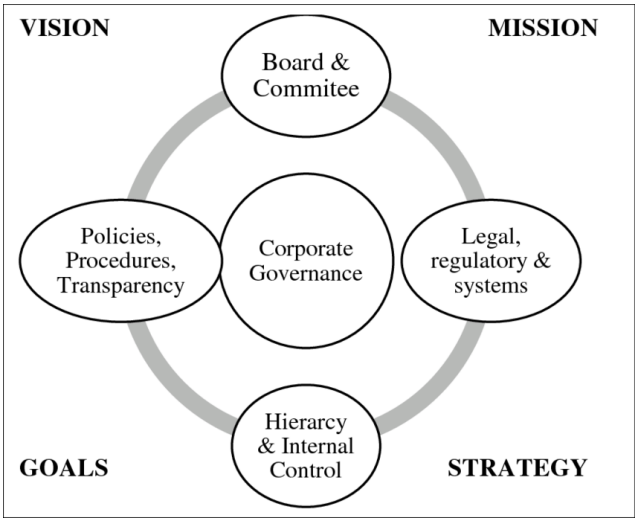


Figure 2.1 Corporate governance key elements
(Source: Institute on Governance, 2016)

Corporate governance key elements consist of legal, and regulatory systems for creating a compatible control environment, then a hierarchical internal control environment. For this environment businesses create policies, procedures, and principles of practices to achieve their goals in line with their strategy. Corporate governance helps them to achieve their vision in line with their mission (IOG, 2006).

Greuning et al. worked on "liberalization and the volatility of financial markets, increased competition, and diversification expose banks to new risks and challenges, requiring the continuous innovation of ways to manage the business, and its associated risks to remain competitive. The increasing market orientation of banks has also necessitated changes in the approach to regulation and supervision. The responsibility for maintenance of the banking system and markets is being redefined, in one country after another, as a partnership among several key players who manage various dimensions of financial and operational risks." (Greuning et al, 2022). They define parties related with a bank as; "bank regulators and supervisors, Shareholders, board of directors, executive management, audit committee, external auditors, public/consumer, investors/depositors, rating agencies and media" (IOG, 2016).

2.2. IT Governance (Enterprise Governance of IT)

"IT management" and "IT governance" terms have different meanings. IT governance defines strategy, and IT management implements the defined strategy. Also, IT governance focus on "structural arrangements", "formal processes" and "relational mechanisms" (Gregory et al., 2018). In Cobit there are 40 processes, "IT management" has a process

(processes) and managing them. They are the owners or custodians of these processes, and run one (or more) of them, but "IT governance" selects which Cobit processes are needed to be more mature or works on what is the maturity level of selected processes. "Enterprise governance of IT" term is used for IT governance, and IT corporate governance term is also used instead of IT governance (De Haes et al., 2020).

IT/IS governance and digital transformation are trending hot topic subjects. Digital transformation is all around the world, and many businesses are still changing digitally (Valentine and Stewart, 2015). Information technologies or information systems (IT/IS) are getting more vital every day. IT costs to the enterprises are so high but it is getting more and more. Worldwide IT spending was projected at nearly USD 4 billion in 2021 (Gartner, 2020). The yearly basis of IT spending is given in Table 2.1.

Table 2.1. "Worldwide IT spending forecast by Gartner" (billions of USD)

	2019 Spending	2019 Growth (%)	2020 Spending	2020 Growth (%)	2021 Spending	2021 Growth (%)
"Data Center Systems"	205	-21	208	1.9	212	1.5
"Enterprise Software"	456	8.5	503	10.5	556	10.5
"Devices"	682	-4.3	688	0.8	685	-0.3
"IT Services"	1,030	3.6	1,081	5	1.140	5.5
"Communications Services"	1,364	-1.1	1,384	1,5	1,413	2.1
"Overall IT"	3,737	0.5	3,865	3.4	4,007	3.7

(**Source: "**Gartner global IT spending report", 2020**)**

In January 2020 due to the Covid-19 pandemic conditions, in the year 2020 overall IT Spending decreases by -5,4% and goes below the year 2019 overall spending (Gartner, 2020). Extreme economic conditions effects corporates' IT spending but are still expected to grow in the fiscal year of 2021, by 3,7%. Gartner express this situation; "The public health interventions that countries imposed to control the spread of Covid-19 devastated global IT spend. Industries facing prolonged lockdowns, such as entertainment and air transport, are cutting total IT spending by more than 30 percent in 2020." ("IT Spending Forecast, 3Q20: Technology Trends Accelerated by COVID," 2020).

However, "some technologies and IT trends accelerated in both adoption and spending". Also, of the pandemic situation digitalization accelerated. Gartner again uses these words to express; "Covid-19 actually brings the future forward" (Gartner, 2020).

The high degree of automation or (hyperlocomotion defined by Gartner) of the business processes has undoubtedly made IT a target for violations of compliance and governance, since in practice the alignment of IT with business objectives often goes hand in hand, and sometimes with neglecting control objectives (Müller, 2008).

Corporate governance is decisive, and is subordinate to corporate governance in the development of IT governance. IT governance deals with the definition of processes that can ensure support for organizational objectives and strategies (Silva et al., 2018). Corporate decision-makers are making IT-related decisions at all management levels and types of (i.e., operational, tactical, and strategic) levels. IT management (operational) and IT governance (more strategic) developed to help corporates to address these issues and ensure effective control of their current and future use of information technologies and all related systems (ISO/IEC, 2015; Peterson, 2004; ISACA, 2018).

At the beginning of the 1990s, the word "IT governance" began appearing in academic research. Loh and Venkatraman (1992) used this term as IT outsourcing is about IT Governance, Henderson and Venkatraman (1993) suggested IT governance as a critical option for how a company is conducting itself in the IT marketplace.

Brown and Grant (2005) work on IT governance, and deals with aspects of IT governance and contingency/risk study of IT governance. Also, ISACA (Information Systems Audit and Control Association) uses this term efficiently. ISACA is an international professional association focused on IT governance. They created IT Governance frameworks like Cobit in the 2000s, and its management guidelines. They used this term for the value creation of IT.

Today IT Governance term has a more spread and common meaning and lots of organizations use a framework and create a method to implement it. IT governance is composed of leadership, organizational structures, and processes that ensure that IT supports the corporate strategy and objectives (Bergmann and Tiemeyer, 2017). Also, IT governance must be an essential part of corporate governance, also present in the coordination between the usage of IT resources and the organization's strategic goals, and must be the duty of the entire organization as a whole. (Huygh and De Haes, 2016).

As a part of corporate governance, the term IT Governance’s responsibility is owned by the senior management team (Bergeron et al., 2017). It includes decision-making and transparency powers to promote positive actions in the IT sector (Bergeron et al., 2017; Weill and Ross, 2004). It can change the organization’s operations and also its strategy. IT

governance helps this change by practices, and tries to ensure that advances made in technology enable organizations to meet their corporate goals, and strategy, therefore, adding value to the organization's profits (Lunardi et al., 2014). Cobit 4.1. categorized governance domains into 5 focus areas. These are depicted in Figure 2.2. every Cobit 4.1. process has more than 2 related focus areas. ISACA defined each process' focus areas as primary and secondary.

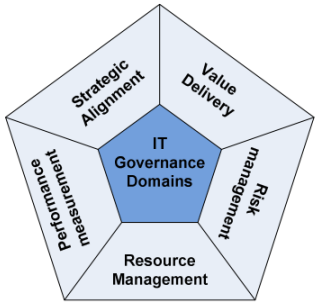


Figure 2.2. ISACA Cobit 4.1. IT governance domains

(Source: ISACA Cobit 4.1, 2007)

In 2007 ISACA defined IT Governance focus areas, so this involves IT governance to risk management, and resource management. IT generally imposes by the business owner as a cost the hidden value of creating efficiency, and adding value to any kind of process. IT Governance defines value delivery mission to the corporates, strategically aligned IT and the business itself can create more and more effective value/performance/service or product.

2.3. IT Governance Frameworks

Weil and Ross described an IT governance system as composed of structures, processes, and frameworks of relation. (Weill and Ross, 2004) IT governance mechanisms are shown in Table 2.2.

Table 2.2. Common IT governance mechanisms

"Decision-making structures"	"Alignment processes"	"Communication approaches"
"Executive or senior management committee"	"Tracking of IT projects and resources consumed"	"Work with managers who do not follow the rules"
"IT leadership committee comprising IT executives"	"Service-level agreements"	"Senior management Announcements"
"Process teams with IT Members"	"Formally tracking business value of IT"	"Office of CIO or office of IT governance"
"Business/IT relationship Managers"	"Chargeback arrangements"	"Web-based portals and intranets for IT"
"IT council comprising business and IT executives"		
"Architecture committee Capital approval committee"		

(**Source**: Weill and Ross, 2004)

The importance of developing institutional structures for IT governance together with the development and maintenance of personal relationships between senior management and all level of personnel in a company and IT. In the mid-2000s, academic researchers concentrated primarily on the real delivery processes for IT governance. While some researchers used exploratory analysis methods to uncover mechanisms for IT governance, others used some mechanisms to create a framework for IT governance, and verify suggested nomological networks. IT governance captured the attention of a group of professionals in the late 1990s. IT Governance Institute (ITGI) was established by the “Information Systems Audit and Control Association” (ISACA) in 1998 as an institute for IT governance. ISACA get an important role in developing IT GRC domains, expanding the importance of IT for organizations, and thereby the need or chance to create efficient control about all domains. ISACA also uses IT governance appeared largely informed by corporate governance, ISACA places IT governance as an integral part of a broad corporate governance system in its prominent ITGI IT Governance publication (ISACA, 2003).

One of the IT governance standards was the “Australian Standard for Information and Communication Technology Corporate Governance” (AS 8015, 2005) established by Principles Australia. This standard offered "[...] a framework of principles for Directors to use when evaluating, directing and monitoring the information and communication technology (ICT) portfolio in their organizations." (Standards Australia, 2005). The norm implemented an IT governance paradigm focused on a "Evaluate–Direct–Monitor" cycle.

AS 8015-2005 model later served as the basis for the ISO 38500 International IT Governance Standard which was first published in 2008 and revised in 2015. The purpose of this standard is to"[...] to provide principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations." (ISO/IEC, 2015), ISO/IEC 38500 standard defines this term “IT governance” as “The system by which the current and future use of IT is directed and controlled.” (ISO/IEC, 2008, 2015). ISO/IEC 38500 is a high-level framework that every kind of organization (kind or size) can use to align their IT with business objectives, and organizational decisions, and meet their legal, strategic, regulative, and ethical obligatory rules. ISO 38500 is recognized around the world because it is a vendor-neutral framework that any organization can use easily to implement.

ISACA (Information Systems Audit and Control Association) is established within the professional culture for the concept “Control Objectives for Information and Related

Technology (Cobit).” Cobit’s first edition was published in 1996. Cobit’s historical improvement graphic showed in Figure 2.3. (ISACA, 2019).

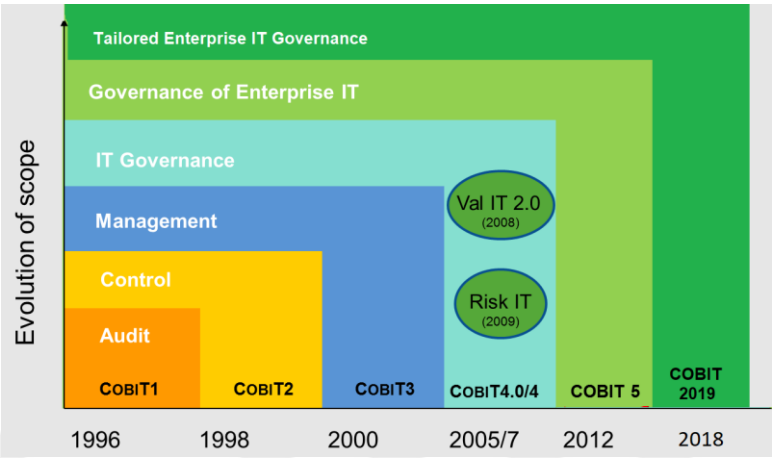


Figure 2.3. Cobit framework historical timeline

(Source: “https://www.isaca.org/why-isaca/about-us/isaca-50/cobit-over-the-years”, 2021)

ISACA developed Cobit for a mature IT management and IT governance system (De Haes et al., 2013). Jewer and McKay (2012) researched IT governance at the board level by using;

(1) The theory of strategic choices to research the relationships between the structure of a board, and its participation in IT governance,

(2) The structural theory to study the relationships between organizational influences and IT governance board involvement.

Joshi et al. (2013) proposed a transparency structure for IT governance, centered on the focused domains of IT governance as identified by the ITGI (2003), aka ISACA. This method can be used to determine the openness of a business regarding its IT governance, and to identify potential domains of accountability regarding IT governance from the firm's point of view. In total, this system for transparency in IT governance includes 39 disclosure elements spread across the following domains:

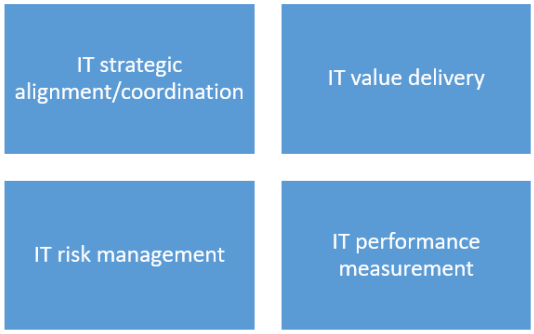


Figure 2.4. IT governance main domains

(**Source**: Joshi et al., 2013)

- "IT strategic alignment" is considered as IT expenditures need to promote an organization's corporate goals and objectives so that current and future market interest can be generated.
- "IT value delivery" applies to the optimization of IT value creation when the term is wider than purely about money (for example; higher productivity of employees, competitive advantage).
- "The risk management" includes the protection of all IT assets, properties and the rehabilitation or recovery of IT from disasters, and business continuity problems.
- "IT performance measurement " is linked to expenditures in IT investments and IT budget. It deals especially focused on IT capital investment and its business value partnership.

The full disclosure framework is given in Table 2.3. along with a description of each object. IT strategic alignment items and their descriptions are given on the table.

Table 2.3. IT governance disclosure framework

IT strategic alignment items	Description
"IT expert on the board"	"One or more board of directors who is/are independent or non-independent with sufficient knowledge regarding IT and information assets"
"IT expert with experience on the board"	"One or more board of directors who is/are with sufficient knowledge as well as work experience regarding IT and information assets"
"A CIO or an equivalent"	"Firm has a special CIO or an equivalent position with respect to IT and information assets at an executive level"
"IT committee"	"A committee looking after IT and information assets at the board level"
"IT risk is part of audit committee or risk committee"	"IT and information asset-related risk are on the agenda of the audit or risk committee"
"IT is part of audit committee"	"IT and information assets' auditing are part of the audit committee at the board level"
"IT steering committee"	"Firm has an IT steering committee which monitors IT management, IT spending, and related cost allocations"
"IT planning committee"	"Firm has an IT planning committee which looks after strategic planning and investment decisions on IT and information assets"
"Technology committee"	"A special committee which looks after IT and related technology architecture, projects, and governance issue at an executive level"
"IT committee at an executive level"	"In some countries, there is a two-tier structure of corporate governance, and in this situation, an IT committee may be formed at an executive level. This committee reports to the supervisory board"
"CIO or equivalent is on the board"	"A CIO or an equivalent position is represented at the board-level committee"

(**Source**: Joshi et al, 2013)

Joshi et al. also defined IT "value delivery" items and their description. They assess GRC actions to create IT value as mentioned in Table 2.4.

Table 2.4. IT value delivery items

IT value delivery items	**Description**
"IT governance framework/standard: ITIL/COBIT/ISO, etc."	"These are best practices and frameworks for IT governance. The firm has adopted or mentioned to adopt any IT governance framework"
"IT as an issue in the hoard meeting"	"IT and information assets' issues are explicitly discussed at the various board-level meeting"
"Suggestion/decision/advise by the board on IT"	"IT and related technology decisions, suggestions at the board level"
"Special report/section on IT/IT projects in annual report"	"A special report or a section dedicated to provide information about IT and information assets"
"IT mentioned as a strategic business issue"	"IT is mentioned as a strategic business issue to accomplish the business mission and goals"
"IT projected as strength"	"IT and information assets are mentioned as the organizational strength to achieve the business objectives, goals, etc."
"IT projected as opportunity"	"IT and information assets are referred to as the key assets to achieve the future opportunities"
"Project updates or comments"	"Updates or comment about ongoing and/or finished (successfully or unsuccessfully) IT and related projects"
"IT is explicitly mentioned for achieving specific business objectives"	"IT has been deployed to achieve one or more specific business objectives"
"Comments/updates on IT performance"	"There is/are comments about good or bad performance of IT"
"IT training"	"Information on IT and related training program for human resource"
"Green IT"	"Efficient and environment-friendly use of is termed as Green IT. A firm has reported on such initiative"
"Direction and status about IT outsourcing and in-sourcing"	"Information regarding in-sourcing or outsourcing of IT"

(**Source**: Joshi et al., 2013)

Another aspect is risk management. In Table 2.5. IT-related risks are classified and their description is given. Through all the risk management frameworks these risks are common, detailed process risks are not defined by Joshi et al.

Table 2.5. IT risk management items

IT risk management items	**Description**
"IT is referred to under the operational risk"	"IT is considered as a potential risk to successful business functioning and being treated as an operational risk"
"Special IT risk management program"	"Firm has a special program to mitigate IT and related technology risks"
"Use of IT for regulation and Compliance"	"IT is used to address the regulations and compliance requirements by the legal institutions"

IT risk management items	Description
“IT/electronic data processing (EDP) audit”	“Firm has explicitly reported regarding IT audit”
“Information and security policy/plan (IT security)”	“Firm has a clear information and security policy for its stakeholders (e.g., customers, employee)”
“The role of IT in accounting and the reporting standards (IAS)”	“IT support for the accounting and to address certain framework (e.g., Basel II)”
“Operations' continuity plan”	“IT and related technology continuity plans are mentioned in case of disaster”

(**Source**: Joshi et al., 2013)

The governance of a corporation has a significant impact on its "tone" or "culture." The culture of an organization may be beneficial or harmful. For a business, a good reputation is earned over a long time and through service. When an organization's culture contradicts a society's ethical or moral norms, its reputation suffers (Long, 2017). Corporate culture enhances the governance of business with all stakeholders' effects. Internal or external parties are involved to create the culture, and managing this is crucial. Also, one of the GRC frameworks OCEG defines itself as “… an organization that uniquely helps other organizations to enhance corporate culture, and integrate governance, risk management, and compliance processes” so implementing a GRC or an IT GRC framework related to the corporate culture, and it affects the related stakeholders.

Another important GRC aspect is the IT performance measurement process. Joshi et.al. defined generally cost-based metrics to measure the performance of IT. They also give intangible assets value differentiation. Direct and indirect costs evaluated.

Table 2.6. IT performance measurement items

IT performance measurement items	Description
“Explicit information on IT Expenditure”	“Financial and non-financial statements containing information on the overall IT expenditure”
“IT budget”	“Financial section of the document has disclosed the budget on IT and information assets”
“IT hardware cost”	“Specific IT hardware cost is mentioned under the IT Expenditure”
“IT software cost”	“Specific IT software cost is mentioned under the IT Expenditure”
“Explicit IT manpower cost is Mentioned”	“Specific IT manpower cost is mentioned under the IT Expenditure”
“IT expenses are mentioned under administrative cost”	“IT and information asset-related expenses are mentioned under the administrative cost”
“IT-related assets are mentioned under intangible assets”	“IT and related asset are referred as intangible assets and financial are provided as intangible assets”
“Direct cost on IT is mentioned in currency or percentage”	“The information on IT spending is given in the percentage of the total revenue or in other accounting ratios”

(**Source**: Joshi et al., 2013)

In the literature review of IT GRC, researching topics are gradually related to IT governance which is deeply relevant in action, thereby offering a holistic view of IT governance. Although academic researchers are specifically interested in particular IT governance-related concerns that are deemed relevant in risk and compliance, academic research for substantiation is also being looked at by the practitioners.

2000-2010 period of IT-related governance frameworks given in Table 2.7, mostly used IT-related best practices, and frameworks like Cobit, ITIL (Information Technology Infrastructure Library, and CMMI (Capability Maturity Model Integration) are still used widely. ITIL, Cobit, OCEG (The Open Compliance and Ethics Group), and other current frameworks are given detailly in the GRC frameworks section.

Table 2.7. IT-related governance frameworks

Framework	Description
IT GAM	"A set of 5 IT Decision Domains (principles. architecture, infrastructure. business applications, investment). Weill and Ross show how to govern each domain for optimal value creation."
ITGDF/GAM	"Part of the ITGAP process. in which managers first map 1T-related processes in their organizations before changing them to conform to one or more governance archetype."
CMM/CMMI	"CMM was originally developed in the mid- 1980s to aid in managing large software development projects. It posits S maturity levels. CMM was replaced by CMMI, which is broader in scope to include most business processes."
ITServiceCMM	"Capability Maturity Model for providers of IT services, with corresponding levels of service maturity."
ITIL V3	"ITIL is a guiding framework of best practices for service and asset management. In its 3rd version. it currently consists of 5 best practice volumes focused around the service lifecycle and continuous service improvement"
ASL	"Provides a framework for IT applications development that centers on 3 areas: functional management. application management and technical management"
SDM SDM2	"Developed in 1970 (by Pandata-since bought by Cap Gemini) and revised in 1987, it presents a 7-stage waterfall model."
SAS 70	"Developed in 1992 as a follow-on to SAS 55 (internal controls), this is an auditing standard to assess the internal controls on transaction processing. Became the basis of the standard eventually advocated by COSO."
ISO/IEC 20000	"Specifications and Code of Practice for IT Service Management. It is the first international standard for IT service management and is aligned with ITIL best practices."
6 Sigma	"Developed by Motorola in 1986, and widely used and adapted since, 6-sigma is a business improvement methodology aimed at measuring and correcting process and product defects. This may include IT services."
Prince 2	"A project management and control methodology developed in 1989 by the UK government for project managers. It defines project management along 8 broad processes. with 45 sub-processes"
AS-8015 (2005)	"The world's first national standard for governing ICTs. introduced in March 2003 and subsequently revised in 2005. It prescribes a 3-sequential-step approach to governing ICT projects and ICT operations: evaluate (uses of ICT)—direct (preparation and implementation of1CT plans and policies to best support the organization) monitor (conformance to polices and performance against the plans)."
ValIT	"A new framework aimed exclusively at IT governance, links management of the IT portfolio to the organization's strategic objectives."

Framework	Description
PMBOK	"The Project Management Body of Knowledge (PMBOK) is a set of standard terminology and guidelines (a body of knowledge) for project management. The body of knowledge evolves over time and is presented in A Guide to the Project Management Body of Knowledge (PMBOK Guide), a book whose seventh edition was released in 2021."
ITIL V4	"ITIL 4 - the most recent release of ITIL, was launched in Feb 2019. It's the first major update to the ITIL framework since 2007, designed in large part to keep up with recent trends in software development and IT operations."
ISO 27001	"ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes."
Cobit 4.1	"Version 4.1 of COBIT was released as an update in 2007. The framework approaches IT controls by looking at all of the information needed to support business requirements and the associated IT resources and processes. COBIT is intended for management, users, and auditors (mostly IT auditors)."
Cobit 5	"COBIT (Control Objectives for Information and Related Technology) helps organizations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organizational goals. COBIT 5, the latest iteration of the framework, was released in 2012."
Cobit 2019	"COBIT 2019 is the latest development of the renowned COBIT framework of ISACA. It addresses organizations' modern technologies, trends, and security needs. It involves other frameworks like TOGAF, CMMI, and ITIL, making it an ideal framework for process unification across a whole firm. In the latest update to COBIT, new theories and concepts have been introduced, including now 40 processes for developing a governance and management program."
ISO 38500	"ISO/IEC 38500 is the international standard for the corporate governance of information technology, and provides guidance to those advising, informing or assisting directors on the effective and acceptable use of information technology (IT) within the organization."

(**Source**: California Management Review vol. 51, no. 3, cmr.berkeley.edu)

Together with the definitions of IT-related governance frameworks in Table 2.7, they reveal the support they give to IT governance. In all new and old approaches, those with and without IT focus are separated. While ITIL, Cobit, ISO 27001, ISO 38500, and ITServiceCMM are directly related to IT, there are Cobit and ITIL frameworks that target IT governance and cover all IT processes rather than a specific area in IT. ITIL, on the other hand, is focused on IT service management, and Cobit differs from others in terms of IT governance. With the latest version of Cobit 2019, a tailored IT GRC model is proposed by adding IT risk and compliance dimensions in addition to IT governance.

2.4. IT risk

Within the scope of this thesis, one aspect of the IT GRC model is IT risk. The importance of the risk dimension for the IT GRC model, which is aimed to be established under this title, has been conveyed in the literature. Topics such as why IT risks are important for businesses today, what types of IT risk categories exist, what international good practices are to manage these risks, and how these risks can be managed better are discussed.

Nowadays, companies are exposed to a wide range of challenges from various cases such as globalization, populism, environmental change, technological change, complicated financial paradigm, and improvements in corporate governance (Gatzert and Martin, 2015; Tekathen and Dechow, 2013; Gordon et al., 2009).

In this digital age, companies are using advanced technology to process their knowledge to achieve their goals, risk management plays an important role in securing the information assets of an enterprise from IT-related vulnerabilities.

One important component of a productive IT security program is an efficient risk management mechanism. This risk management mechanism's main objective for a company is to secure the enterprise not just its IT properties, but all IT-related business processes. A business point of view is important in ISO and NIST standards. High-level sponsorship, and management support are critical to comply with a risk framework or a standard. Accordingly, the risk management mechanisms are complicated and must not be viewed solely as a technological task undertaken by the IT professionals who run and administer the IT infrastructure but as the organization's critical management function (NIST 800-39, 2011).

Risk management is an understanding of the real situation, and a method to recognize subject matter risk, risk assessment's main objective is to reduce risk to an acceptable level. IT risk management is the process that which an IT organization can measure the risk's costs, and the likelihood of IT-related or business-related effects. IT management tries to make improvements in project performance by organizing the IT procedures/processes and creating effective data to reach the goals of their organizations.

The leader of an organizational entity has to make sure that the company has the requisite resources to accomplish its task. In the face of real-world challenges, these project owners will assess the protection resources that their IT departments need to provide the desired maturity level of needed mission support. Most organizations have strict IT security budgets; thus, IT vulnerability protection investment needs to be looked at as closely as other management or executives' decisions. When used successfully, a well-structured and highly integrated risk management approach will help the organization's management to define appropriate and required controls for delivering necessary protections and capability (Risk IT, 2009).

IT risk or business risks are involved together, and IT risks if occur affect the business. It can happen with both unpredictable pace and severity, posing difficulties in achieving strategic goals, objectives, or targets. IT risks are categorized in Figure 2.5.

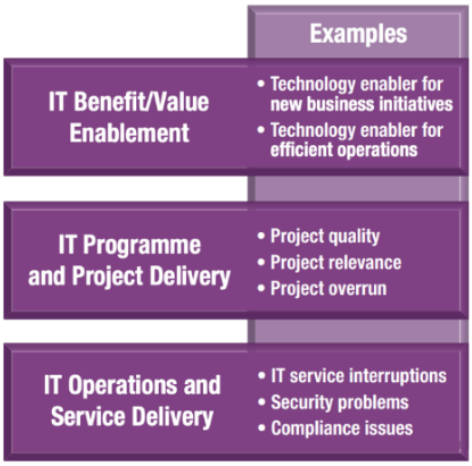


Figure 2.5. IT risks categories
(Source: ISACA Risk IT, 2009)

• "IT benefit/value enabling risk"; Opportunity to leverage technology to enhance business process performance or effectiveness, including as an enabler for new market strategies.

• "IT program and project delivery risk"; Associated with IT's commitment to innovative or enhanced enterprise solutions, typically in the context of projects and programs. It applies to controlling investment portfolios.

• "IT operations and service delivery risk"; Together with certain facets of IT infrastructure and systems efficiency that can add disruption or value loss to the organization.

IT risks is an integrated part of the enterprise's general risk environment, as shown in Figure 2.6. Dividing corporate risks into 6 different categories, ISACA stated that strategic, environmental, market, credit, operational, and compliance risks may all be related to IT risks. IT-related risks can arise from technology operations and service processes, as well as from IT-based projects or programs. The enterprise trying to obtain the IT benefits will also add the IT risks to the enterprise risk pool. IT risk is related to all business areas, and IT governance-related strategic and environmental risks can be related to IT. All the operation which are involved in IT creates IT risks that need to manage.

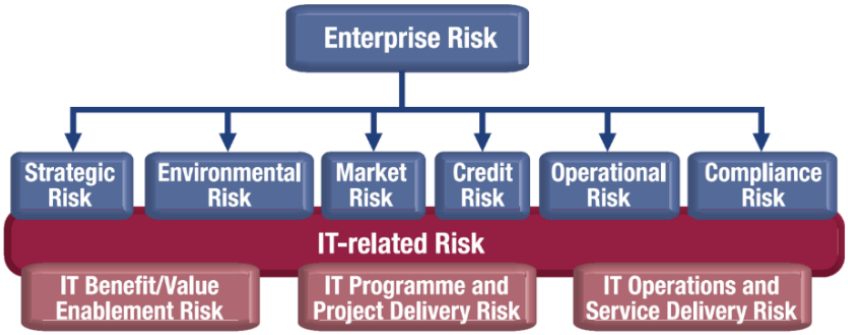


Figure 2.6. IT risk in the risk hierarchy

(Source: ISACA Risk IT, 2009)

Many IT risks may occur due to problems with third parties (delivery and solution development) both IT and business partners (for instance, a large business effect can be achieved if the IT supply chain risk is caused by a large supplier) can affect on these issues. Effective IT risk management requires a deep understanding of major dependencies. There is always a risk in IT, regardless of whether an organization is or is not known. In this context, potential major IT risk problems must be detected and handled.

IT risk management also requires a professional and well-understood of technology or infrastructure dependencies. Critical system may have dependencies and if exist, system deficiencies should be recognized and monitored. It is important to understand and handle important IT risks and plan their response in this context.

2.4.1. IT Risk Frameworks

Various IT risk frameworks have been developed in the IT risk management area, also in academy Lonita et al. (2013) and Abie and Borking (2012) have worked on and assessed them. Companies find the right ones to implement them. Frameworks for IT risk management are usually based on general objectives and properties.

2.4.1.1. Cobit "Control Objectives for Information and Related Technology"

Cobit is a very comprehensive framework that focuses on the management and governance of IT. The main aim is to align business and IT. IT risk management is a component of Cobit. ISACA created an IT risk management framework, depicted in Figure 2.7.

Figure 2.7. ISACA's risk IT framework

(Source: ISACA Risk IT, 2009)

ISACA risk IT framework includes the following steps (ISACA, 2009);

1. Risk evaluation; In this step, after the information gathering step, a risk analysis is made and a risk profile is created. IT-related risks and business relationships are also determined. Risk identification is the basis for the first step to understand the business goals and the relation of these goals to IT. Sometimes risks stem from IT threats that could affect business goals. In doing so, existing weak points and known probabilities become considered.

2. Risk response; In this step, risks are managed. Action plans are prepared for risks. All IT-related issues are determined, and activities for solving cost effectively are determined. After a prioritization is made to determine which risk should be addressed first and which can be treated later, response plans created by the risk's likelihood and impact.

3. Risk Governance; With this step, IT risks are associated with basic risk management processes. Risk-aware processes are carried out, ensuring that business decisions are taken by considering risks. The maintenance of risks is continuous. As the risks are affected by the internal and external factors of the institution, the risks also need to be constantly changed and updated. The company should operate risks as cost-effectively as possible. There could be remaining residual risk within the company's tolerance range. Every risk should be dealt

with appropriate mitigation techniques (avoidance, mitigation, transfer, or acceptance) (Beißel, 2013).

IT risk management in Cobit is only part of the overall risk framework and there are strong links to the generally applicable requirements in Cobit (ISACA, 2015). Cobit principles apply to all content, including IT risk management. These are; consideration of stakeholder interests, coverage of the entire company, uniformity, a holistic approach, and the separation between governance and management. ISACA also created Cobit 5 for Risk. In Cobit 5 for Risk, ISACA created two perspectives; "risk function and risk management perspective". They are related to Cobit 5 enablers. From a "risk management perspective core risk, governance and risk management processed and ISACA describes how risks can be mitigated by using Cobit 5 enablers". (ISACA, 2019) From a risk function perspective, ISACA describes "how to build and sustain a risk function in a business by using Cobit 5 enablers", from a risk function and risk management perspective (ISACA, 2019).

2.4.1.2. FAIR ("Factor Analysis of Information Risk")

FAIR offers a standardized framework and a basic guide to IT risk management. The instruction is limited to the basics without going into specific details. The focus is rather on clear definitions of terms with taxonomy and a clear structuring of the work steps. Companies can quickly create a uniform basis based on this structured information

The steps in FAIR for IT risk management (The Open Group, 2009) are as follows:

1. Identification of scenario components: In this first step identifying components to compile threat scenarios can be used. The assets that are at risk are the focus. Multiple levels can also be taken into account because some assets can affect others. Threats level needs to be identified. They become human/system and internally/externally divided.
2. Evaluation of the frequency of loss events: This involves several variables calculated and related to each other. A threat is measured by its frequency and strength. It is also considered as probabilities and control strengths. This results in the expected frequency of actual damage.
3. Evaluation of the expected amount of loss: First, all known threats are examined for their effects. Then determine which threats are most likely to occur.
4. Deriving risks: After defining the frequency and the amount of the expected damage, derive risks with response plans. With these values, you can now calculate the risks. These

can be in a two-dimensional matrix classified and assigned to any risk levels, like “low, medium, and high”. The fair model is depicted in Figure 2.8.

Figure 2.8. The Fair model

(**Source**: “Using the FAIR Model to Quantify Third-Party Cyber Risk, NormShield,” 2019)

The process of how to evaluate “risks” based on the Fair model is depicted in Figure 2.9. In this risk management system, it is stated that to reach an effective risk management system, it is necessary to establish an accurate risk governance model, perform meaningful measurements, make effective comparisons and make decisions with qualified information. Decision points relate to risk appetite, risk itself, solution options, and resources/capabilities. These policies are supported by processes and technologies, threats, assets are controlled, awareness, continuous communication with talent, and a risk management mechanism are established with supported processes. Areas defined in the fair model should be defined by the practitioners and provided as input to the proposed effective risk management system (The Open Group, 2009).

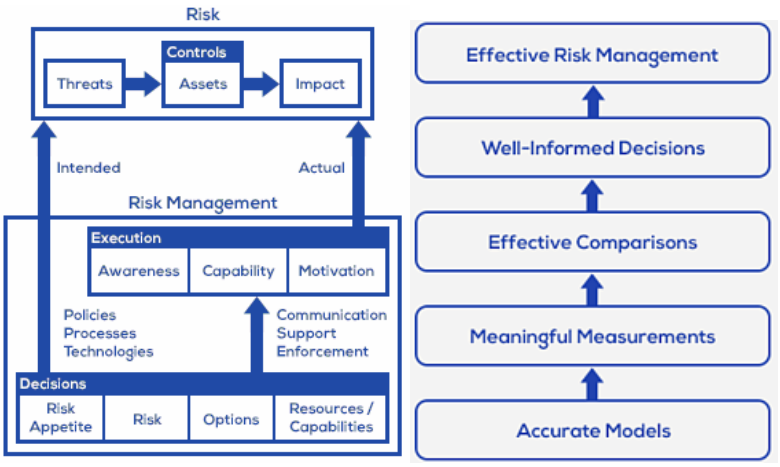


Figure 2.9. Implementing an effective risk management system

(**Source**: Using the FAIR Model to Quantify Third-Party Cyber Risk, NormShield, 2019)

2.4.1.3. FRAAP ("Facilitated Risk Analysis Process")

FRAAP is a qualitative risk analysis method (Peltier 2014). It always applies to exactly one asset, a system, an application, or a process that is focused. The analysis team consists of representatives from business departments and IT so that both the business goals and existing risks vulnerabilities and controls in IT can be considered.

The procedure with FRAAP is divided into three steps:
1. The Pre-FRAAP is an introductory step. In this step create the description of the scope, an information flow diagram, a list of members, and defining terms of definitions.

2. The FRAAP session step; consists of brainstorming by the team members, to identify possible weaknesses that could affect achieving business goals. The team members find a risk level for any threat by determining the likelihood of occurrence and impacts.

3. The Post-FRAAP includes a final analysis of the results and the completion of a summary management report. After going through the FRAAP steps, the owners or process responsible decide which protective measures are should be implemented.

2.4.1.4. ISO 31000 Standard

ISO 31000 is not a risk management framework even though it is a standard that contains basic principles and general processes for IT risk management. In line with the ISO standard 31000: In 2009 "MoR" (Management of Risk) was developed by Axelos. Axelos was established in 2014 by the United Kingdom Government to develop, manage and operate qualifications and best practices in methodologies owned by the Government Office of Commerce. ISO 31000 is not only defining the general process of IT risk management but also describes how it works with various company goals, it can be designed specifically. The steps from the ISO standard will be going through sequentially. In addition, communication can take place at any time and advice take place. Monitoring and assessment of risk management not only at the end but also in parallel with the entire process. The steps are as follows;

1. Create context: The company defines its goals, and internal and external parameters for risk management and specifies the scope and the criteria for the risk process.

2. Identify risks: The company should identify sources of risk, identify areas, events, causes, and, consequences.

3. Analyze risks: This phase serves to create an understanding of the risks. This involves sources of risk, causes, positive and negative consequences as well as probabilities are considered.

4. Assess risks: This phase is to support decisions on risk treatment. The information found on the identified risks is compared with the previously specified criteria and towards the underlying context. This allows for creating recommendations for action deduce.

5. Treat risks: To influence the risks appropriately, in this phase, different options are considered for action and selected the best option. This also changes the company's tolerance threshold for risks while considering the effectiveness of the options for action.

6. Monitoring and evaluation: The company should periodically or ad hoc examine measures whether the risk management processes are effective. through new events, important changes can occur or new risks have arisen.

General “ISO 31000” risk management process is depicted in Figure 2.10. Its method is based on plan, do, check, and act as other ISO-based standards.

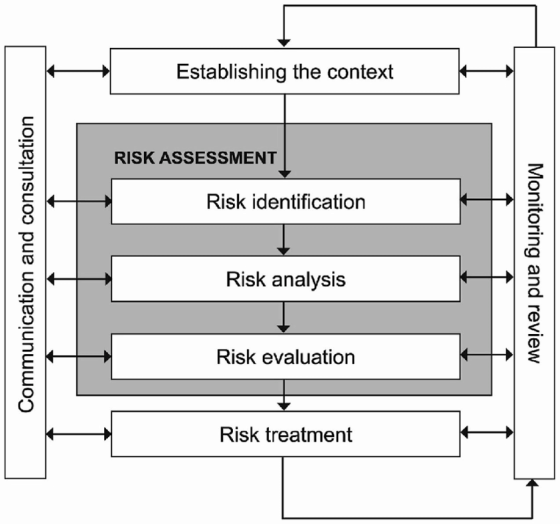


Figure 2.10. ISO 31000 the risk management process
(**Source:** AS/NzS ISO 31000:2009)

2.4.1.5. OCTAVE (“Operationally Critical Threat, Asset and Vulnerability Evaluation”)

OCTAVE was created by the CERT/CC (“Coordination Center of the Computer Emergency Response Teams”). This team is part of the SEI (“Software Engineering Institute”), a government-funded research and development institute of Carnegie-Mellon University. In this framework economic perspective of IT, risk management is in the foreground. The technical perspective is more in the background.

OCTAVE Allegro has 8 steps, these are:

1. Development of criteria for risk measurement: In the first step, the conditions are created to assess risks qualitatively and to understand the impact of risk in the organization. For this purpose, criteria for risk measurement, which take into account the specific circumstances of the organization are prioritized.

2. Development of profiles for property objects: In this step, risk profiles are described and developed. Risk profiles are special properties and values of assets. In the further course, risk profiles create the basis for the identification of threats and risks.

3. Identification of containers for information assets: containers are where information assets are stored, transported, or processed. Containers can also be outside the control of the organization. The assignment of assets to containers clarifies boundaries and other properties of information objects.

4. Identification of problem areas: The problem areas are identified in this step. Real-world scenarios are used to address threats and this describes undesirable effects.

5. Identification of threat scenarios: First, the known problem areas are elaborated by the properties of the associated threats. Then other threats are searched and visualized with a threat tree.

6. Identification of risks: Before this step, the effects of the threats are collected. effects of all potential threats will be referred to as a risk, for example, financial loss or reputational damage.

7. Analysis of risks: This step is determined as a quantitative risk assessment. It is based on the impact and probability of a risk for the organization and affected area.

8. Selection of risk management method: In the final step, the risks are prioritized by the ratings. The risks that should be reduced impacts or likelihood are identified and a corresponding strategy is developed. Octave's 8 steps risk management process is depicted in Figure 2.11.

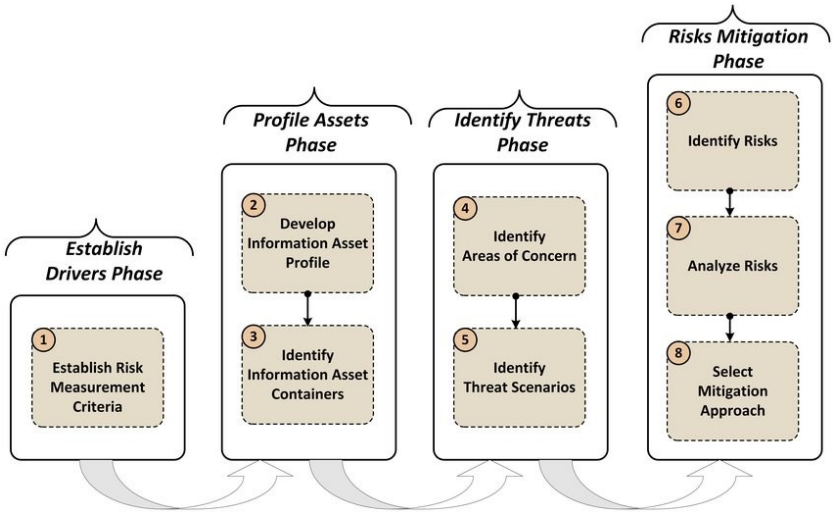


Figure 2.11. Octave Allegro risk management process

(Source: Caralli at. all, 2007)

2.4.1.6.RMF ("Risk Management Framework")

RMF was developed by NIST (National Institute of Standards and Technology). This framework is on the life cycle of IT systems. RMF is especially for companies, which are very strongly oriented to IT systems and their risk management want to align with IT. Due to the strong focus on IT systems, the framework can also be a useful addition to other frameworks, to be able to look at IT systems more precisely. The security lifecycle comprises six steps (NIST, 2010).

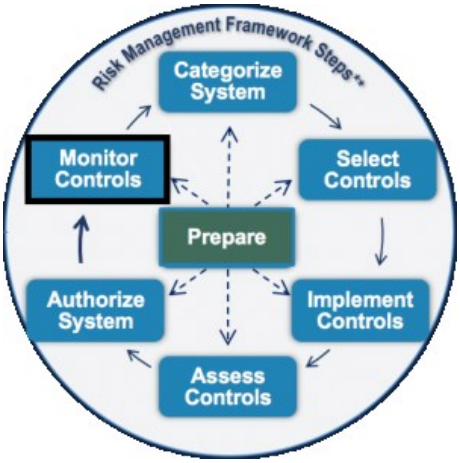


Figure 2.12. NIST's 6 steps for Risk Management Framework

(**Source**: "https://www.cybersaint.io/blog/six-steps-of-the-nist-risk-management-framework", 2021)

There are other risk management frameworks like RMM created by RIMS (Risk and Insurance Management Society) and TARA (Threat Agent Risk Assessment) developed by Intel. These frameworks are focused on a special field and will not express the details.

2.4.2. Risk Mitigation Techniques

Risk mitigation is a structured technique that utilizes to reduce risk. According to best practices like Cobit or NIST risk mitigation can be successfully managed through such risk mitigation options:

• Risk Assumption; Accepting future risk and maintaining the activity of the IT system or implementing controls to reduce the risk to an appropriate level

• Risk Avoidance; To prevent risk by removing the cause and/or effects of risk

• Risk Limitation; Reduce risk by implementing controls that mitigate the adverse impact of weakness performing a threat (e.g., use of assisting, protective, preventive, detective checklist or controls)

• Risk Planning; Managing risk through the creation of a risk mitigation strategy to identify, enforce and sustain controls

• Research and Acknowledgment; Reduce the risk of failure by identifying the weakness or defect, and study measures to fix the vulnerability

• Risk Transference; to move the liability to certain options, such as buying insurance, to cover the loss.

An organization's goals and purpose should be weighed when picking any of those methodologies for risk mitigation. Addressing all known risks may not be feasible, so priority should be provided to those which have the potential to cause significant impact or damage to the assets. The choice used to mitigate the risk and the approaches used to enforce controls that differ for each company.

NIST advises “best of breed” approach is to use appropriate options/methodology, along with the appropriate risk mitigation option. The techniques and risk mitigation process are depicted in Figure 2.13.

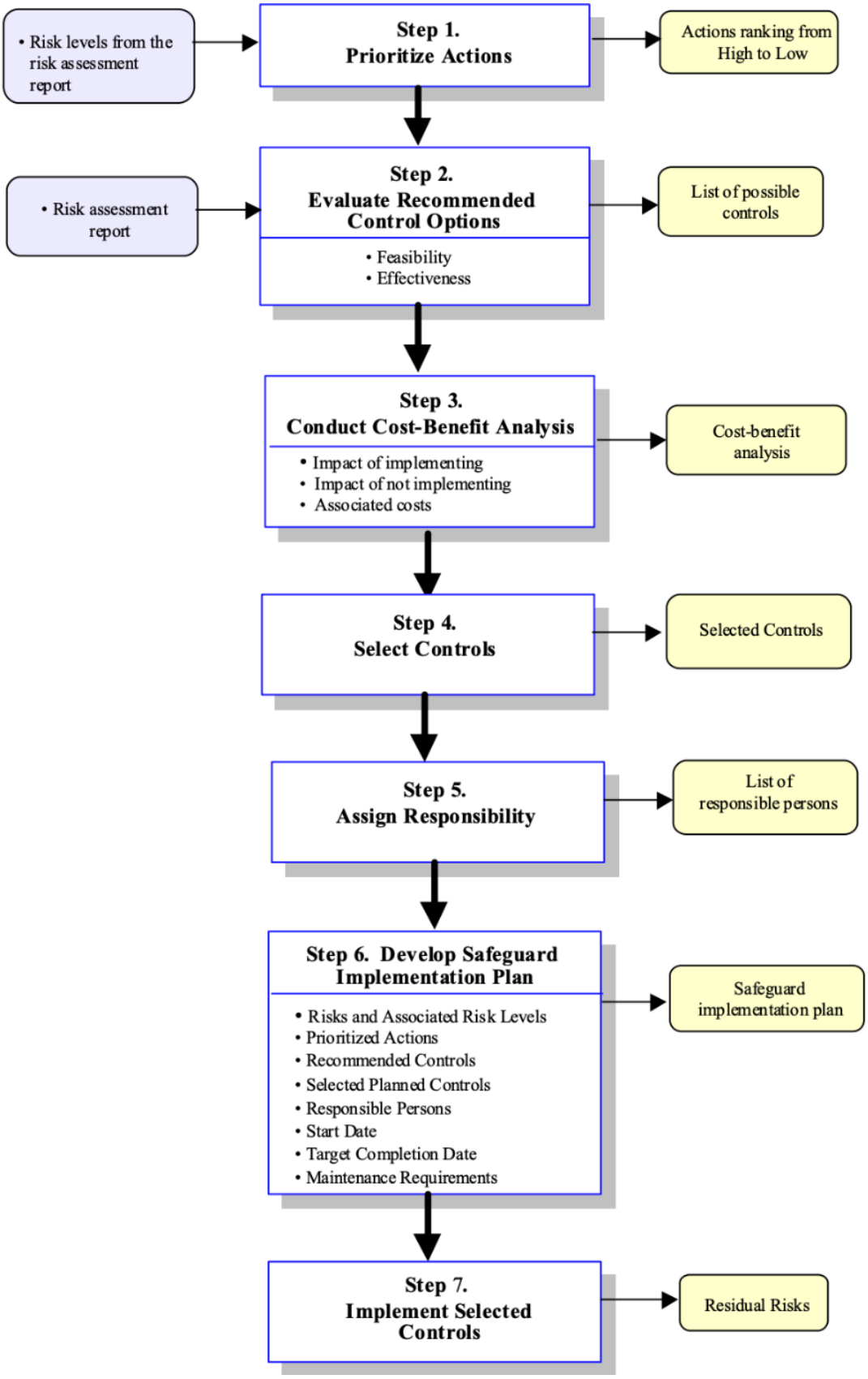


Figure 2.13. Risk mitigation techniques

(**Source:** NIST SP 800-30 framework, 2012)

2.5. IT compliance

Within the scope of this thesis, one dimension of the IT GRC model is IT compliance. Under this title, the importance of the compliance dimension for the efficiency of IT governance and the IT GRC model, which is aimed to be established, has been conveyed in the literature.

National and international standardization organizations grew after the major corporate scandals in recent history, these corporate scandals effects regulatory authorities to create new rules, and regulations to arrange related sectors with obligatory laws, regulations, and legislation. The awareness level significantly increases after the creation of a regulation. Compliance (to be compliant) definition is “acting by existing laws, regulations, protocols, standards and specifications.” (Tarantino, 2008).

As a result, several new regulations, protocols, policies, or guidelines emerged intending to control the business itself in accordance with the created rule. This supports government or stakeholder trust and investor protection. For companies, this means they must have the relevant legal, regulatory, and other requirements known and obeyed. A company is considered "compliant" if it is part of its business all relevant external but also internal (self-imposed) requirements are fulfilled. Accordingly, there is compliance if all are binding for the company's legal norms are verifiably observed (Klotz, 2009).

The best-known legal norms are for example the “Sarbanes Oxley Act (SOX)”, created by the “International Accounting Standards (IAS),” the minimum requirements for risk management (MaRisk), “Basel III” and the “Law on Control and Transparency in Corporate division” (KonTraG) and “Solvency II”. Requirements are not only legal norms but also standards or best practices, such as the ISO/NIST standards or PCI-DSS (“Payment Card Industry Data Security Standard”, regulations for credit and other payment cards), GDPR (General Data Protection Regulation) or industry-specific good practices such HIPAA (Health Insurance Portability and Accountability Act).

Also, contracts and internal guidelines for work organizations are compliance requirements. The intensity of compliance can be measured by representing a pyramid. The foundation of the pyramid is mandatory compliance with legal and other legally binding requirements. On the second All best practices (norms, standards, reference models), and compliance should be done voluntarily, but compliance on the other hand by important stakeholders (customers, business partners of the Companies) can be enforced (Strasser and Wittek 2012, 2013). The top of the pyramid is represented by the voluntary commitment of companies, and certain

external and internal requirements (e.g., social responsibility). Stakeholder expectations play a key role at this level. Decisions for these reasons can lead to Shift content in the individual levels of the pyramid (Behringer 2013). This pyramid model is a metaphor to prioritize the compliance importance for an enterprise.

IT compliance is part of corporate compliance. It carries the rapidly increasing importance of IT for corporate success. A uniform formulation of the IT compliance term cannot be found in the literature (similar to the concept of IT governance) depending on which perspective you take; different definitions are used. IT compliance term is common in the basic idea that IT compliance knowledge and compliance with all requirements to the company. This is also the established process and in particular awareness of compliance requirements.

Falks suggests that good IT compliance consists of four components:

• Prevention of violations of the law motivated by corporate ethics and politics and disregard for similar legal norms,

• Motivated fulfillment of competitive requirements, based on industry-specific considerations,

• Establishment of an IT risk management and an internal control system (ICS) for IT according to the principles of proper management and storage of records and documents in electronic form and data access

• Management's liability in the event of a violation of compliance requirements. It is a task of IT compliance to recognize this relationship, from which the necessary conclusions for governance and risk management issues to draw and compliance with all regulations relevant for corporate IT to be monitored (Falk, 2012).

IT compliance is the state in which all generally applicable legal standards relevant to the company's IT can be demonstrated be respected. The “broad” view also implies compliance with other external as well as internal requirements, which the company calls relevant and accepted. These include standards, norms, and company-internal guidelines, which on the one hand have a voluntary character, and compliance with them is therefore decided on a company-specific basis can. (Sowa and Fedtke 2011; Klotz 2009).

On the other hand, legal standards can refer to these same standards. Standards can also become the "usual professional view" (Best Practice) or corporate guidelines can help meet a requirement be imperative, which in turn becomes an indirect obligation to comply with

leads. IT compliance should not be confused with IT-based Corporate Compliance. (Strasser and Wittek, 2012).

In principle pursue IT compliance and IT-supported corporate compliance with the same goal, the fulfillment of relevant requirements. IT-supported corporate compliance implies the use of IT, with the help of which compliance with the regulations is ensured ("Compliance through IT"). This includes special software, usually as a component of a GRC software suite that draws attention to (impending) violations or can prevent them in advance (e.g., programmed regulations in standard software to comply with the principles of proper accounting), especially GRC software suites. (Papazafeiropoulou and Spanaki, 2016). In contrast, compliance focuses the IT function ("Compliance of IT") on the fulfillment of requirements in and especially for the IT function. Examples include planning that meets specifications, methodical development, and proper operation of information systems based on suitable (e.g., modular, scalable) IT architectures according to common norms, standards, and other best practices. In practice, both perspectives have to be considered together. IT compliance is made up of IT-supported corporate compliance and compliance with the IT function together (Teubner and Feller, 2008; Klotz, 2009).

Since the effort to create an IT GRC model within the scope of the thesis will be created for the Turkish banking sector, the IT-specific regulations of BRSA have been examined in detail. Although the reasons for the IT GRC model to be created specifically for the banking sector have been explained in detail in the previous pages, the proposed model based on Cobit 2019 can be applied to all businesses other than the banking sector. Creating the model with the participation of all relevant business stakeholders with a holistic perspective of Cobit is an industry-agnostic approach. Examining the compliance dimension in the banking sector-specific is an important limitation. Because, in the absence of such a restriction, it will not be possible to determine which specific legislation will be provided as input to the model proposed as compliance. The regulations published by BRSA, which establishes regulations as an official authority in the Turkish banking sector and monitors their compliance, are obligatory. It has been ensured that all regulations to be provided as input to the IT GRC model include all current and in-use legislation of BRSA's IT regulations. In the following pages, these details are shared in the content of the thesis.

2.5.1. “Turkish Banking Regulation and Supervision Agency (BRSA)”

Banking Regulation and Supervision Agency’s mission is “to carry out the functions of regulation, supervision, and enforcement within the aim of providing reliability and stability in financial markets, ensuring the efficient running of the credit system, protecting rights and interests of savers and developing financial sector considers strategic planning as one of the main instruments to fulfill its duties effectively.” (BRSA, 2020)

BRSA mentioned on their website they are fully in line with international standards; “With its Implementing Decision no. 2016/2358 dated 20.12.2016, the European Commission acknowledged that the regulatory and supervisory framework of Turkey’s banking sector is equivalent to the European Union (EU) legislation in terms of the EU Regulation 575/2013 on Prudential Requirements for Credit Institutions and Investment Firms.” (BRSA, 2020).

BRSA created Turkish banking and financial institutions (like payment authorities) regulations. To comply with BRSA’s regulation, Banks gives a huge effort. IT-related regulation is wide in subjects but limited. Some major regulations and their most important issues are mentioned.

The BRSA’s IT-related legislative information here is given to explain the legislative provisions that will be input to the proposed GRC model of the thesis and the reason for choosing Cobit as the base framework. For cases where banks are audited by independent auditors based on Cobit and banks will be audited as in the communiqué prepared by the regulatory authority, if any unaddressed area/process occurs in the communiqué, banks need to comply with Cobit. Relevant regulations pointing to Cobit are shared. In the third part of the thesis, the Electronic Banking legislation (published in 2021), will establish an objective relationship map with the Cobit practices in the compliance dimension of the IT GRC model, and its basic features are shared in detail. Since the relationship map of 224 articles of this regulation and Cobit's 1202 action was created, the content of the legislation was explained.

2.5.2. “Regulation on Information Systems Audit to be Made in Banks by Independent Audit Institutions”

BRSA regulated the independent audit institutions with the help of “Regulation on Information Systems Audit to be Made in Banks by Independent Audit Institutions”. In this regulation, independent audit and advisory firms are obligated to rule their work within its scope of it. External audit firms’ IT audit works are performed by the rule of this regulation. External auditors also control the internal audit department's maturity and govern it. BRSA

is regulated as “The authorized institutions are obliged to audit and evaluate general controls and application controls. Firstly, their obligations about general control concerning the processes under the main titles of;” Audited main areas of IS by independent audit institutions is depicted in Figure 2.14.

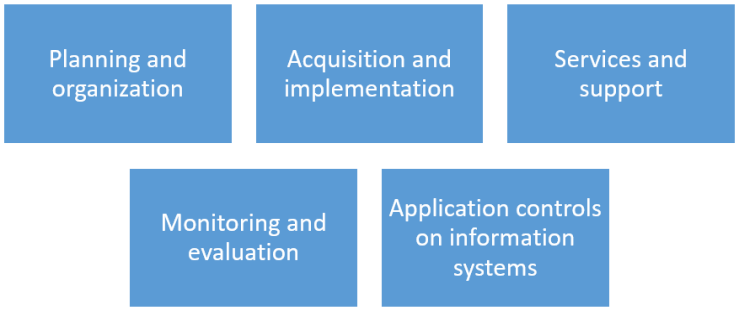


Figure 2.14. Audited main areas of IS by independent audit institutions (**Source:** “https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0131.pdf”, 2021)

After auditing these main domains independent audit firms should evaluate and assess the information systems governance processes and create a report. The IS auditing controls are divided into two main areas. Application and general controls. Within the main domains, there are control points (or controls) that are expected to be controlled by the auditors.

2.5.2.1. Application controls

Application controls are wide-ranging audit areas and should be audited annually. The concept of application controls in this regulation “internal audit system disclosed in the Regulation on Internal Audit of Banks and Risk Management Systems published in the Official Gazette dated February 8, 2001, and Nr. 24312” (BRSA, 2010).

According to IIA (“The Institute of Internal Auditors”) Application controls are defined as “controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting.” Therefore, the objective of application controls is to ensure the information mentioned in Figure 2.15. (IIA GTAG, 2010).

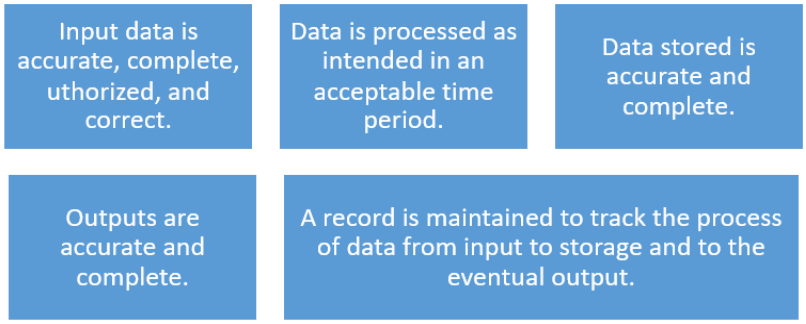


Figure 2.15. Information technology controls by IIA

(**Source:** GTAG 1: Information Technology Controls, 2010)

Application controls relate to commonly used tools or techniques. If a system is used to run processes, it needs integrity, accuracy, and consistency. These needs include input quality, output accuracy, processing quality, time-limited correct service capability, accurate and consistent data storage capability, etc. with expanded.

ISACA shows the application and general control relation and boundaries of business, general, and application controls in Figure 2.16.

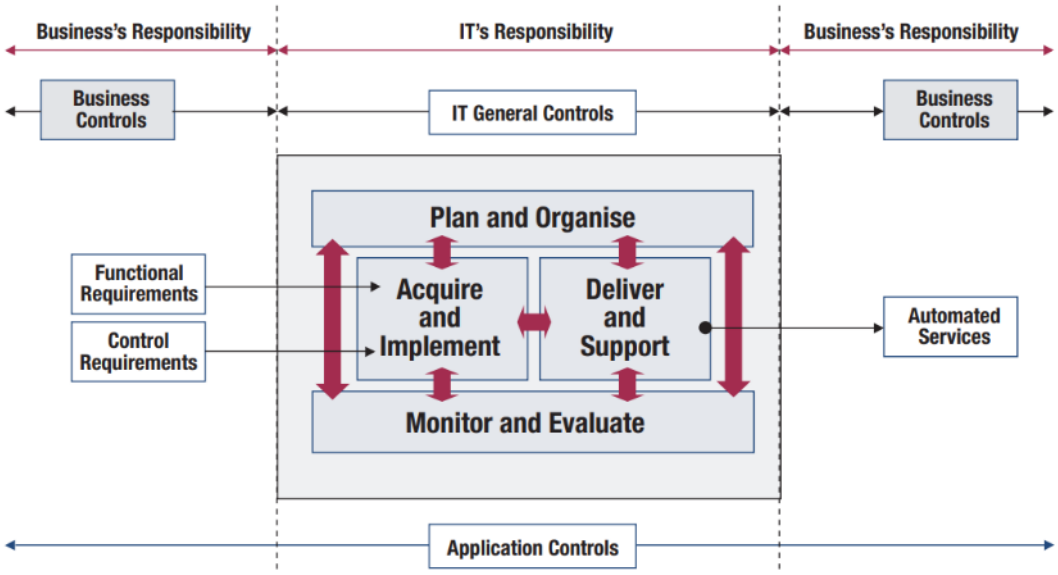


Figure 2.16. Application and general control relatedness by ISACA

(**Source:** ISACA Cobit 4.1. Framework, 2007)

IT General controls are related to all the IT-based domains. Application Controls' responsibilities are changeable, sometimes it's the responsibility of IT, or sometimes the business itself. It is individual applications objected to control and can be owned by IT or other departments. BRSA regulated this area defining each important control depicted in Figure 2.17.

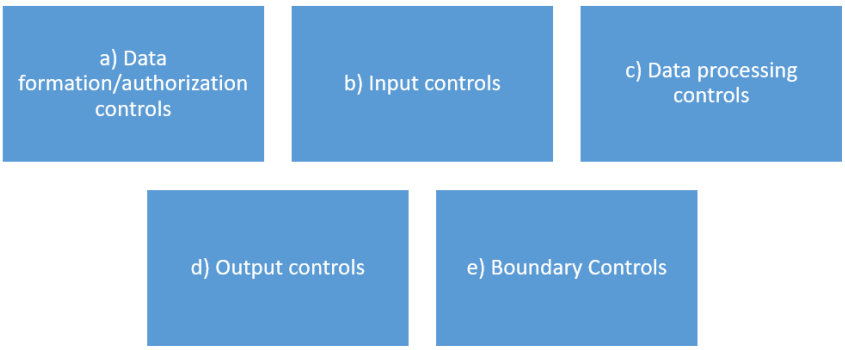


Figure 2.17. IT general controls defined by BRSA

(**Source:** "https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0131.pdf", 2021)

2.5.2.2. IT General Controls

Within the scope of general controls are audited concerning the 10 processes. These processes are mentioned in Figure 2.18.

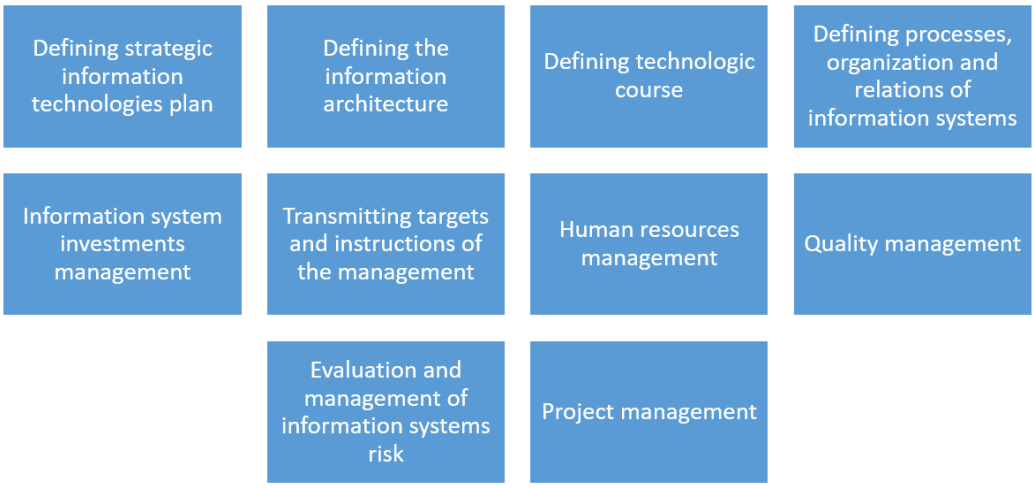


Figure 2.18. IT general controls

(**Source:** "https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0131.pdf", 2021)

BRSA created rules for the acquisition and implementation of general controls concerning the processes of:

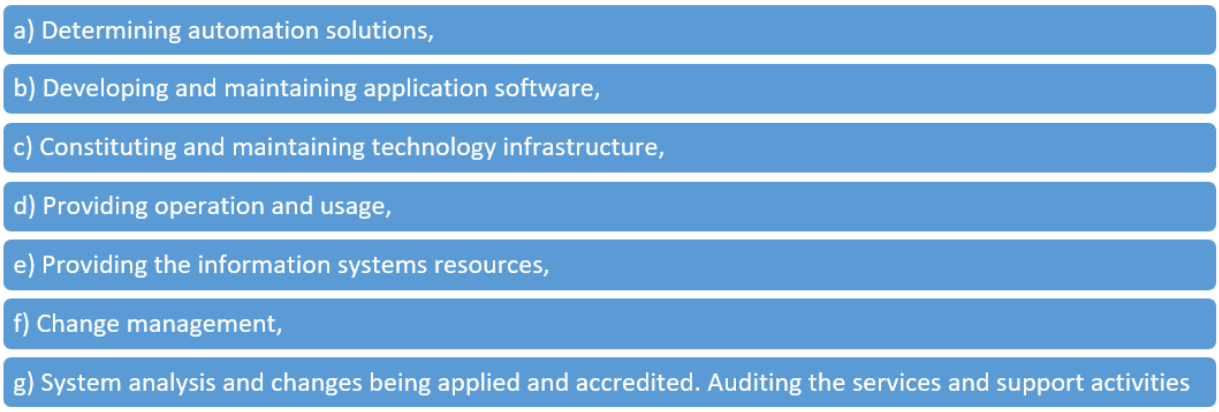


Figure 2.19. General control's main processes

(**Source:** "https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0131.pdf", 2021)

BRSA, article-16; "Service offered and support activities refer to offering the needed services safely and continuously including the required training. Within the scope of general controls concerning the services offered and support activities, control targets are audited concerning the processes of;"

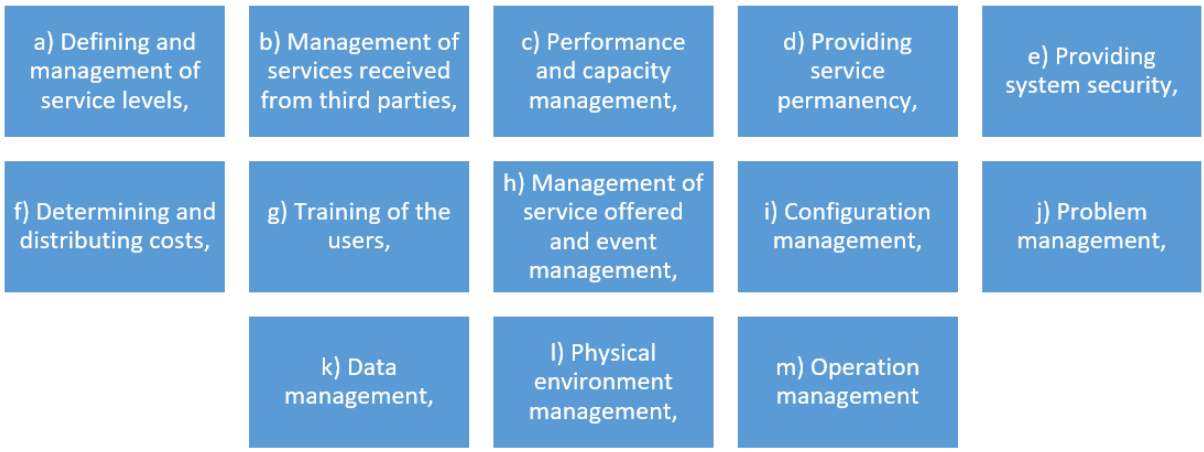


Figure 2.20. BRSA's defined I&T control target

(**Source:** "https://www.bddk.org.tr/ContentBddk/dokuman/mevzuat_0131.pdf", 2021)

BRSA, article-16 continues; "Monitoring activities include the periodical evaluation of the appropriateness and quality of the controls established concerning information technologies, by the party under audit. Within the scope of general controls concerning monitoring and evaluation, control objectives are audited concerning the processes of;

a) Monitoring and evaluating the information systems performance,

b) Monitoring and evaluating the internal control,

c) Providing the consistency of the party under audit to the relevant legislation including internal procedures and principles,

d) Ensuring corporate governance concerning information systems."

IT General controls cover all I&T-related processes but not in a specific way. General procedures should be defined for these processes. Banks used these regulations to define master rules and to create detailed rules they used best practices like Cobit.

2.5.3. "Communiqué on Principles to be Considered in Information Systems Management in Banks"

BRSA created this regulation to inform Banks about how to manage their information systems and processes. In Communiqué BRSA mentioned its aim; "to lay down the minimum principles and procedures to be considered in information systems management which banks use in performing their activities."

The regulation starts with the information systems' importance for the management of IS in banks. In Communiqué BRSA states the importance as; "The bank treats information systems management as part of corporate management practices. Strategies relating to information systems are adjusted to the business targets for the bank to carry out its operations in a stable, competitive, and improving line, factors concerning information management are positioned in the appropriate place within the administrative hierarchy and necessary financing and human resource is assigned for accurate management of information systems. The Bank establishes policies, procedures, and processes concerning information systems management. Procedures and processes are reviewed and renewed, if necessary, regularly in accordance with the changes in the line of business or technological developments. The efficiency of the management established on information systems is provided by the contribution of studies to be performed within the scope of risk management, internal control system and internal audit." As mentioned BRSA creates essential rules to be compliant with. With this regulation, BRSA regulation coverage increases to a high level. These rules were valid between 2011 to 2020. After creating the "Information Systems and Electronics of Banks Regulation on Banking Services" regulation in 2020 Banks started to be compliant with this regulation. Still, the bank's control environment is compliant with the "Communiqué on Principles to Be Considered in Information Systems Management in Banks" due to the passing period.

Other important sections in BRSA's Communiqué are as follows;

“Risk Management on Information Systems”

- “Information Systems risk management”
- “Management surveillance”
- “Establishment and management of security control process”
- “Management of support service procurement process on information systems”
- “Identity validation”
- “Incontestability and assigning responsibility”
- “Segregation of duties”
- “Authorization”
- “Consistency of transactions, records and locations”
- “Establishing audit trails”
- “Data confidentiality”
- “Informing customers”
- “Confidentiality of customer information”
- “Information systems continuity plan”
- “Emergency and Unexpected Events Plan”

Section Two;

- Information Systems Controls
- Implementation controls
- General controls
- Follow-up of Controls

Section Three;

- “Special Transactions”
- “Internet Banking”
    - Provisions to be used in internet banking
    - Surveillance of the management
    - Establishment and management of Security control Process
    - Identity Validation
    - Incontestability and assigning responsibility
    - Establishing audit trails
    - Informing the customers
    - Service continuity and rescue plan
- ATM
    - ATM security

Section Four;

- Wireless Communication Technologies
- “Situations not provisioned by the Communiqué”

“Article 34 — (1) In case of situations not provisioned by this Communiqué; the principles and procedures taken place within the Regulation on Internal Systems as well as the principles and procedures taken place within the Cobit documents presenting the internationally accepted information technologies control targets are applied.”

By the article 34, BRSA forced Banks to be compatible with control objectives defined in Cobit best practices. Also, in the regulation, the version of Cobit is not mentioned by the way the regulation was submitted year Banks used Cobit 4.1 to be compliant in their IT processes.

With this article, the framework for creating the proposed GRC model of the thesis has been ensured to be Cobit. Cobit’s latest version was selected due to the regulatory obligation.

2.5.4. “Information Systems and Electronics of Banks Regulation on Banking Services”

BRSA prepared the “Regulation on Banks' Information Systems and Electronic Banking Services” regulation in 2019. It was published in the Official Gazette No. 31069 dated March 15, 2020, and entered into force on July 1, 2020.

The regulation is important for some reasons, “Open banking services”, “API” (application programming interface), cloud computing concepts, and technologies have been introduced to the banking legislation for the first time. Other repeated parts explained detailly and regulations coverage of IT processes are increased. It can be understood that the regulation was prepared by a high technology talented professional team, they used lots of best practices mixed into this regulation. Defined all processes are generally clear and create rules in a mindful reason to comply.

Regulation is divided into four sections. The first section is about preliminary provisions. BRSA gave a basis and made an introduction of the regulation in this part. Parts detail has given in Table 2.8.

Table 2.8. Preliminary provisions

Preliminary Provisions	Purpose and scope
	Basis
	Definitions and abbreviations

(Source: “https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm”, 2021)

Regulation continues with the Risk Management part. Although in Communique risk management mentioned before, in this part BRSA creates rules about how to govern information risks on a Bank in detail. The board of directors must approve the IT strategic plan and establish a strategy committee. This part has 7 sections listed in Table 2.9. and its article numbers are given right next to its domain.

Table 2.9. Risk management

Risk Management and Establishment of Controls Regarding Information Systems	Information Systems Governance
	Managing IS Risk
	Information Security Management
	System Development and Change Management
	Information Systems Continuity and Availability Management
	IS Outsourcing
	IS Internal Control and Internal Audit

(Source: "https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm", 2021)

"Risk Management and Establishment of Controls Regarding Information Systems" main section has 33 related articles, their relatedness to main areas is depicted in Figure 2.21. BRSA creates detailed rules to manage information security management. 12 of articles are about IS security. This part creates a governance basis by the first IT GRC's, "G"; governance part. Continues with IS risk management and creates "R"; the risk dimension of a GRC system. Other parts and as a whole create "C" compliance dimension.

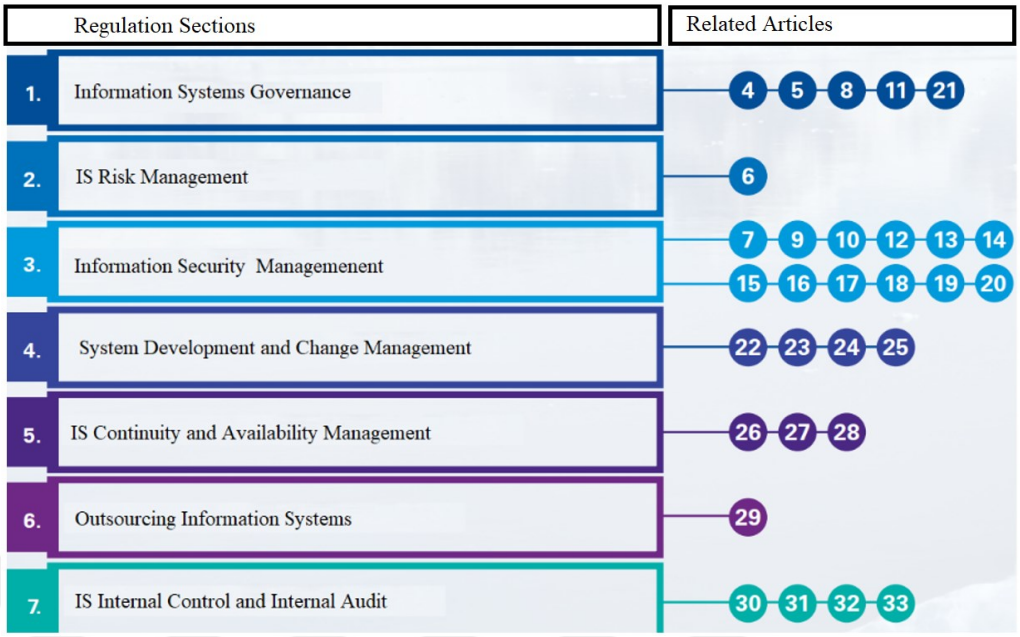


Figure 2.21. Risk management and establishment of controls regarding information systems (**Source**: Translated from; "https://assets.kpmg/content/dam/kpmg/tr/pdf/2020/03/bilgi-sistemleri-elektronik-bankacilik-hizmetleri.pdf", 2021)

The third section is about Electronic Banking Services. BRSA creates general controls to regulate this area. Nowadays banks try to imply new channels to serve more digitally. In this section mobile, internet, atm, and open banking standards were created. Related areas and article numbers are mentioned in Figure 2.22.

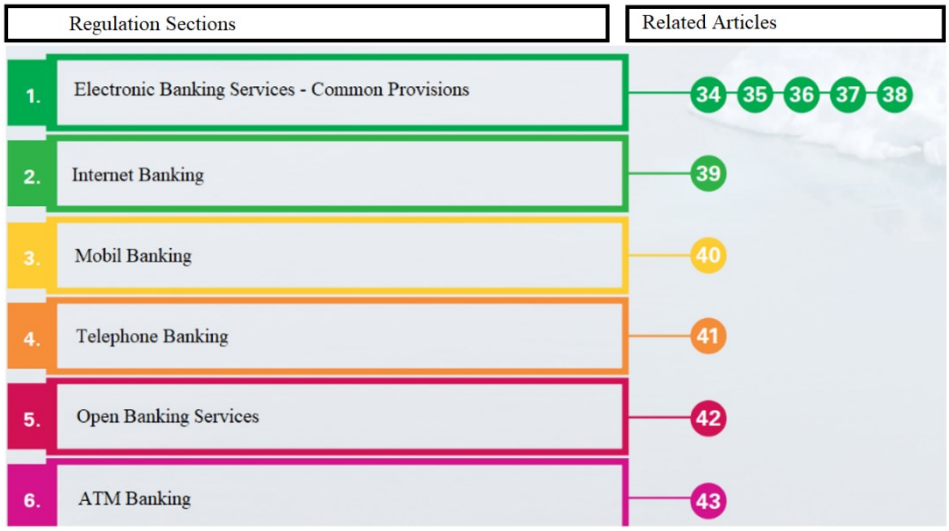


Figure 2.22. Electronic banking services

(**Source**: Translated from; "https://assets.kpmg/content/dam/kpmg/tr/pdf/2020/03/bilgi-sistemleri-elektronik-bankacilik-hizmetleri.pdf", 2021)

Regulation's IS banking services-related articles are mentioned in Table 2.10.

Table 2.10. IS regulation on banking services-related articles

Section No	Section Name	Article No	Article Name
1	Information Systems Governance	4	Management oversight roles and responsibilities
1	Information Systems Governance	5	IS policies, procedures and process documents
2	Managing IS Risk	6	Inventory and classification of information assets
2	Managing IS Risk	7	IS risk management process
3	Information Security Management	8	Information security organization, roles and responsibilities
3	Information Security Management	9	Data privacy
3	Information Security Management	10	Privacy level of data
3	Information Security Management	11	Identity and access management
3	Information Security Management	12	Integrity controls
3	Information Security Management	13	Creation and tracking of audit trails
3	Information Security Management	14	Network security
3	Information Security Management	15	Security configuration management
3	Information Security Management	16	The vulnerability and patch management
3	Information Security Management	17	Physical security controls
3	Information Security Management	18	Cyber incident management, penetration testing and cyber intelligence sharing
3	Information Security Management	19	Increase awareness of information security
4	System Development and Change Management	20	Defining the information architecture
4	System Development and Change Management	21	Project management
4	System Development and Change Management	22	System development, deployment and installation
4	System Development and Change Management	23	Application controls
4	System Development and Change Management	24	Change management
5	IS Continuity and Availability Management	25	Primary and secondary systems
5	IS Continuity and Availability Management	26	IT operations management
5	IS Continuity and Availability Management	27	Accessibility management and backup
5	IS Continuity and Availability Management	28	Ensuring continuity of information systems
6	IS Outsourcing	29	The management of the outsourcing process
7	BS Internal Control and Internal Audit	30	IS internal control activities
7	BS Internal Control and Internal Audit	31	IS internal audit activities
7	BS Internal Control and Internal Audit	32	Ensuring monitoring and assurance of finding
7	BS Internal Control and Internal Audit	33	Personnel training and resource allocation

(Source: "https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm", 2021**)**

- **Electronic Banking Services**

BRSA create and update some compliance rules for alternative channels used in Banks. In "Communiqué on Principles to Be Considered in Information Systems Management in Banks" the regulation BRSA defined master rules but in time they were not updated and increased the number of questions directly asked to the BRSA. This showed that this regulation is not enough to meet Bank's needs. With this regulation, BRSA gives new requirements and answers to the sector. BRSA creates high-level (maybe a starting point) rules of open banking services and also announces in near future they will create more detailed regulations on this subject.

In Table 2.8 these regulations' electronic banking services parts and related articles (Table 2.11. and 2.12) are mentioned.

Table 2.11. Electronic banking services

Electronic Banking Services	Common Provisions
	Internet banking
	Mobile Banking
	Phone Banking
	Open Banking Services
	ATM Banking

Table 2.12. Electronic banking services regulation-related articles

Section No	Section Name	Article No	Article Name
1	Common Provisions	34	Authentication and transaction security
1	Common Provisions	35	Undeniability and assignment of responsibility
1	Common Provisions	36	Monitoring of Transactions
1	Common Provisions	37	Informing customers
2	Internet banking	38	Authentication and transaction security on Internet banking
3	Mobile Banking	39	Mobile banking authentication and transaction security
4	Phone Banking	40	In telephone banking authentication, transaction security and quality of service
5	Open Banking Services	41	Authentication and transaction security in open banking service
6	ATM Banking	42	Authentication and transaction security at ATMs

(Source: "https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm", 2021**)**

2.6. GRC and IT GRC

The GRC stands for “Governance, Risk and Compliance” as an interconnected term that defines various operational practices, from the creation of external and internal audit control practices and continuous inspection procedures to the establishment of positions which obligations of business processes and users of the system, to data analytics procedures. PricewaterhouseCoopers audit and consultancy firm first introduced the term GRC in 2004, which has since been a common term and an effective emerging approach to an organization's business requirements (Gill and Purushottam, 2008). According to the OCEG’s red book, GRC is defined; “a shorthand reference to the collection of critical capabilities that must work together to achieve Principled Performance. GRC denotes governance, risk management, and compliance, but it connotes much more than those three terms simply put together into an acronym” (OCEG, 2019).

GRC is an integrated, holistic and company-wide approach that aims to ensure that companies are ethically correct and in accordance with their risk appetite, internal guidelines and external regulations through the alignment of strategy, acting processes, technology and people and thereby improving (their) efficiency and effectiveness (Racz, Weippl, and Seufert, 2010). It is important that organizations have been governed, and risk and compliance have been managed. GRC is not new and expresses the importance of all related dimensions OCEG evaluates this “...GRC, as we understand it today, totally revolutionary GRC is viewed as a well-coordinated and integrated collection of all of the capabilities necessary to support Principled Performance at every level of the organization. GRC doesn’t burden the business, it supports and improves it” (OCEG, 2019).

In literature, Racz et al. created a frame of reference for integrated GRC. In every aspect of strategy, people, technology and processes are assessed to have an integrated and holistic view to govern and manage risk and compliance, and depicted in Figure 2.23. Other important inputs are internal policies, external regulations and risk appetite. GRC is an organization-wide effort to be successful, every level of the organization should involve in the process to support and engage the desired results. These results are wrapped up as ethically correct behavior, improved efficiency and effectiveness (Racz et al., 2010). In the proposed model, a structure that integrates the 3 fundamental dimensions of the GRC and is organized to cover the entire organization and in which all operations of the enterprise are supported/managed in harmony in line with the GRC system. It is predicted that a business

managed in this way would spread ethical and correct behaviors and produce outputs with increased efficiency and effectiveness/productivity. Ensuring the existence of these basic requirements in the model proposed in the thesis, Racz et al. suggested model is consistent with other GRC frameworks for example Cobit's 40 processes include these for 4 main areas and organize operations, and createf value for businesses. Again, it is seen that OCEG's proposed GRC model covers more than these dimensions. This framework details have given in the following pages.

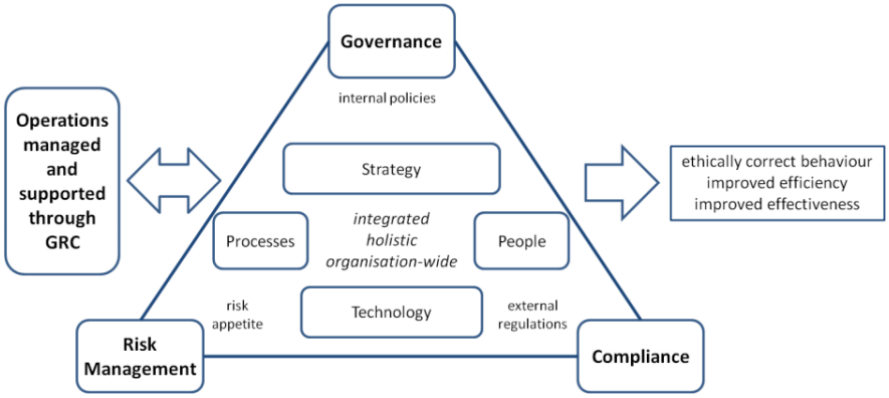


Figure 2.23. Frame of reference for integrated GRC
(**Source**: Racz et al., 2006)

Corporations typically embrace streamlined GRC solutions for their current structures, but some GRC applications take a particular methodology that involves a whole GRC strategy; reorganizing the whole operating process and meeting a positive response of GRC concepts. Many large organizations around the world had been implemented GRC applications, and small or medium-sized enterprises have also recently taken an interest in adopting the streamlined GRC approaches and systems.

While GRC embedded systems have only been possible in recent years, companies have often adopted GRC standards either through manual processes or through the use of non-integrated automated solutions. Despite its relevance for the organizations, however, scholarly work on the integrated GRC program was not conducted (Racz et al., 2010).

A large number of researchers have been studying GRC since then and the increasing number of approaches to integrating the individual disciplines. While various publications on the development and the proposed conceptual frameworks, reference models and architectures about GRC (Tapscott, 2006; Mitchell, 2007; Frigo and Anderson, 2009; Marefika and Nissen, 2009; Paul, 2009; Racz et al., 2010; Vicente and da Silva, 2011; Nits and Marefika, 2014), others focus on the operationalization of GRC-related methods and concepts and their

IT implementation in the operational context (including with GRC software solutions) and the associated implementation processes (Gericke et al., 2009; Racz, Weippl, and Seufert, 2010; Wiesche, Schermann and Krcmar, 2011; Spanaki and Papazafeiropoulou, 2013). GRC conceptual models have been created in the literature, but it has been discussed that the application example in a bank (within the scanned databases; Web of Science, Google Scholar, WISO, EBSCO, ACM, IEEE Xplore, SpringerLink, Emerald) has not yet been created.

GRC supports the same general concept and is broad in nature. It is noteworthy that the edition presented by the Open Compliance and Ethics Group (OCEG), an organization of non-profit representatives of the comprising companies such as the big four audit and consulting firms (KPMG, Ernst & Young, PwC, Deloitte) or Amazon, ISACA have become a significant focal point of analysis and practice in a comparatively short amount of time.

The principles of governance, risk and compliance are interwoven into one perspective, the GRC is related to dimensions such as accountability, ethics, internal control and assurance, which Drori (2006) defined as a "discursive package" in the framework of the broader governance field. Throughout the GRC world, different concepts and logic have become "absorbed" and "infused" throughout these numerous organizational and technical areas, permeating the practice of IT, accounting, compliance, legal and market practitioners. One of the most comprehensive and in operational practices on the most widely used and recognized frameworks for integrated GRC on the work of (Mitchell, 2007) and has since been supported by “Open Compliance and Ethics Group” (OCEG) maintained and developed. The OCEG is a not-for-profit organization that wants to help companies, a so-called Achieving Principled Performance.

OCEG’s GRC business case is mentioned in Figure 2.24. In this figure OCEG depicted the state of lack of GRC and after GRC managed in a business. Without GRC state, a business cannot integrate its processes and this increases the complexity. This unnecessary complexity and lack of integrity are based on uncontrolled domains. This results in wasted resources and wasted information. Lack of governance a corporate cannot manage or govern its most important values like data or information. This creates fragmentation between departments and increases complexity. Duplication of work can occur and also poor integration and lack of visibility can create organizational and functional silos. These silos create duplication and alignment between these silos is hard. In this picture, OCEG metaphor

this situation as slipping through the cracks. A disjointed strategy creates a lack of effective oversight. Unintegrated GRC affects business performance badly. Moreover, according to OCEG in an integrated GRC case corporations create a baseline for common methods, common vocabulary, shared services and shared technology to govern. Integrated and quality information create a visible environment to control. All the participants along with the corporate itself easily align with the business strategy. Integrated departments create higher quality information, process optimization, better capital management and reduced costs. Integrated risk and control activities can create improved effectiveness and protect reputation.

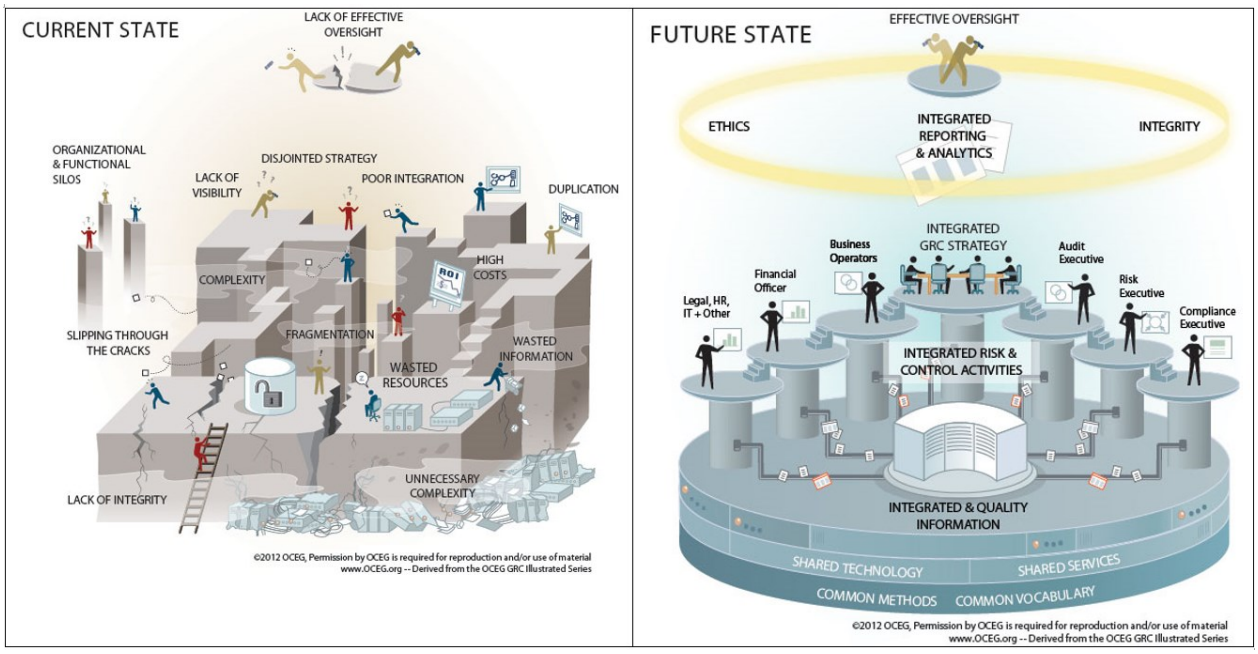


Figure 2.24. The business case for Integrated GRC (**Source:"**https://go.oceg.org/illustration-how-do-we-make-the-business-case-for-integrated-grc-updated", 2021)

OCEG's "universal outcomes of high-performing GRC capabilities that every organization should seek to achieve." is mentioned in Figure 2.25. These 10 outcomes generally repeat in other GRC frameworks.

Figure 2.25. Universal GRC outcomes
(Source: OCEG Redbook 3.0, 2019)

2.6.1. IT GRC

IT GRC is a subdomain of GRC and the relation between GRC and IT GRC is highly important. In a corporation, it would be deficient that IT GRC model creation without a general and organization-wide GRC implementation. Technology firms sometimes use the IT GRC term instead of the common GRC. They are highly related but different. Businesses can create their GRC or IT GRC models integrated together or separated. In Figure 2.26. Racz et al. created a relation diagram between IT and business operations and GRC and IT GRC relations. They all support and align with each other on the basis of strategy, processes, people and technology. These 4 areas are seen in devops management culture. Devops is a cultural philosophy that enables the management of two main areas in IT in harmony. Although these two areas are generally divided into two development and operations, there may be new areas added to them. Security is one of these areas, sometimes it can be seen as cyber security or information security. In addition to the management of 3 main areas of devops culture, people, process and technology, it also deals with issues such as corporate strategy and IT and business alignment (Gill et al., 2018). Although the following areas are explained in detail in the articles written in the field, the concept of people generally refers to all parties working in these fields and producing value in accordance with this culture or benefiting from these products or services. It envisages that all processes related to these parties are managed, supported and developed in accordance with the strategy in harmony with processes and technology. On the other hand, in the process dimension, envisages the management of all IT-related processes of the enterprise with all the relevant "people" who manage them, effectively and appropriately defined processes. In terms of technology, the devops culture envisages evolving from human labor-intensive operations or processes that eliminate all repetitive tasks possible with automation to simpler and faster processes (Macarthy and Bass, 2021). In order to achieve this evolution, concepts such as technology and continuous improvement, continuous development or, with a more technical approach, continuous deployment and continuous integration come to the fore. It aims to achieve strategic goals by managing all these technology tools in harmony with the devops culture (Sen, 2021). Business operations and IT alignment or supports each other in the baseline of a devops culture. IT GRC model based on devops culture creates value for both business and IT together. Racz et. al. suggest these creating the fundamental concept of a harmonic GRC and an IT GRC approach.

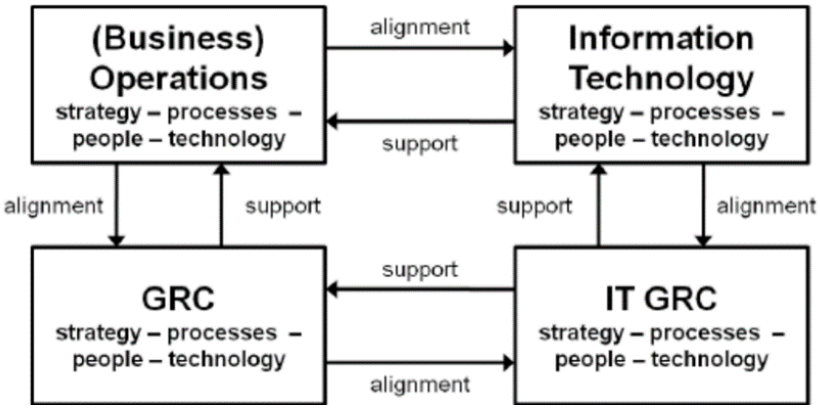


Figure 2.26. "GRC and IT GRC in the business and IT context"

(**Source**: Racz, et al., 2006)

According to Rath and Sponholz, "IT GRC deals primarily with issues of information security, IT compliance, IT and data governance, IT risk management, and IT revision"(Rath and Sponholz, 2009). Business operations and information technology operations and management are based on again these 4 bases. Strategy, people, process, and technology. IT uses technology to create business value. Business uses created technology of IT, to create products or services for their customers. Sometimes IT directly creates products or services for their customer. IT strategic alignment is important with business strategy. Without a clear definition of IT and business strategy, they would not collaborate and support themselves. These alignment of support flows is crucial to continuing success in processes. Business GRC and IT GRC again support and align together. Their basis is the same as operations but different in governing bodies. (Racz et al., 2006)

To enable GRC in business Racz et al. created a process model for IT GRC. It was an analysis of three best practices firstly process models come from ISO/IEC 38500:200, and ISO created this standard for IT Governance and second, the COSO (Committee of Sponsoring Organizations) ERM (Enterprise Risk Management) framework used for risk management processes, finally a generic model for IT Governance stemmed from Cobit EDM "Evaluate Direct and Monitor" domain (Racz, Seufert, and Weippl, 2010). The model is depicted in Figure 2.27.

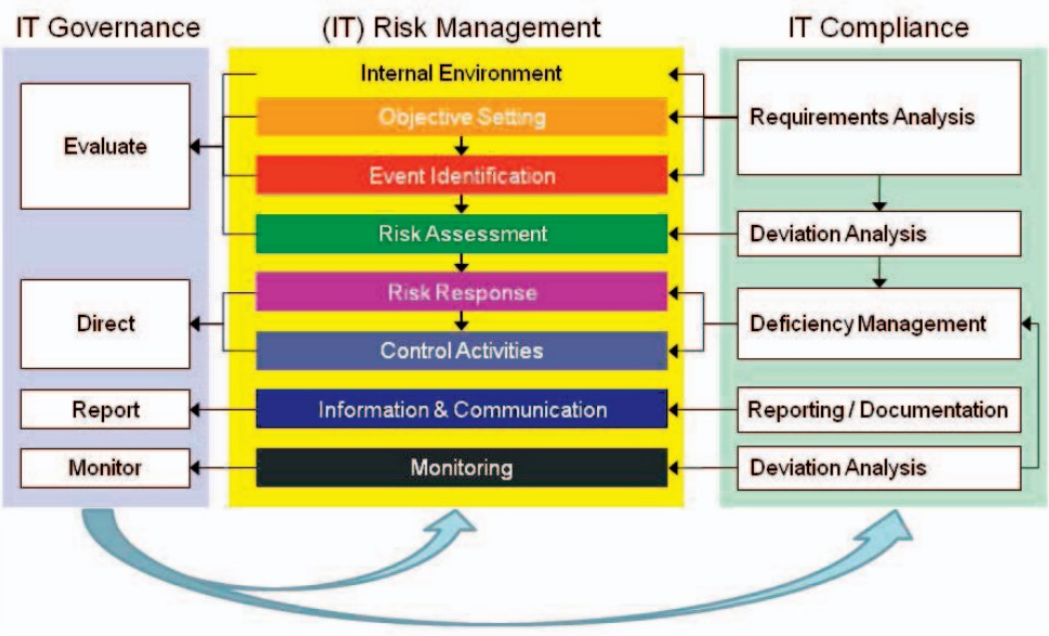


Figure 2.27. Process model for IT GRC

(**Source**: Racz et.al., 2011, COSO, "Enterprise Risk Management - Integrated Framework,", ISO/IEC 38500:2008 - Corporate governance of information technology)

Pedro Vicente and da Silva created a "Business Viewpoint for Integrated IT Governance, Risk and Compliance" model. In this model they evaluated relatedness and all the information flows between related domains. They expanded monitoring processes in all IT governance, risk management and compliance areas. Also, they created a business architecture. Their model is based on "a process model for IT GRC and a conceptual model for GRC, we use ArchiMate to model the behavioral, structural and informational structure of the business viewpoint - business processes, roles and business objects respectively." For example, in the "Evaluate IT Governance" subdomain they define critical business-related policies, risk appetite, culture, strategy and key objectives and relate them to risk management-related subdomains like internal environment. (Vicente and Silva, 2011). In Figure 2.28, their model and information flow are depicted.

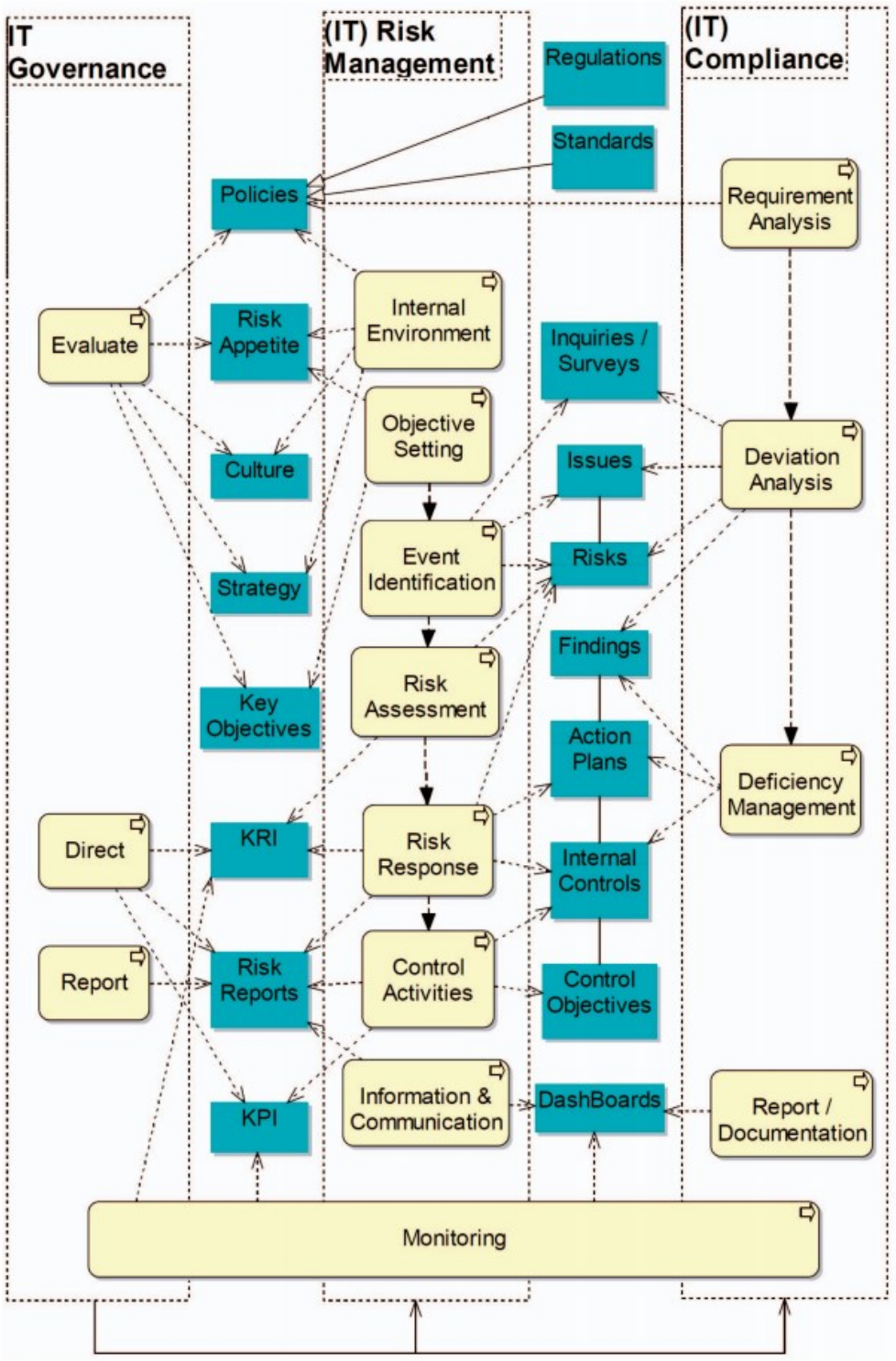


Figure 2.28. Business process model for IT GRC, modeled with ArchiMate (**Source**: Vicente et al., 2011)

In this model IT, governance dimensions are evaluated, directed and reported (in Cobit they are "evaluate, direct and monitor") and they create outputs to IT risk and IT compliance dimensions. Four main areas are defined and the monitoring process includes the whole processes. This model, which is considered to contribute significantly to the determination

of important areas and outputs for GRC on the basis of IT, can be applied to IT organizations of small-sized enterprises. Because in enterprises with large-scale or complex IT organizations, much more diverse and related processes are operated than the outputs specified in the model, and inputs and outputs that establish complex relations with each other can occur.

2.6.2. GRC Frameworks

There are lots of GRC models created by many organizations. International quality and standardization associations or big four audit companies (KPMG, PwC, E&Y and Deloitte) created them. Audit and assurance companies like KPMG, Deloitte, PwC, E&Y are creating their own model to give/sell services on this subject. Their methodology generally uses the same concept but in a different way. Also, nowadays, some big companies like Amazon create and share their GRC model too. In this part of the thesis, GRC frameworks are explained and evaluations are made for each framework.

2.6.2.1. OCEG ("Open Compliance and Ethics Group")

OCEG defined itself as "a nonprofit think tank that invented principled performance and GRC to solve age-old problems" (OCEG, 2019). OCEG framework defines GRC as a "system of people, processes, and technologies that enables a company, among other things, to;

- understand and prioritize stakeholder expectations,
- the business objectives consistent with its values and risks to set up,
- to achieve the goals while optimizing the risk profile and values to protect,
- within legal, contractual, internal, social, and ethical boundaries to work,
- relevant, reliable, and timely to the relevant interest groups to send information
- to make the performance and effectiveness of the system measurable"
  (OCEG, 2019).

"The GRC Capability Model" is an essential part of the framework - also known as the Red Book. It describes central components, elements and practices for the implementation and management of GRC activities.

A GRC activity summarizes all processes and activities that contribute to the system or are part of the system (Figure 2.29.) (OCEG, 2019)

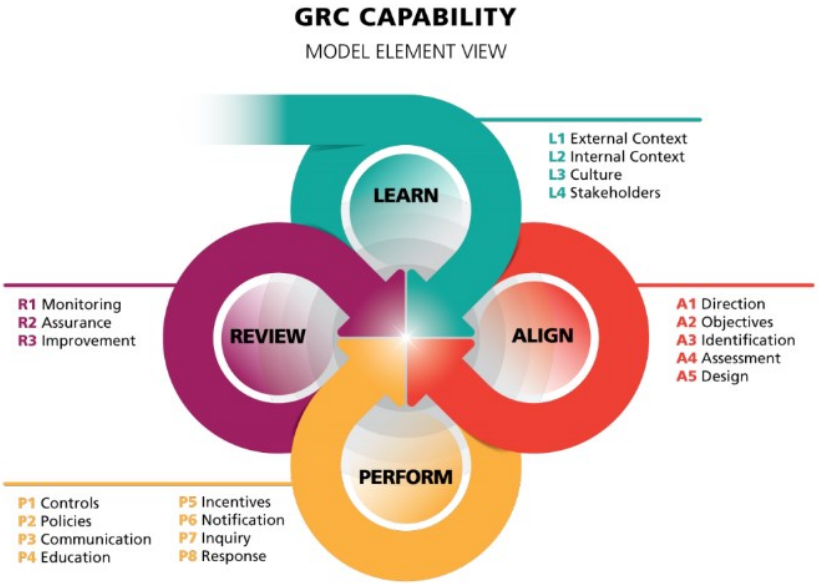


Figure 2.29. OCEG's GRC capability model
(**Source**: GRC Capability Model (Redbook), OCEG)

"The GRC Capability Model" consists of four components (learn, align, perform and review), which, depending on the already existing maturity level, are sequential as well as in any order, in principle, however, should be applied continuously. Each component comprises a number of integrated elements (20 in total) which, in addition to basic principles and critical success factors, use various practices (OCEG, 2020).

In addition, numerous proactive, detective and responsive measures and controls are listed that companies should consider or address when implementing their GRC activities and implement them in a suitable "mix" in order to achieve a principal performance (OCEG, 2019).

In the GRC Capability Model, the OCEG offers additional materials that contain further procedures for assessing the degree of maturity (GRC Assessment Tools - also Burgundy Book) and are intended to help identify technological solutions that support the individual elements of the GRC Capability Model are suitable and could be used "GRC Technology Solutions Guide" (OCEG, 2019).

2.6.2.1.1. Learn

In this domain, OCEG mentioned the aim as “Examine and analyze context, culture, and stakeholders to learn what the organization needs to know to establish and support objectives and strategies” (OCEG) these domains are consist of 4 subdomains as external context, internal context, culture and stakeholders. Learn domain details given in Figure 2.30.

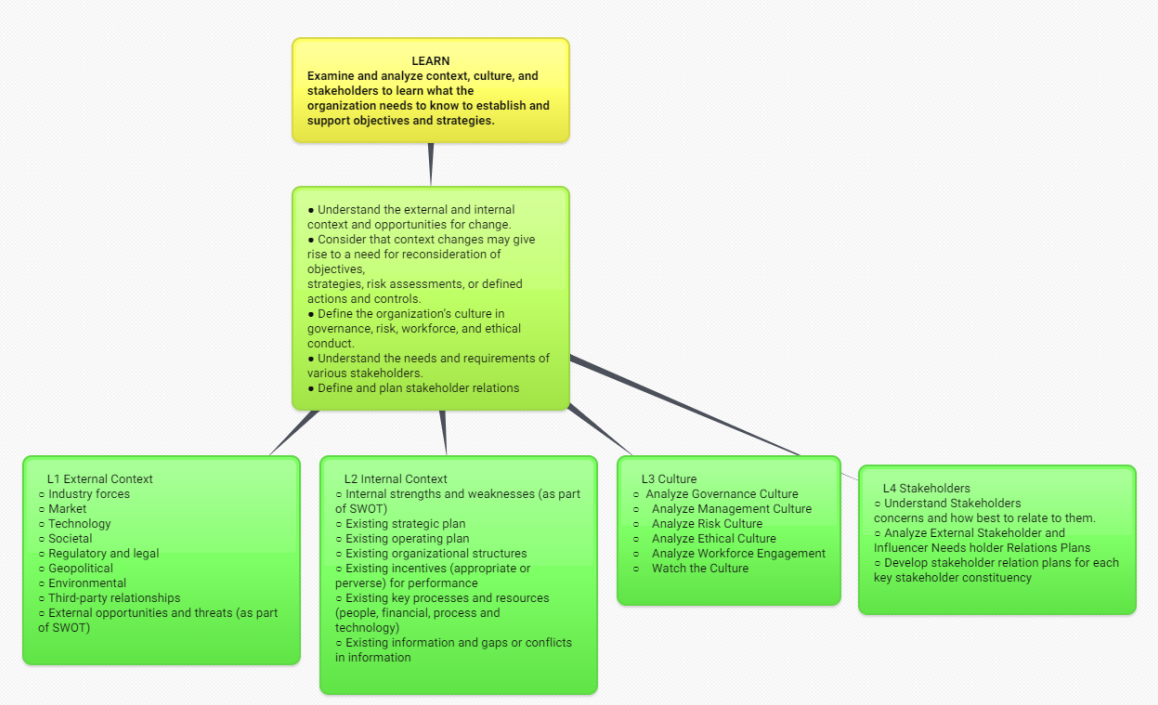


Figure 2.30. OCEG capability model “learn” domain details
(**Source**: OCEG GRC Capability Model, 2019)

External context comes from outside of corporate, industry standards or market, technology is a sample of these forces. Business GRC is affected by these types of factors.

Internal context stems from the business itself for example existing strategic plan, operating plan, organizational structure, or all the business processes and policies.

Another subdomain is culture, business culture affects governance and GRC itself. Governance and Management culture give the clue of tone at the top. Organizations get an ethical example of top tiers.

Analyzing risk and ethical culture affects the workforce’s decision-making techniques and processes are the way stakeholders choose the work done (in an ethical way or not). Stakeholder involvement and understanding are important too. External stakeholders and related parties are important to influence organizational GRC processes. A stakeholder relation plan is another important input to creating a successful GRC in a business.

2.6.2.1.2. Align

In this domain, OCEG mentioned the aim as "Align performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements." Align domain details are given in Figure 2.31. it consists of 5 subdomains, to align business strategy, performance, risk, and compliance objectives between all related parties.

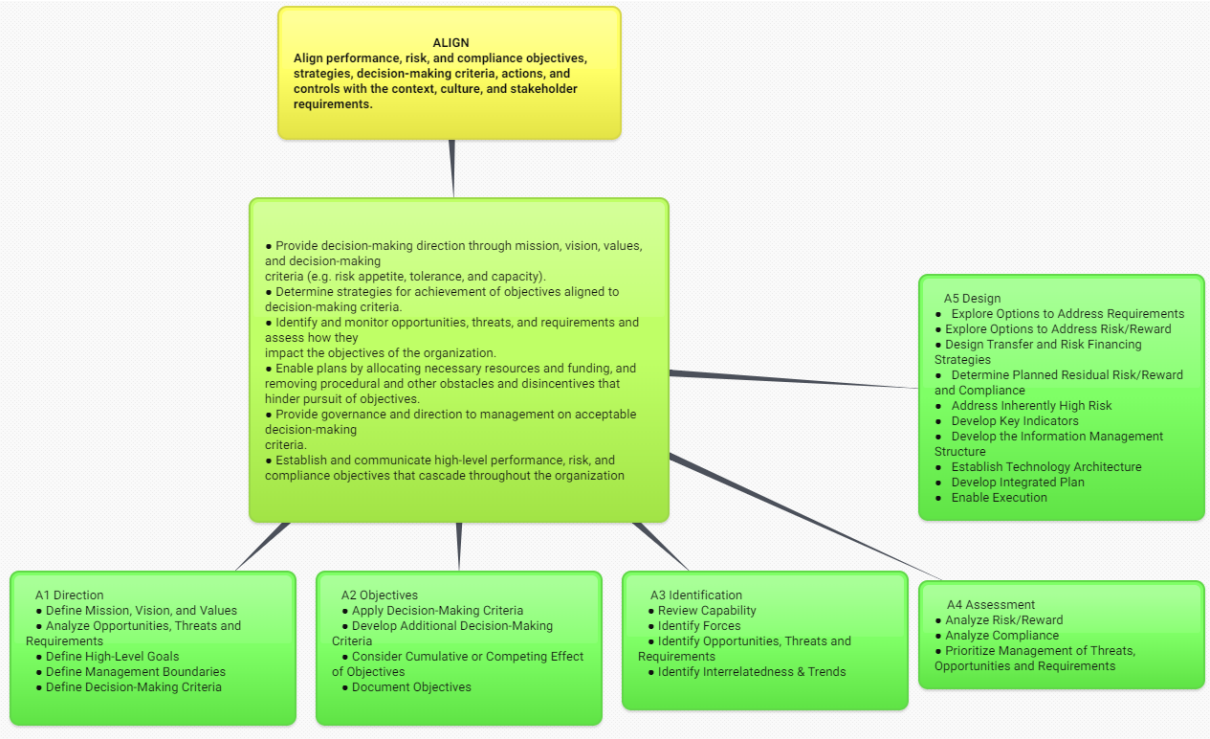


Figure 2.31. OCEG capability model "align" domain details
(**Source**: OCEG GRC Capability Model, 2019)

Management needs to create direction for the organization, they need to create a vision, mission and values. This continues with high-level goals and other SWOT (strength, weakness, opportunity, and threat) dimensions. To align the business to its vision and goals, GRC again creates the objectives and decision-making criteria. Identifying all the related opportunities or threats is again an important part of implementing a successful GRC management. Continuous assessment and as a result of a redesign in a life cycle to get better risk management.

2.6.2.1.3. Perform

In this domain, OCEG mentioned the aim as "address threats, opportunities, and requirements by encouraging desired conduct and events, and preventing what is undesired, through the application of proactive, detective, and responsive actions and controls." Perform domain has 8 sub-domains related to addressing all related GRC activities depicted in Figure 2.32.

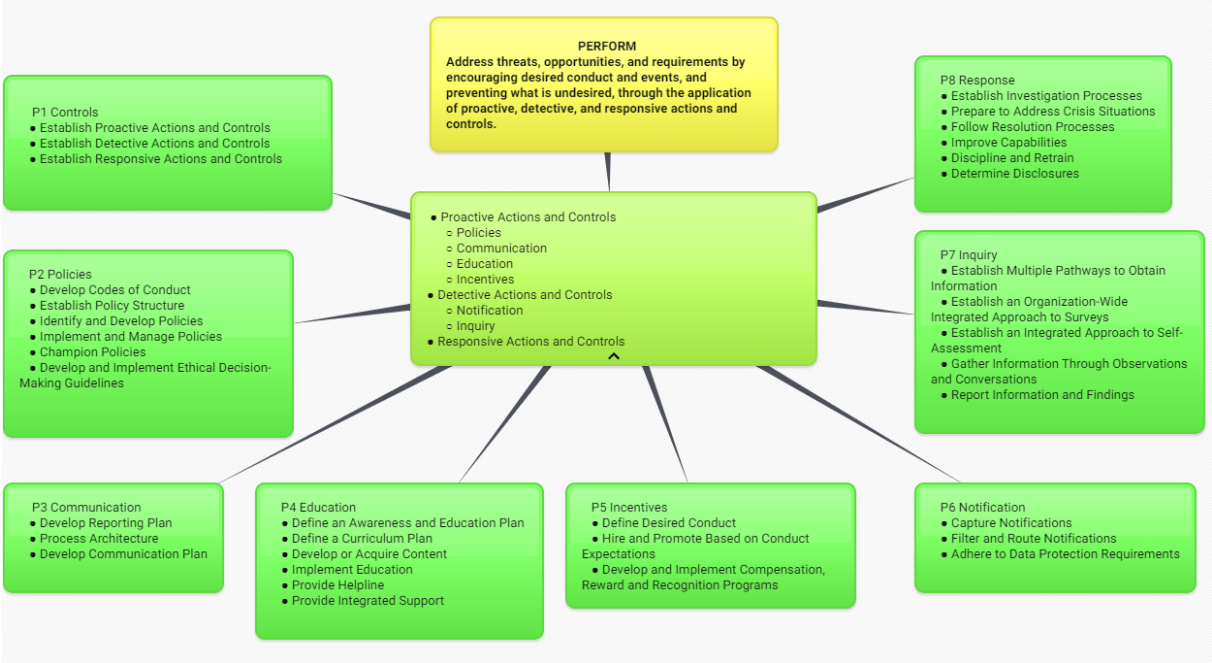


Figure 2.32. OCEG capability model "perform" domain details
(**Source**: OCEG GRC Capability Model, 2019)

Creating a mature GRC needs to perform in diverse areas. Creating proactive/detective controls, effective policies to code of conduct or a communication plan to process architecture is important. Defining education plans to involve stakeholders helps integrated support. Incentives are needed to develop compensated controls, creating a GRC is a long journey and sometimes delivers notification, GRC teams need to filter and route required information and adhere to data protection requirements.

Information gathering techniques are important to establish an organization-wide integrated approach. Getting all quality and required information management and related mechanisms need to respond in an instant time, to improve capabilities.

2.6.2.1.4. Review

In this domain, OCEG mentioned the aim as "Conduct activities to monitor and improve the design and operating effectiveness of all actions and controls, including their continued alignment to objectives and strategies." OCEG review continuously GRC activities to get mature processes. Monitoring and continuous evaluation create a better performance to govern risk and compliance requirements. Process details are depicted in Figure 2.33.

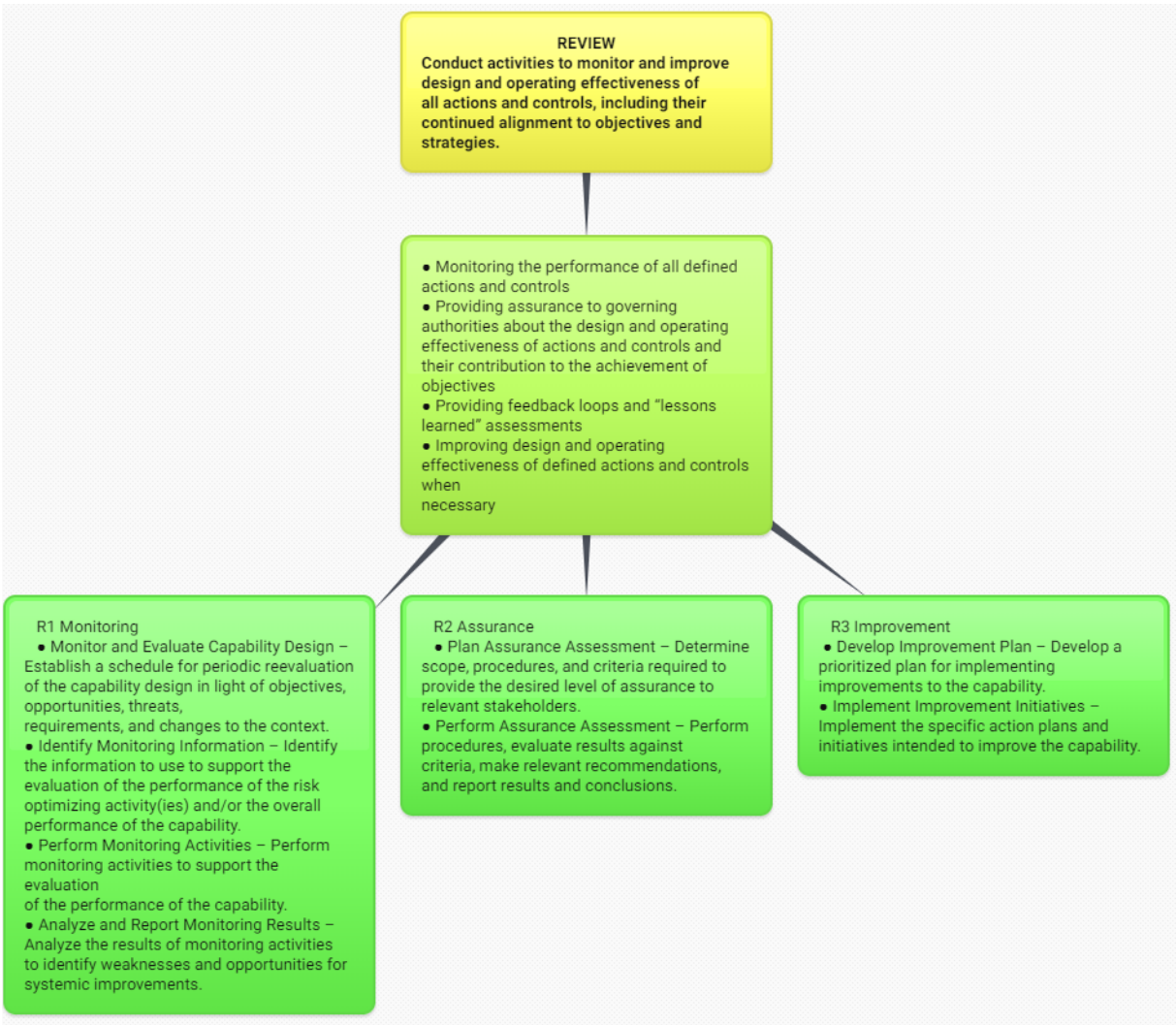


Figure 2.33. OCEG capability model "review" domain details
(**Source**: OCEG GRC Capability Model, 2019)

Monitoring, assurance and continuous improvement are essentially important to implement GRC on business processes. Analyzing and reporting all the related monitoring activities and assuring governing body about conclusions creates the result of improvement.

Resources and tools, guidance, GRC solutions council, executive support and solutions, assessment, measurements and benchmarks are mentioned to design GRC on a corporate. OCEG designed professional certifications to educate GRC stakeholders, especially

governing council need to gain information about how to implement this framework. Although, the famous red book has enough information to implement in which domain, it is recommended to be a member of the council and get all resources and related certifications to implement it better.

OCEG's GRC model is evaluated as a comprehensive approach that relates to the corporate governance principles. To govern the business requires high-level oversight of the enterprise management. Its IT relation mentioned on previous pages.

2.6.2.2. OCEG IT GRC

OCEG created an IT roadmap for IT GRC model creation. OCEG mentioned in this roadmap IT project, priorities and processes are driven by GRC. IT strategies architecture and applications are considered as an integrated part of GRC. The fragmented situation of IT, may be harmful for the organization. IT strategy is defined by business strategy but it is mutually empowering each other. IT can easily create silos and these increase the IT costs fast. Efficiency and effective use of all IT resources are crucial so, effective oversight is essential.

OCEG offers 4 steps to implement IT GRC aligned with the common GRC. It starts with the definition of IT principles and strategy. Related IT professionals come together to assess their needs like information, process/transaction, control/monitoring, documentation and system of record needs. CIO, governing body, risk officers, audit executives, labor lawyers and other IT participants define IT and business integration of corporate strategy. The second step is to define the as-is situation. OCEG defines all existing processes and their maturity level to define gaps between the to-be vision. To vision leverage existing technology investments, they look for areas to consolidate technology to serve multiple GRC areas. Technology integration into core business gains business to meet GRC needs. The fourth step is to define priorities, projects, budgets and ownership. GRC process continues with the definition of all related processes ownership. The priorities and most relevant projects start with the sponsorship of executive-level management teams. OCEG recommends starting in a specific area and, avoiding big-bang solutions. It takes time to be mature, it is an evolving process.

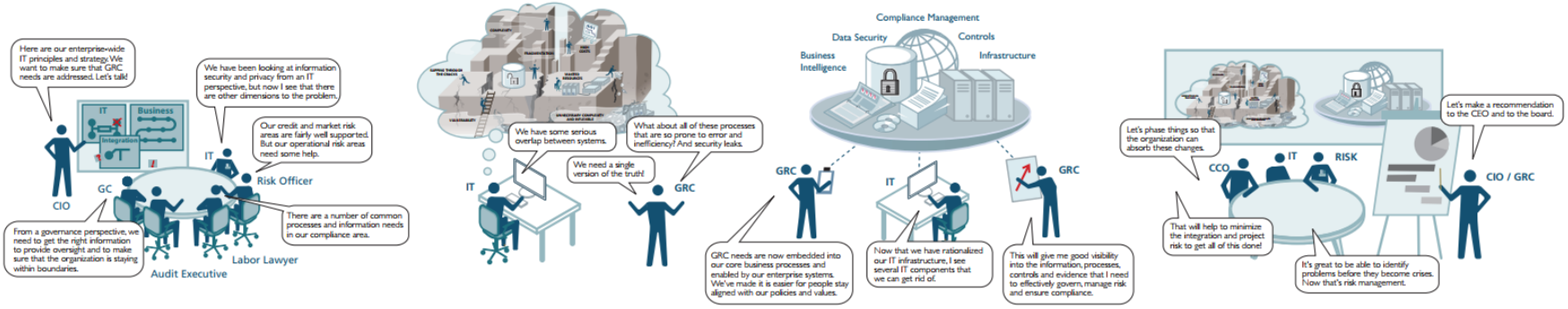
OCEG also offers a maturity model, it has 5 levels. After implementing an IT GRC model GRC stakeholders can assess themselves with this simple method. Defined "Learn", "Align", "Perform" and "Review" stages again can be usable in the process. The whole process and maturity model is depicted in Figure 2.34.

IT Roadmap for GRC

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM SAP

Information technology projects, priorities and processes are being increasingly driven by governance, risk management, and compliance (GRC) considerations. But there is a great deal of confusion and uncertainty about how to proceed. The reason: IT strategies, architecture decisions and applications have not approached GRC considerations in a comprehensive and integrated manner. Companies have typically dealt with GRC needs in fragmented fashion. Moreover, there has been limited attention to automating controls and enabling the information requirements necessary to improve the efficiency and effectiveness of GRC processes and programs. Whether you are considering the GRC impacts on how you manage IT, or wondering how IT can make GRC better, it is necessary to begin with a well established framework. Follow this roadmap to start the journey to align you IT assets with your GRC.



IT Principles & Strategy

Get GRC practitioners at the table with IT professionals to discuss how IT can support GRC needs:

- Information needs
- Process / transaction needs
- Control / monitoring needs
- Documentation / system of record needs

"As-Is" Situation

inventory all of the existing processes and the technology that supports these processes:

- What do we already have in place?
- Who owns and maintains these systems?
- Who operates them?
- What do they really do?

"To-Be" Vision

Define, enhance, evolve an enterprise architecture that supports GRC needs. Leverage existing technology investments where possible and look for ways to consolidate technology to serve multiple GRC areas. Integrate technology into core business processes to serve GRC needs.

Priorities, Projects, Budgets & Ownership

GRC and IT professionals work together to define priorities and specific projects to phase into the ultimate vision.

- Try to start in a specific area and expand
- Try to avoid "big bang" solutions
- Consider parallel operation of "high stakes" systems
- Involve business leaders in prioritization
- Assign ownership and accountability

GRC / IT Maturity Model

1 Unaware

Businesses at this stage do not understand the interdependencies of governance, risk and compliance and few if any IT resources are allocated to GRC.

- Ad hoc approach to technology
- Little if any technology in place
- Information is not available let alone shared
- New requirements are not easily addressed
- Success is not measured

2 Fragmented

Businesses at this stage see some of the interdependencies between governance, risk and compliance, but do not provide a common platform for GRC.

- Tactical, siloed approach to technology
- Silos have systems in place w/o integration
- Information is not shared between silos
- New requirements within a silo are addressed without considering other areas
- Measurement is difficult

3 Integrated

Businesses at this stage see the need to integrate GRC systems to provide better information and results. A common GRC platform and approach is in place.

- Unified approach to GRC
- Silos are broken down
- Information is shared across the enterprise
- New requirements are rapidly addressed by a common platform
- GRC benefits are measured

4 Aligned

Businesses at this level align and leverage the GRC platform to realize not only GRC benefits, but also general business benefits such as growth, profitability and asset utilization.

- Strategic approach to aligning GRC with the overall business
- Silos are nonexistent
- Technology is consolidated wherever possible
- Business benefits are measured

5 Optimized Platform

Businesses at this level use a common language and set of metrics to continuously improve the platform year over year.

- Strategic approach to optimize the GRC platform
- GRC technology and non-GRC technology are almost indistinguishable
- GRC is "baked into" all business systems
- Business benefits are measured and improved year over year

Figure 2.34. OCEG's IT Roadmap for GRC
(**Source**: "https://go.oceg.org/illustration-what-is-the-it-roadmap-for-grc", 2021)

OCEG IT GRC road map could not be considered as a model that can be handled alone and used to create an IT GRC model. It can be considered as a branch of the main tree that enables businesses that will establish a system on the basis of GRC to include the IT field in the process. The model introduced as the IT maturity model is similar to other frameworks, but the main framework documents do not include details on metrics and basic metrics. It has been rated as highly usable for businesses that will initiate a comprehensive GRC program with the participation of all stakeholders from the start. Compared to other GRC frameworks in the field, it is a rare framework whose documentation is open source and whose content can be evaluated. It is a good practice of increasing international recognition that has also provided certification programs for practitioners and supervisors to ensure specialization in this field. Specific to IT GRC, it has been evaluated that an IT organization does not have the foundations to establish an IT GRC model by considering it alone, besides, it can enable to produce of a model by considering all basic GRC processes for IT.

2.6.2.3. Amazon GRC Model

Amazon is a big tech company that defined itself as "Earth's most customer-centric company. Amazon is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Fire tablets, Fire TV, Amazon Echo, and Alexa are some of the products and services pioneered by Amazon." (Amazon Who We Are, 2017). Amazon created a GRC model focused on its cloud business area. It has 3 dimensions; its framework's biggest picture is depicted in Figure 2.35.

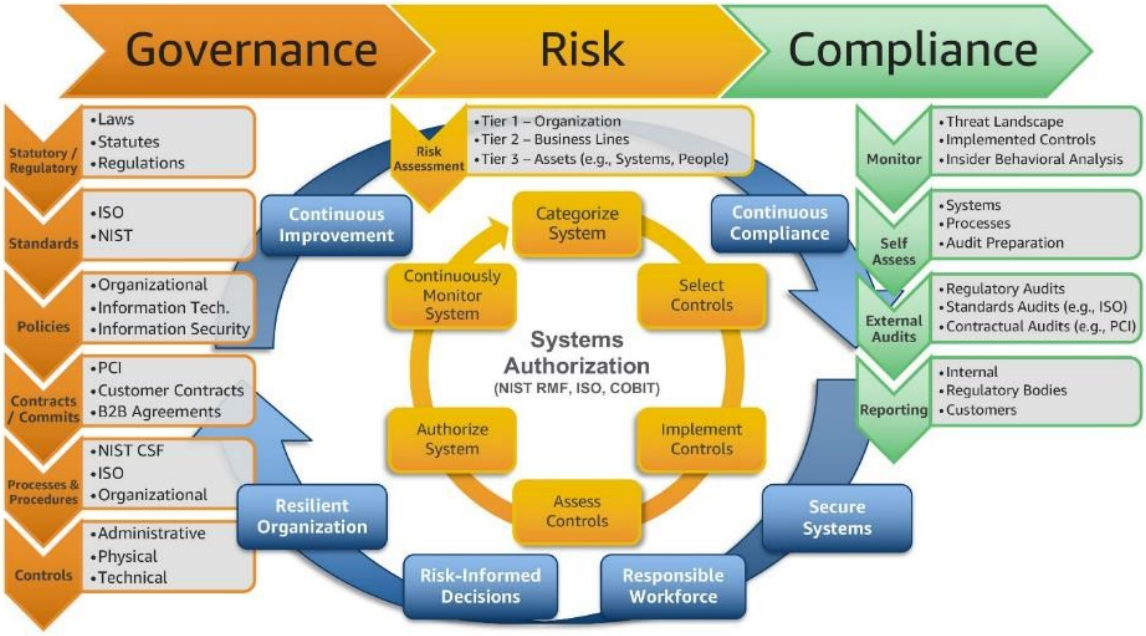


Figure 2.35. "Scaling a governance, risk, and compliance program"
(**Source**: Amazon Web Services, 2018)

In Amazon's model governance is defined firstly with the importance of compliance requirements, then continues with an assessment program to evolve the maturity level. Finally, it recommends that updating and publishing the policies, processes, and procedures—the model's governance detail given in Figure 2.36.

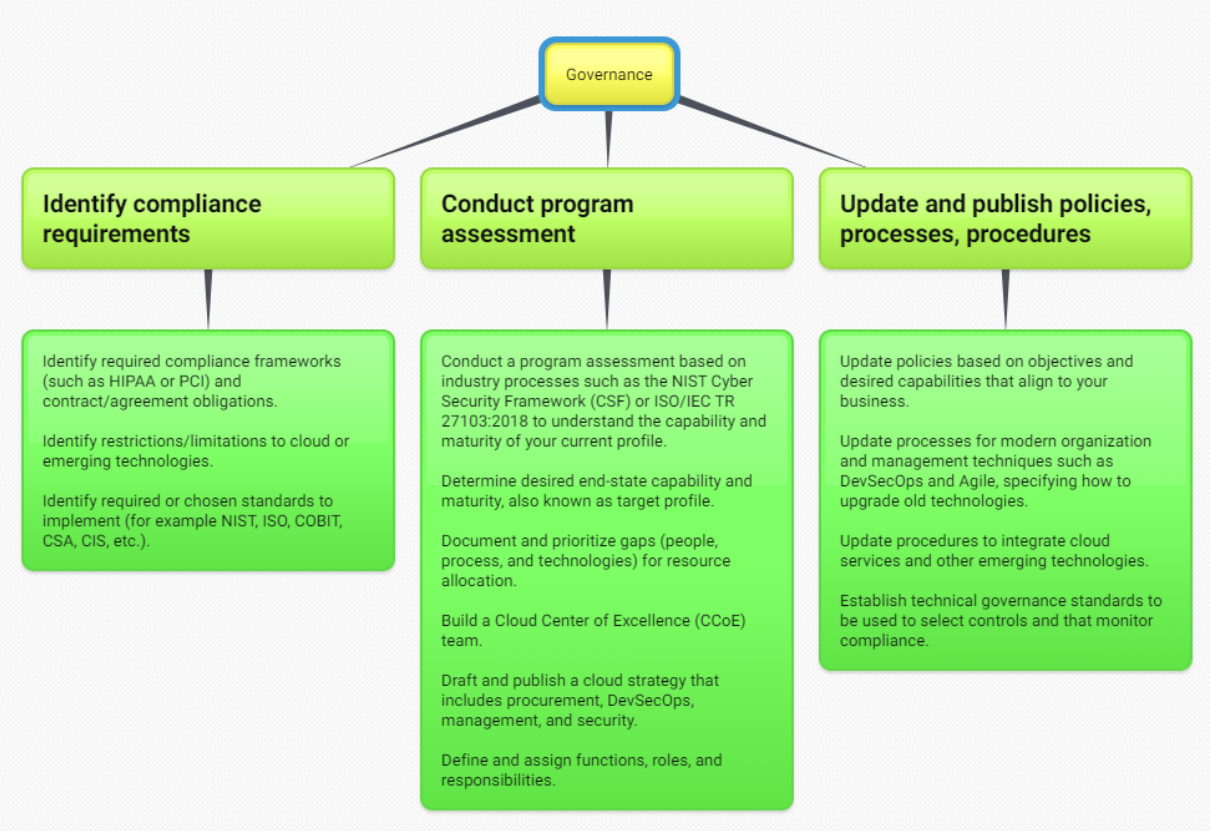


Figure 2.36. Amazon's GRC model "governance" domain
(**Source**: Amazon Web Services, 2018)

In the risk management dimension (depicted in Figure 2.37) Amazon creates a simple approach, which reminds the Project Management Institute risk management process. Firstly, conduct a risk assessment and create a draft risk plan. Then creating response plans for them with incorporating and authorizing all related systems and stakeholders.

Figure 2.37. Amazon's GRC model "risk management" domain
(**Source**: Amazon Web Services, 2018)

In compliance with dimensions Amazon recommends monitoring compliance chances and continually self-assessing to comply with all the improvements on them. Responding to internal and external changes to manage risk is important. Communication inside and outside corporate to report related events and changes in risk levels should be continuous.

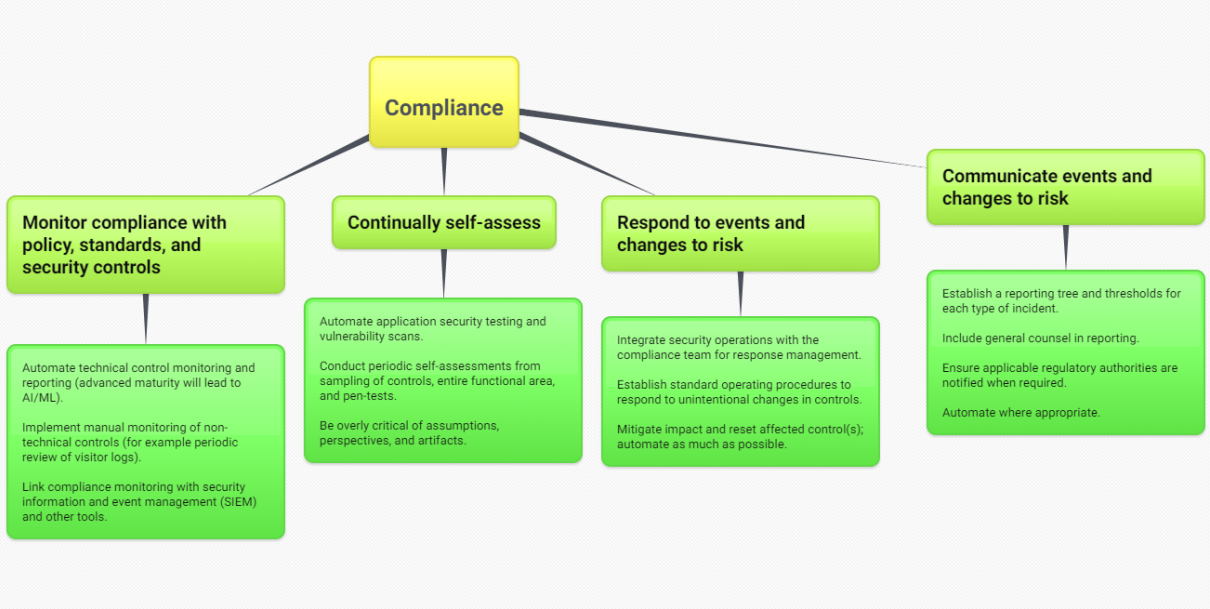


Figure 2.38. Amazon's GRC model "compliance" domain
(**Source**: Amazon Web Services, 2018)

In Figure 2.38., every aspect of GRC and its ecosystem can be seen. In USA ISO, NIST, HIPAA ("Health Insurance Portability and Accountability Act"), PCI-DSS, or any other regulators create their compliance requirements. IT relation is high in this GRC model. Amazon focused on cloud service and gives examples of cloud service. Mark Schwartz who is an Enterprise Strategist at Amazon Web Services defined two types of governance. The first type is "The first type of governance is used when there's a universal control we want to apply. For example, there are the processes that we set up to meet compliance frameworks like SOX, HIPAA, GDPR (General Data Protection Regulation-EU GDPR), and so on, or to get a clean audit at the end of the year." Which comes from the regulator. "There are controls for approving expenditures, for HR, for information security. In IT, we often create enterprise architecture standards, such as which programming languages and platforms to use, how to tag cloud resources, or how we'll implement authentication and authorization. The standards become rules that are enforced through mechanisms and processes, like architectural or peer code reviews. This type of governance is about rules and their enforcement; they must be applied rigorously and auditable. In the strictest sense of the

word, they are bureaucracy." ("Governance in the Cloud and in the Digital Age: Part One | Amazon Web Services," 2020)

IT creates its procedures and control environment but it is important to gain a conceptual framework for the enterprise-wide understanding of all defined controls and related policies. Amazon's GRC model is the first in its area created by a specific company.

2.6.2.4. KPMG's GRC TOM; A pragmatic and holistic approach

KPMG is a consultancy and audit firm widely working in lots of countries. KPMG creates and sells GRC services to businesses. KPMG defines its GRC model as the "Integrated Governance, Risk and Compliance Target Operating Model (TOM)". This model consists of 8 dimensions. In Figure 2.39. main dimensions mentioned. (KPMG, Elst, et al.., 2019)

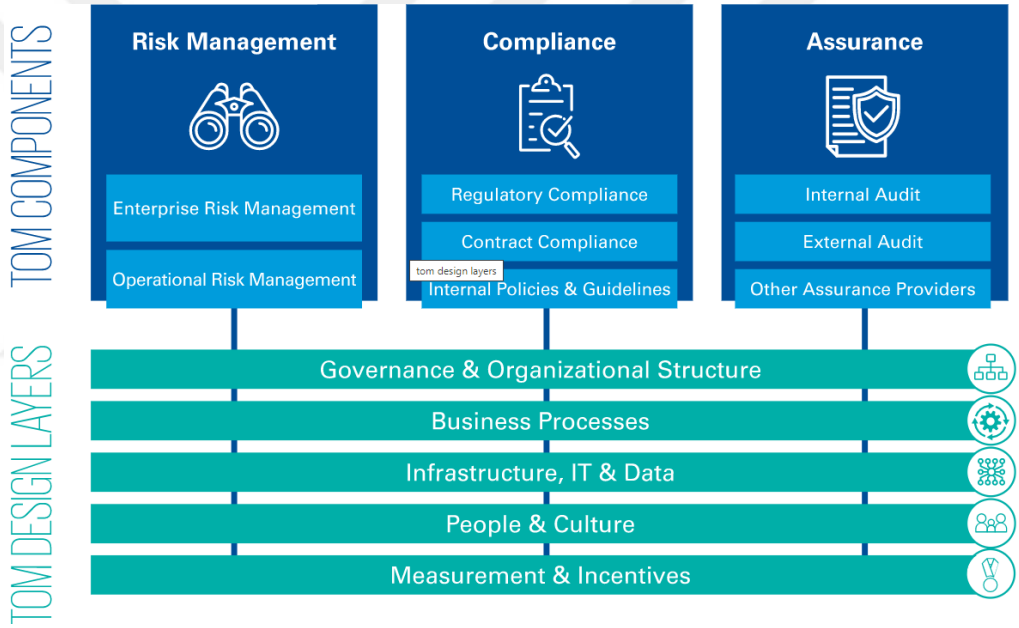


Figure 2.39. KPMG's integrated governance, risk, and compliance target operating model (TOM)
(**Source**: KPMG GRC Services, 2019)

To implement the model KPMG advises following these 8 steps. Explanations of all steps are mentioned below, the continuous lifecycle is depicted in Figure 2.40. master view and step details. To implement TOM model in a corporation KPMG gives consultancy. Their model is not clear enough to implement by a company itself. The main considerations about their GRC implementation method could be understood, but in detail, there are only several documents to create a TOM-based GRC model. Before the TOM model KPMG created the GRC operation model and Enterprise GRC Model it has more details in some documents. Detail about this model was given too.

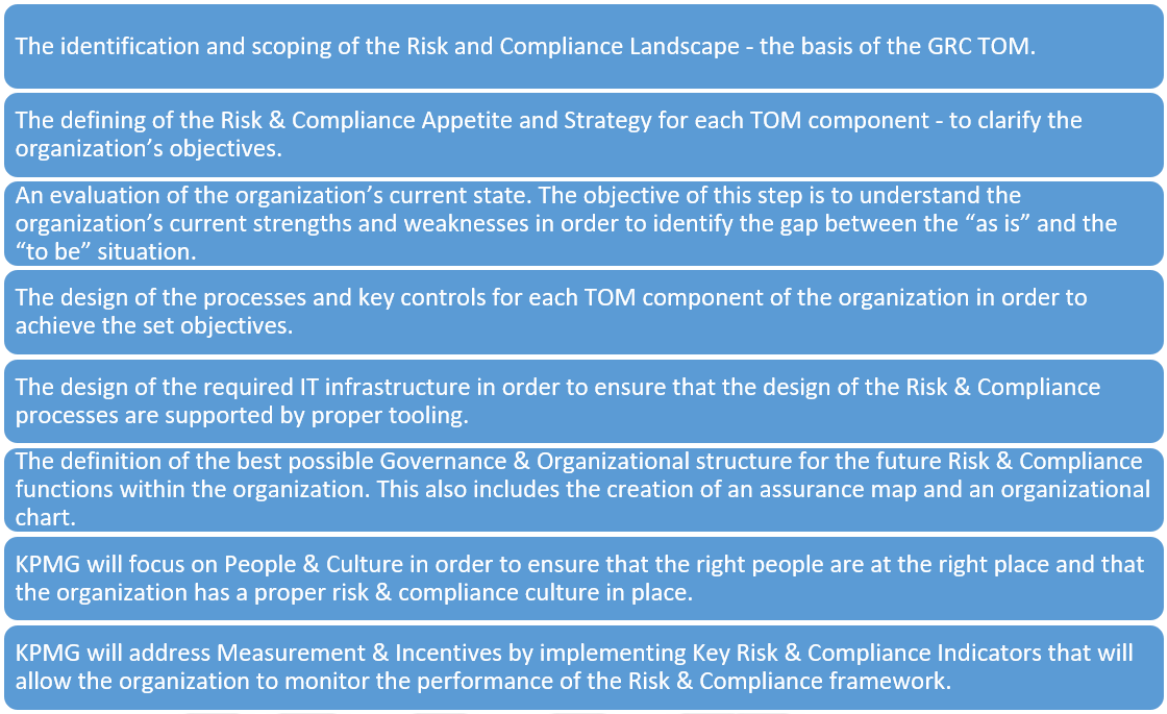


Figure 2.40. KPMG's 8 steps and their details for the continuous GRC (**Source**: KPMG GRC Services, 2019)

KPMG firstly focuses on the compliance requirement and the risk appetite of related corporations. After definition, they assess the strategy to assess as-is and to-be. After evaluating the current state. The process continues with the design step. GRC model creation needs to be unique and tailored for every organization. Because it depends on internal and external factors. As in the seventh step people and technology changing in every sector. The final step is about continuous improvement. Measurement and incentives are continually assessed and process maturity is trying to be better. ("Integrated GRC Target Operating Model," 2020)

KPMG also creates a GRC operational model which consists of 6 main areas depicted in Figure 2.41, it is older than mentioned TOM model but has a similar domain to the OCEG and Amazon's GRC models/frameworks.

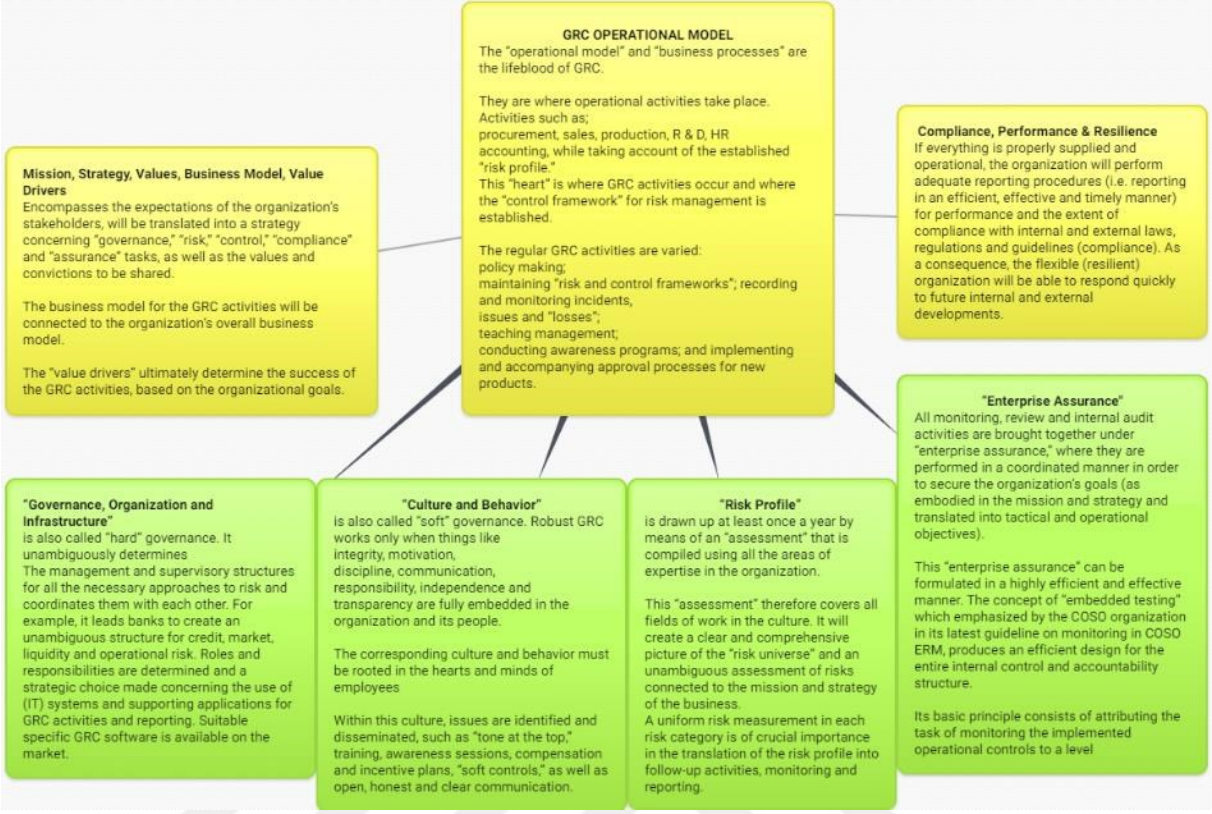


Figure 2.41. KPMG GRC operational model domains.

(Source: "https://assets.kpmg/content/dam/kpmg/us/pdf/metricstream-better-together.pdf", 2021)

KPMG evolved its model to an enterprise-wide integrated operating model, essentially general GRC models insist on governance methods, not on operation ones. Although it is called an operation, the most important areas are again related to the governing body and its requirements. They created an implementation guide for their model, but its ingredient is not enough to implement the business itself. They are selling consultancy services to implement this model in corporations.

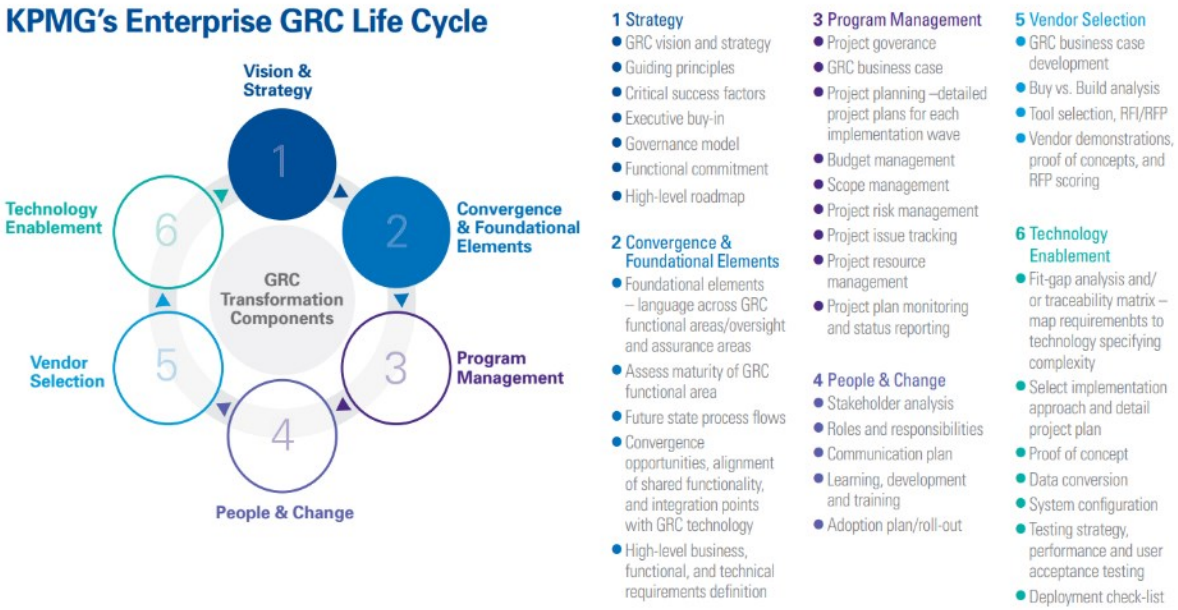


Figure 2.42. KPMG's enterprise GRC lifecycle

(Source: "https://assets.kpmg/content/dam/kpmg/us/pdf/metricstream-better-together.pdf", 2021)

In KPMG's enterprise GRC lifecycle technology enablement is the sixth step in creating a successful GRC on a business depicted in 2.42. It has 7 goals like fit or gap analysis/ traceability matrices to map requirements, implementation approach selection, and proof of concept on the system and data-related issues. Their GRC strategy generally works on a software-assisted process. So, after creating a GRC program that is fixed with the companies' vision and strategy, it continues with suitable GRC vendor selection to make business case development, and buy versus build analysis to gain a GRC application.

An example of the components of KPMG's GRC scan is depicted in Figure 2.43. All dimensions of internal control levels and current and target statuses are defined. ("Successful Governance, Risk and Compliance within reach - Compact", 2018)

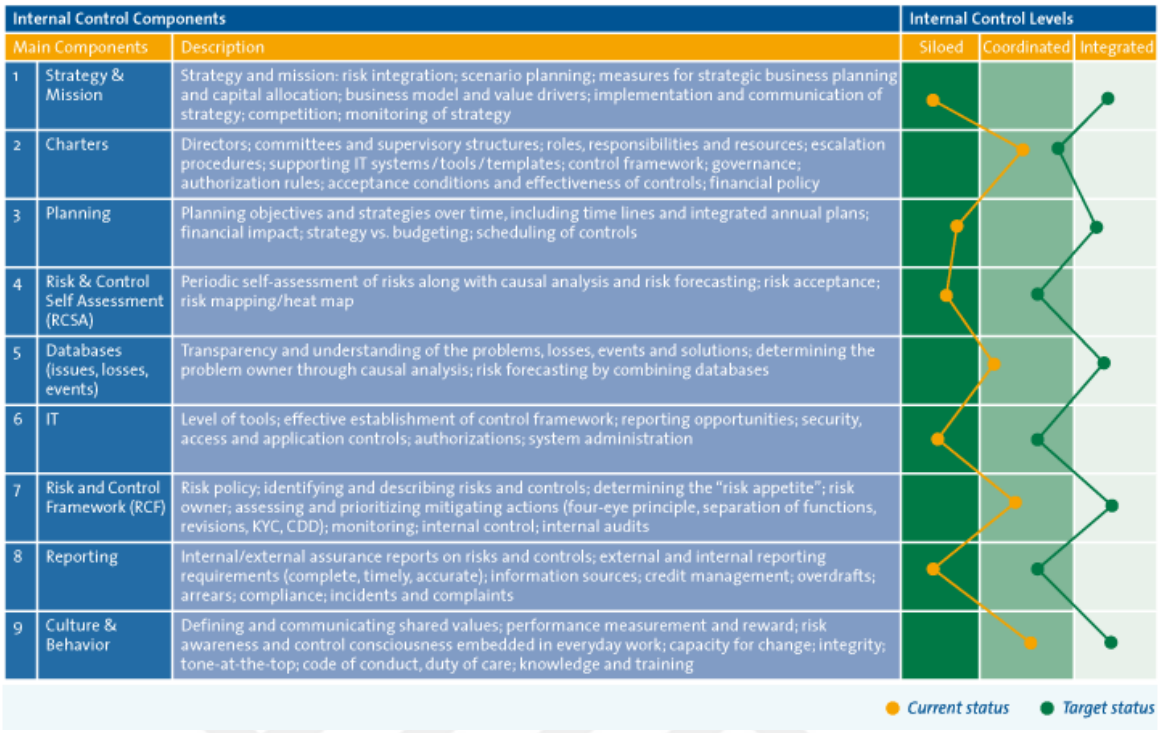


Figure 2.43. KPMG's GRC scan (gap analysis sample)
(**Source**: "https://www.compact.nl/articles/successful-governance-risk-and-compliance-within-reach/", 2021)

KPMG also creates a "Technology Assessment Diagnostic Model" to help businesses launch or refresh their GRC technology initiatives. Their method has 6 steps, again it starts with an assessment and a gap analysis and continues with implementation and continual improvement. The model is depicted in Figure 2.44.

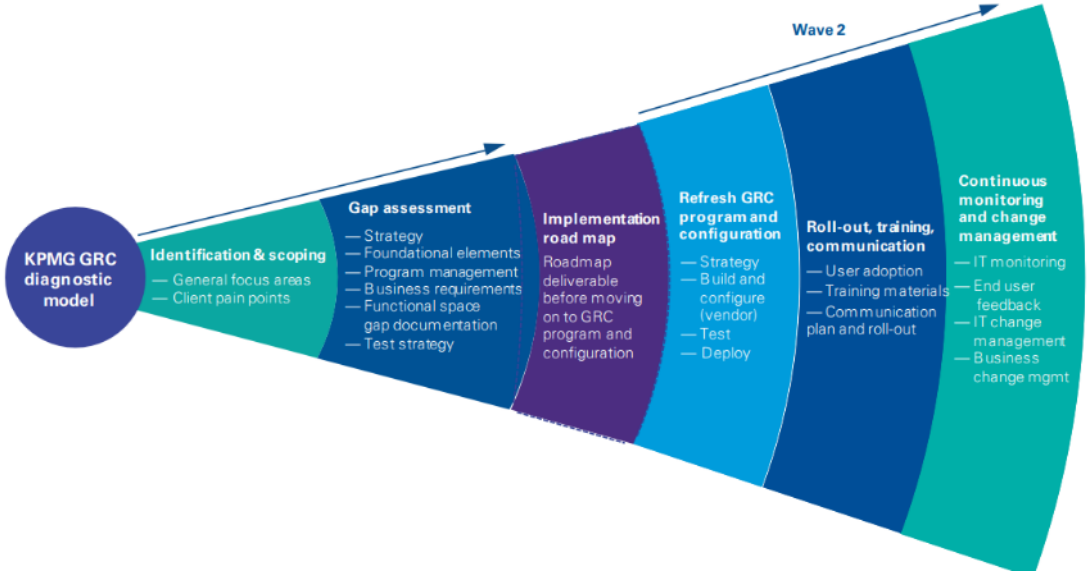


Figure 2.44. KPMG's technology assessment diagnostic model
(**Source**: "https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/07/implement-grc-technology-the-right-way.pdf", 2021)

2.6.2.5. PwC- GRC Enablement Model

PricewaterhouseCoopers is a consultancy and audit firm and defined its aim as "help organizations and individuals create the value they are looking for, by delivering quality in Assurance, Tax, and Advisory services" (PricewaterhouseCoopers, 2011)

GRC is "a coordinated effort to ensure communication and collaboration between different stakeholders in the management of risk and control of the organization." (PwC, 2019) PwC creates a model to enable GRC management based on 3 main areas corporate governance, risk management, and compliance management.

The process starts with understanding the business. GRC enablement models create GRC process automation and integration roadmap, tool evaluation or design/develop or acquire. The process is depicted in Figure 2.45.

Figure 2.45. PwC's GRC enablement model and processes (**Source**: "https://www.pwc.com/sg/en/risk-assurance/assets/grc-enablement-solution-2019.pdf", 2021)

PwC defines its GRC model's final aims as sustainable business performance. PwC uses its GRC models to consult businesses to create a GRC program. Their final recommendation contains to buy an application to use enterprise-wide. PwC generally advises using RSA Archer. GRC is not only about using an application its most important domain is governing body's effectiveness. Executive managers gain information about all risk-related and compliance-required issues and take them into account. PwC states this as behavioral insight and optimizing culture. PwC GRC management methodology is mentioned in Figure 2.46.

Figure 2.46. PwC, GRC management methodology

(**Source**: PricewaterhouseCoopers, 2019)

With the help of these 7 steps and GRC tools or mechanisms, the business enables GRC to gain business to sustainable performance. PwC defines IT GRC in these principles. IT organization, job description, skills, and competencies-based processes and procedures create an interface with operational IT. IT governance framework uses IT governance structures, processes, policies and standards to create decision models, and important key IT decisions with the enablement of communication, and change management, technology, performance management and benefits tracking. IT GRC implementation method is depicted in Figure 2.47.

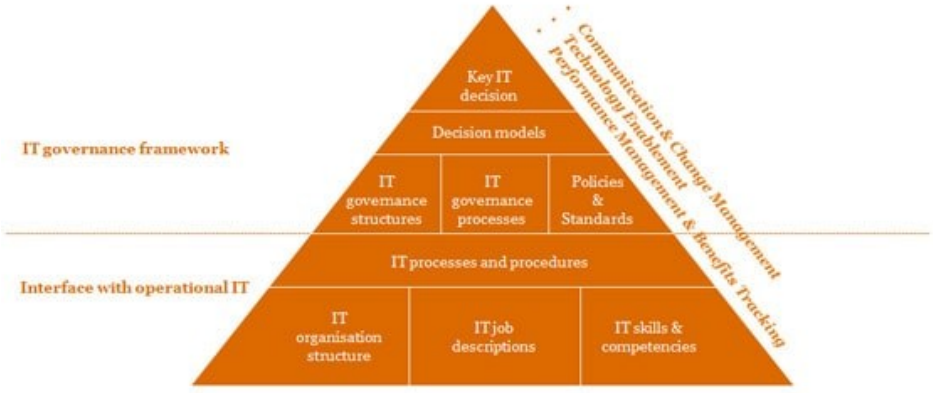


Figure 2.47. PwC's IT GRC implementation method

(**Source:** PricewaterhouseCoopers, 2011)

With the growing number of IT-related laws, regulations and policies or guidelines that apply to companies, the number of rules relating to IT is also increasing. At the same time, the increasing number of rules to be observed creates a particular challenge to control, control and monitor them (thus ensure compliance) alongside the IT and the company. The focus of considerations, in particular, those laws, ordinances and guidelines that have an impact on IT or on the business processes of a company supported by IT (Böhm, 2008).
Business strategy generally creates policies and other processes, and procedures to create a vision and mission. Processes should have their own controls to create unique and quality products, services and other end-user-required materials. In this thesis, all business-related IT objectives and their business strategy are to implement in all organization's policies, processes and all other procedures are analyzed. IT control environment and all related risk control matrices used in the sample bank.

2.6.2.6. Cobit 5

Cobit 5 is "an IT and a business framework for the governance and management of enterprise IT which is created by ISACA" (ISACA, 2018). Cobit 5 has 5 domains, these domains and their main purpose is depicted in Figure 2.48.

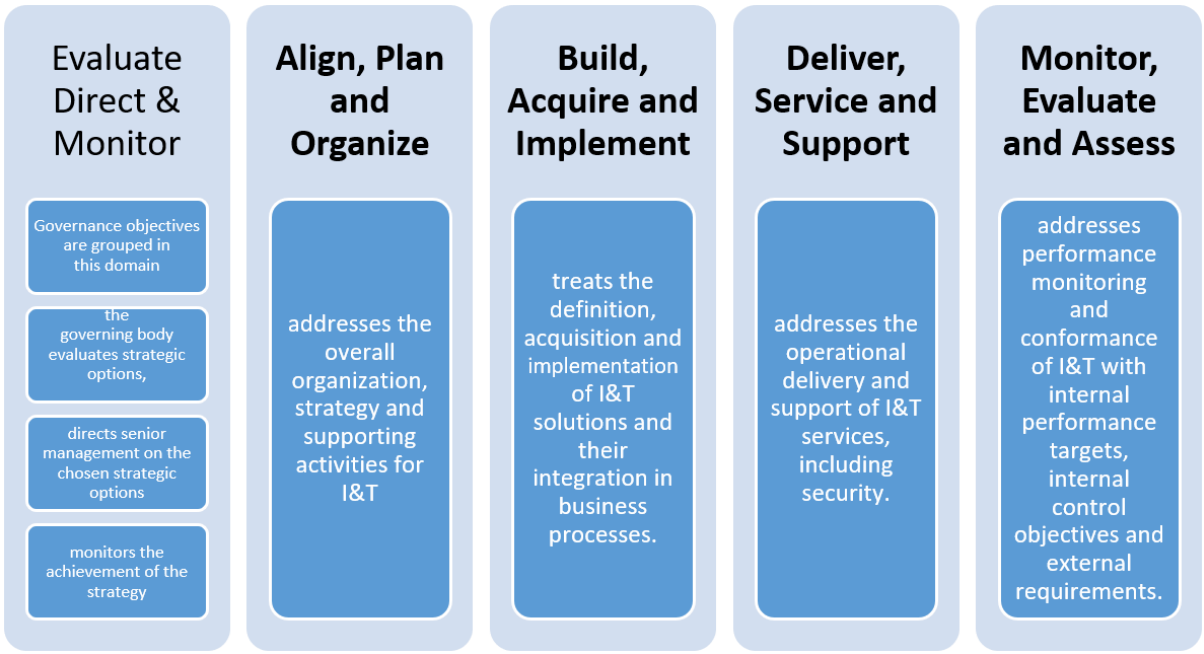


Figure 2.48. Cobit's domains and main purposes
(**Source**: ISACA, 2021)

Cobit 5 provides a comprehensive framework that supports companies in achieving their goals in the context of the governance and management of corporate IT. Cobit 5 helps companies to create an optimal IT value by striving for a balance between benefit realization and optimization of risks (at different levels) and the use of resources. (ISACA, 2012)

Cobit 5 enables holistic governance and management of IT for the entire company. All of them are functional areas of responsibility for the company and IT are seamlessly integrated and the IT-related interests of internal and external stakeholder groups are taken into account. Cobit 5 is a generic approach and therefore suitable for companies of all sizes, regardless of whether it is a commercial enterprise, non-profit organization or a public sector body act.

Cobit 5 is based on five fundamental principles for the governance and management of corporate IT, Cobit 5 principles are depicted in Figure 2.49.

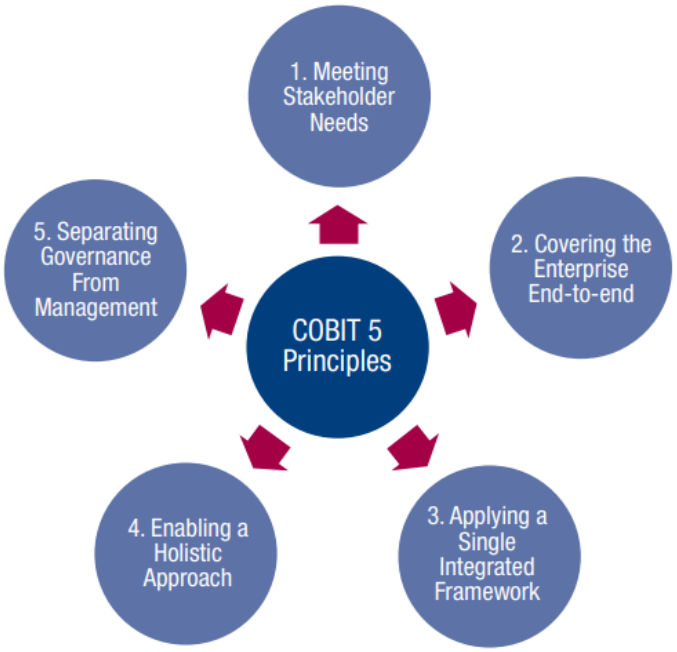


Figure 2.49. Cobit 5 principles
(**Source**: ISACA, 2021)

- "Principle 1: Meeting Stakeholder Needs"

Companies have tasks of creating value for their stakeholders by creating a balance between realizing benefits, optimizing risks and using resources. Cobit 5 provides all processes and other enablers ready to support the creation of value through the use of IT. Because every company pursues different goals, Cobit 5 can be adapted to the respective company context

via the target goals cascade. General corporate goals are converted into manageable, specific, IT-related goals and these are then assigned to specific processes and practices.

- “Principle 2: Covering the Enterprise End-to-end”

Cobit 5 integrates IT governance into Corporate governance:

It covers all functions and processes within the company; Cobit 5 doesn't just focus on the “IT function”, but treats information and related technology as resources that everyone in the business needs to deal with.

It regards all IT-related enablers for governance and management as company-wide and consistent, internally and externally, they encompass everything and everyone relevant to the governance and management of company information and the associated IT.

- “Principle 3: Applying a Single, Integrated Framework”

There are numerous IT-related standards and best practices, each providing guidance for a sub-area of IT activities. Cobit 5 integrated on a broader level of further relevant standards and frameworks and therefore serves as an all-encompassing framework for Corporate IT governance and management.

- “Principle 4: Enabling a Holistic Approach”

For efficient and effective governance and efficient and effective management of corporate IT requires a holistic approach that combines various, interacting components are considered. In Cobit 5, various enablers have defined that point to it are designed to implement a comprehensive governance and management system for corporate IT to support. In general, everything that contributes to the achievement of the company's goals is referred to as an enabler. Seven enabler categories are defined in the Cobit 5 framework: “principles, guidelines and frameworks, processes, organizational structures, culture, ethics and behavior, information, services, infrastructure and applications, people, skills and competencies” (ISACA, 2018).

- “Principle 5: Separating Governance from Management;”

The Cobit 5 framework defines the differences between governance and management. These two disciplines come with different types of activities but are connected, they require different organizational structures and serve different purposes. Cobit 5 represents the essential distinction between governance and management.

For ISACA Governance definition is “Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives.” And management definition is “Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives” (ISACA, 2012)

Cobit 5 has 37 processes, distributed in 5 main domains. All processes are mentioned in Figure 2.50.

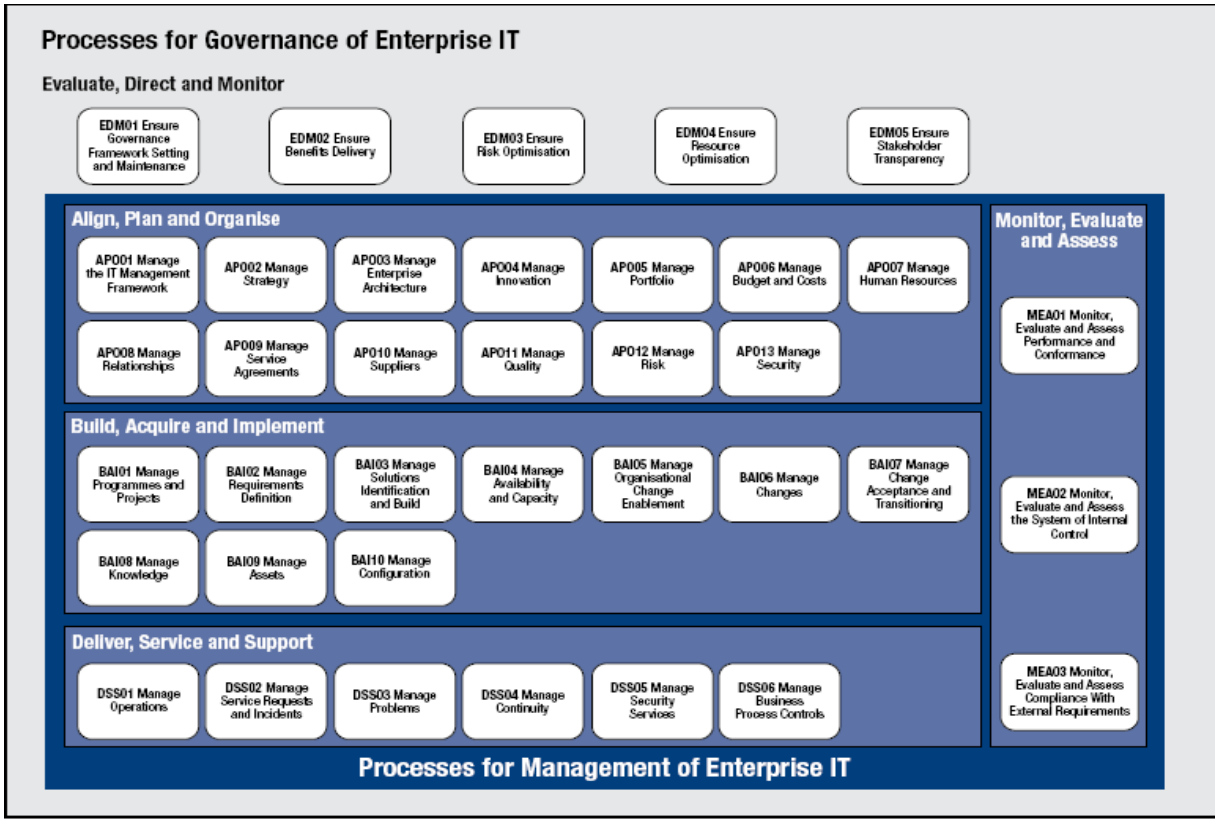


Figure 2.50. Cobit 5 processes
(**Source**: ISACA, 2021)

Cobit 5 is an input for Cobit 2019. In thesis, Cobit 2019 was used to design the tailored IT GRC model. In this model, ISACA takes Cobit 5 framework as an input “Cobit Core” to the model and uses design factors to create a specific tailored GRC model.

2.6.2.7. Cobit 2019

ISACA defined Cobit 2019 as “Cobit 2019 is based on Cobit 5 and other authoritative sources. Cobit is aligned to several related standards and frameworks. The analysis of related

standards and Cobit's alignment to them underly Cobit's established position of being the umbrella I&T governance framework." (ISACA, 2018)

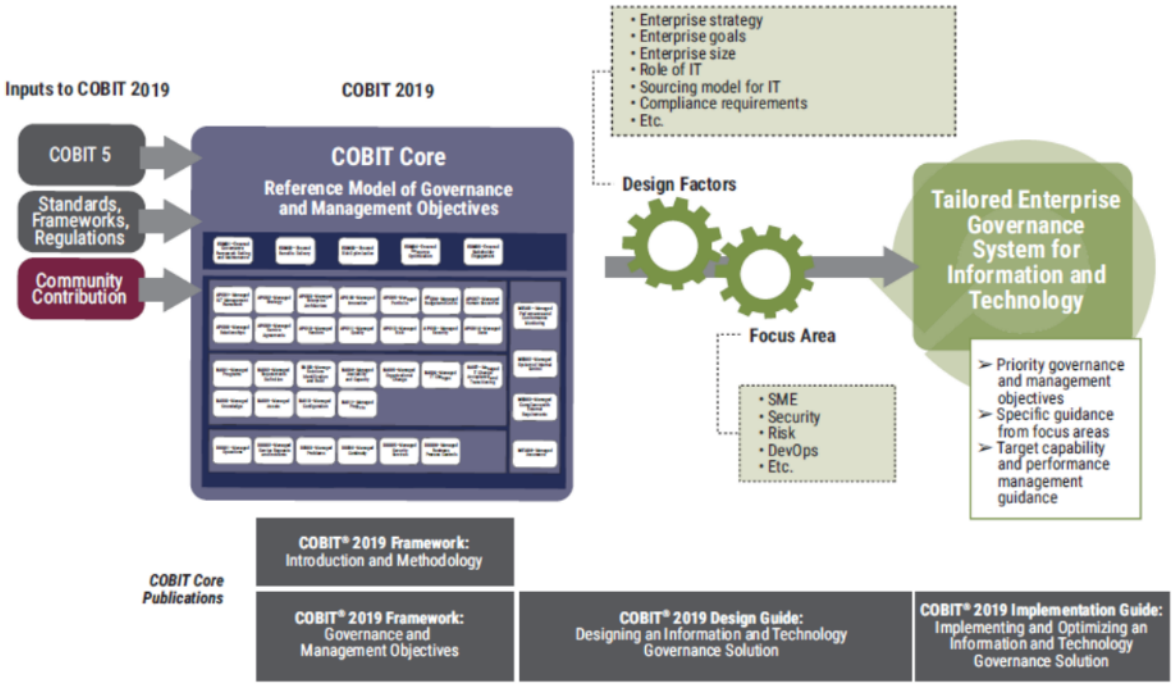


Figure 2.51. Cobit 2019 framework
(**Source**: ISACA, 2018)

Figure 2.51. shows the high-level overview of Cobit 2019, and how the different ISACA Cobit core publications cover different aspects.

The Cobit product family consists of 4 main books. Their descriptions are as follows;

- Cobit 2019 Framework: "Introduction and Methodology"; "Introduces the key concepts of Cobit 2019."
- "Cobit 2019 Framework: Governance and Management Objectives"; "Comprehensively describes the 40-core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks."
- "Cobit 2019 Design Guide: Designing an Information and Technology Governance Solution"; "Explores design factors that can influence governance and includes a workflow for planning a tailored governance system for the enterprise."
- "Cobit 2019 Implementation Guide: Implementing and Optimizing an Information and Technology"; "Governance Solution represents an evolution of the Cobit 5

Implementation guide and develops a road map for continuous governance improvement. It may be used in combination with the Cobit 2019 Design Guide" (ISACA, 2018)

Cobit 2019 is an updated version of Cobit 5. Cobit 2019 most important specification is to be adapted for every kind of business. The design guide makes it effective to use in every size and type of business adoptable. Main differences between Cobi5 and Cobit 2019 are given in Table 2.13.

Table 2.13. Cobit 2019 versus Cobit 5

Cobit 2019	Cobit 5
9 Principles (6 Governance system principles, 3 framework principles)	5 Principles
7 Components of the governance system	7 Enablers
Cobit core model (5 governance objectives and 35 management objectives)	Cobit 5 process reference model (5 governance processes and 32 management processes)
Goal cascade "1. Stakeholder drivers needs cascade into enterprise goals 2.Enterprise goals cascade to alignment goals 3.Alignment goals cascade to governance and management objectives. 13 Enterprise goals, 13 Alignment goals"	Goal cascade "1. Stakeholder drivers influence stakeholder needs 2.Stakeholder needs cascade to enterprise goals 3.Enterprise goals cascade to IT related goals 4.IT related goals cascade to enabler goals 17 enterprise goals, 17 IT goals"

(**Source**: Global Success Systems, 2019)

In Cobit 2019, ISACA defined implementation methods by creating design factors (DF). DFs do not exist in Cobit 5. Cobit 2019's performance model is aligned with CMM, but in Cobit 5 Cobit capability assessment is aligned to ISO 15504 model-based process assessment model. PAM guide and assessor guide are designed for performing assessments. Cobit 2019 final output a tailored GRC system, because of this unique model to create a model and BRSA's address to be compliant with Cobit encouraged to create a Cobit 2019-based IT GRC model and define its practices in relation to new published BRSA regulation.

2.7. Literature Review Results

As a result of the literature review, it's seen that the related subjects and especially the subject of "IT Governance" have been tackled from many aspects, in literature IT GRC model generation sample is very rare.

GRC theory samples are categorized as “conceptual and based on the theory”, Some papers are “implementation of the GRC concept”, and only a few “case studies”. IT GRC model creation effort is generally seen on big 4 consultancy firms’ special effort. IT GRC-related papers generally mentioned GRC theory. Racz et al. mentioned IT GRC in 2006 firstly. Literature review journal selection criteria are based on a literature review paper by Smet and Mayer 2016. Smet and Mayer made a systematic literature review, their model based on D. Tranfield, Denyer, and Smart’s "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," and Boell and Cecez-Kecmanovic’s, "On being 'systematic' in literature reviews in IS,” on Journal of Information Technology.

Literature review search criteria are based on related keywords GRC, IT GRC, IT Governance, IT risk and IT compliance. Researched paper years are between 2010 to 2020, 10 years period. Advanced search criteria are defined as paper title, abstract, and keywords. The bulk results are mentioned in Table 4.1. Publications were found using related journals’ search engines.

Table 2.14. GRC-related papers search results from Journals

	GRC	IT GRC	IT governance	IT risk	IT compliance
“MIS Quarterly”	0	0	9	3	0
“Information Systems Research”	12	1	369	459	118
“Information Systems Journal”	8	3	239	255	126
“Journal of Management Information Systems”	6	2	126	128	25
“Journal of the Association for Information Systems (JAIS)”	3	1	174	216	69
“European Journal of Information Systems”	2	1	113	229	72
“Journal of Information Technology”	1	1	112	161	48
“Journal of Strategic Information Systems”	1	1	119	175	49
Total	33	10	1261	1626	507

Directly IT GRC-related only 10 papers were found but 60, (4,75%) of IT Governance-related papers include IT GRC subjects. 31, (1,9%) of IT risk-related papers again include IT governance and IT GRC aspects but only a few compliance subjects. IT compliance-focused papers are generally related to a special regulation or a best practice. These papers’

subjects are various and not directly about GRC subjects. Only 22 (4,3%) of them mentioned IT governance and IT GRC.

After reviewing all related papers, IT GRC related 63 papers selected from listed journals, selection criteria (inclusion criteria) are; must directly related with selected subject, must be an academic journal, available online as full text, journal discipline related with management information systems, business administration or IT governance/management, time period between 2010-2020. Other GRC and "G", "R" or "C" related papers were again evaluated but they are generally related within a specific IT process, in common they are generally focused on IT security and IT sourcing/outsourcing or vendor management. Selected samples are based on IT GRC or its various and essential subdomains. To have a widely GRC-related literature review another review was made with a methodology based on Fettke 2006. Racz et al. made a GRC-based literature review by this methodology used for creating observations. They found GRC-related papers by "Publications were found using the search engines of WISO, EBSCO, ACM, IEEE Xplore, SpringerLink, Emerald, Google, the Vienna University of Technology and Ludwigshafen University of Applied Sciences libraries, and through manual browsing on relevant websites." These databases searched and found IT GRC-related 42 papers in the period of 2010-2020. Total of 103 papers were evaluated by the methodology depicted in Figure 2.52.

Property		Category	Application
1. Type		natural language and mathematical-statistical	quantitative in observations, qualitative in definitions analysis
2. Focus		theory	GRC definitions are theoritical concepts
3. Target	Formulation	explicit	see "motivation" section
	Content	integration	integration of publication content in a definition for research
4. Perspective		neutral	no leading hypothesis defined in advance
5. Literature	Selection	explicit	see below in "methodology" section
	Scope	selective	keywords, sufficient length, degree of product-independent information, text-based format
6. Structure		holistic by topic	identification of commonalities
7. Target group		practicioners, general and specialised researchers	primarily directed towards researchers
8. Future research		explicit	see "future research" section

Figure 2.52. Literature review methodology created by Racz et al.
(Source: Racz et al., Publication review properties (based on Fettke 2006))

Literature review was made on Web of Science and Google Scholar databases also to have a consistent comparison of WISO, EBSCO, ACM, IEEE Xplore, SpringerLink, Emerald databases searched After categorizing and evaluating 103 papers, they are evaluated for the observations mentioned in Racz et al.'s observations updated version in Table 4.2. In this table given in Racz et al. 2000-2010-year period GRC literature review's result and made a comparison of these two decades. After mentioning these new observations mentioned. Racz et al. evaluated 107 GRC-related papers. Generally, new observations align with each other but cast doubt on some points. In the table on the left side, their observation results are given and on the right side 2010 to 2020 observation is given.

Table 2.15. GRC literature review observations two-decade comparisons.

Observation	2010 (Racz et al.)'s Result	*2010-2020 Literature Review Result*
"There is basically no scientific research on GRC as an integrated concept"	*"While lots of research exists on the 'G', the 'R', and the 'C' as separate topics, the potential integration moves under the radar of scientific research. 2 of the 107 sources identified a mere two deserve the label 'research paper'. Both publications only provide short definitions of governance, risk management and compliance separately. Observation demonstrates the lack of research participation in GRC."*	*After 10 years period, the researcher created GRC-related and also "G", "R", and "C" related separate papers. In all individual research papers about G, R or C or other 2 dimensions (G+R or G+C) mentioned. 31 of 103 papers are about directly GRC (also ERM or IRM). This observation should be updated, researchers mentioned that GRC (ERM/IRM) is an important issue in their papers.*
"Software vendors, analysts, and consultancies are the main GRC publishers"	*"We categorized our sources by authorship, distinguishing software vendors, analysts, consultancies, scientific research personnel and independent experts. Co-authorship was applied in four cases. For interviews only, the role of the interviewee was considered. The review shows that GRC software vendors are the most active group providing GRC publications, closely followed by analysts and consultancies. Together these three parties participated in 94% of the selected GRC publications. GRC is obviously dominated and driven by the business community."*	*Still partially a true observation. GRC publications especially which are related to a software vendor, generally explain why these tools are crucial to companies. There is a big software industry related to GRC, which creates research. They defined themselves as; "Regulation Technologies". 12 Software implementation case study evaluated, 15 of big four consultancy firms' papers. Also, consultancy firms get agreements to set up and implement these GRC tools in a company so it is a grift subject to count dependently. 10 years ago, maybe this ratio is too high but in this period of time researchers create papers for the GRC term itself. Only 18% of papers confirm this observation.*
"Software technology is the prevailing primary topic."	*"When publications are dominated by software vendors followed by consultancies that help implement technologies, it is not surprising that software technology is the prevailing topic in these works. 57 publications (53%) "Primarily treat technology. This finding underlines the importance of technology as an enabler of GRC."*	*Not a true statement for these years period. There are still software vendor publications but the primary topic changed to how to integrate all the related G-R-C domains together. Also, the GRC started to evolve ERM and IRM, risk-based models. Only 12 papers' primary topic was GRC technology or a software implementation or tool selection. (13%)*

Observation	2010 (Racz et al.)'s Result	*2010-2020 Literature Review Result*
"Regulatory compliance is the main driver of GRC, challenged by risk management."	*"We listed all reasons explicitly named as GRC drivers in publications. 43 out of 107 publications do not mention any GRC drivers. Of the remaining 64, 25 (39%) consider the increasing number of regulations to drive GRC. 18 (28%) name increased risk, 10 (16%) the potential for cost reductions, 8 (12,5%) mention the increased complexity of business due to market dynamics, globalization and other factors."*	*A true observation, regulatory compliance is the main driver of GRC. In literature research 46 (47%) papers mentioned this issue as an important factor, a domain, a driver. In every country, regulations are different. So, compliance requirements are so complicated. Although these complicated compliance requirements, %24 of the papers create a solution to use a mainstream best practice to comply with these regulation issues. While using ISO, NIST or any other framework like Cobit or OCEG's GRC they integrate their local regulations with these best practices again. The subjects evaluated for selected 103 papers and 32 (33%) named increased risk, 12 (13%) the potential for cost reductions, and 17 (18%) mention the increased complexity of business due to market dynamics, globalization, and other factors.*
"ERM is an important methodology within GRC"	*"We wanted to find out how often enterprise risk management (ERM) or its synonyms were mentioned in GRC publications. References to ordinary risk management were not accounted for. 58 publications (54%) mentioned ERM."*	*A true observation, ERM also IRM (Integrated Risk Management created by Gartner) is still an important methodology, the ratio is below 2010 (32%) for ERM or IRM. These concepts started to use widespread, especially in integrated risk management.*

New Observations about GRC or IT GRC

Observation 1: "IT GRC is a subdomain and should be considered in a part of GRC" (Racz, 2010); GRC is an umbrella framework that covers all the enterprises' processes, and IT processes included. GRC-related researches widely cover all the business domains and also IT. IT GRC-related researches are directly focused on IT processes to align with related business processes. In 37% GRC related research are mentioned IT GRC or technology processes are a part of the main GRC domain in a corporate.

Observation 2: "IT risk management and also IT security management is mostly mentioned IT GRC issues" (Racz, 2010); IT GRC-related researches are mainly divided into two areas. IT risk or IT security-related researches are 24%, and others are mostly IT Governance related 16%.

*Observation 3: "Cobit is most often researched IT governance framework in literature": (Racz, 2010);*23 of 103 papers mentioned Cobit. They used it as the best practice. Researchers worked on a specific Cobit domain and create maturity models to comply with it. Cobit can be used in various sectors. Especially in universities or financial institutions.

Observation 4: "Strategic alignment is the main objective in IT GRC frameworks" (Racz, 2010); IT GRC or GRC-related research mentioned this issue as an important one. Strategic alignment is the main objective of some frameworks like Cobit or ITIL. This notion is emphasized many times. 36% of researchers mentioned this concept in their research.

Considering the new observations and 10-year differences, it is seen that the number of academic publications in the field of GRC has increased, but new approaches have emerged and started to attract the attention of the academy. Although the concepts of integrated risk management or corporate risk management are not new concepts, they have started to be used instead of or together with GRC. Although there is an increasing number of researches specific to IT GRC, it has been observed that when academic studies in IT governance intensify, studies are also produced in the field of IT risk due to increasing IT risks and especially information security or cyber security. In particular, IT compliance has increased in the current situation, although there has been a small number of academic studies in the past, but its increase has been limited compared to other fields. When all these developments are evaluated together, it can be concluded that the concepts of GRC and IT GRC continue to be important for academic researchers and that the IT GRC sub-fields are studied intensively. Within the scope of the thesis, there is no papers or thesis in searched databases that deals with all these areas together and compiles the known/intensely used frameworks and conveys IT relations. A bank application is another unique concept. The thesis aims to fill the gap in this field.

2.8. Literature Review Results in Turkish Journals and Thesis

In Turkish literature, the thesis subject "IT GRC" has never been studied before. Only a few IT governance-related papers and thesis are found in local articles and YÖK (Yüksek Öğretim Kurulu, Council of Higher Education) thesis databases. Among global papers, the "application in Turkey" has never been stated. This literature gap was especially considered in designing the following research studies. It has been understood that an IT GRC model creation and implementation in a bank is a unique concept.

The Turkish banking sector is a highly-regulated area, which is based on high technology and innovation. This results in the importance of IT governance. Without effective IT governance and lack of supervisory management, IT risks emerge and compliance deficiencies can easily appear. BRSA punishes in high process for all IT-related findings. These punishments are sometimes tangible with money and sometimes it can cost to stop operating the part of a process or to close the whole bank. The audit process (internal or external) is highly critical for banks to provide additional assurance to the board of directors.

Additionally, role of IT in a Bank and the relation between banks' service portfolio is based on the used technology, such as digital channels to give services to customers in a time range of 365-day 7/24 performance. IT service stability/continuity and systems security are other crucial aspects and the IT risk domain inherits these critical processes. The IT compliance domain again manages regulations in all IT-related areas. Regulators try not to set any free area on the compliance definition process, after creating needs of regulation they mapped their regulation to a best practice. Cobit 4.1. is a serious best practice sample for the banking sector. Again, banks should select an IT security management standard and every year should show the independent auditory boards that they are compliant with their selected best practices.

Although in Turkish thesis and paper databases, IT GRC subject has never been studied, there are a few IT governance and management practices and IT risk-related papers. IT compliance-related papers are very few and they are sector-related. There are a lot of primary and secondary relevant resources and methods in Turkish big 4 and other consultancy firms' journals. Also, there are some global and local companies served in Turkey to create an IT GRC model and software applications to sell to corporates. RSA and MetricStream have mostly known as GRC applications. There are more than 20+ applications in this area, In

Figure 2.53. bests are depicted in Gartner 2020 magic quadrant report. Some GRC applications are better for vendor risk management or overall risk management.

Figure 2.53. GRC-related software tools Gartner magic quadrant

(Source: Gartner, 2020**)**

In Turkey TAC created an application and a framework to manage GRC in any sector. They created CONIG® (Converged Information Governance) as an IT governance framework based on lots of best practices. These best practices are mentioned in Figure 2.54.

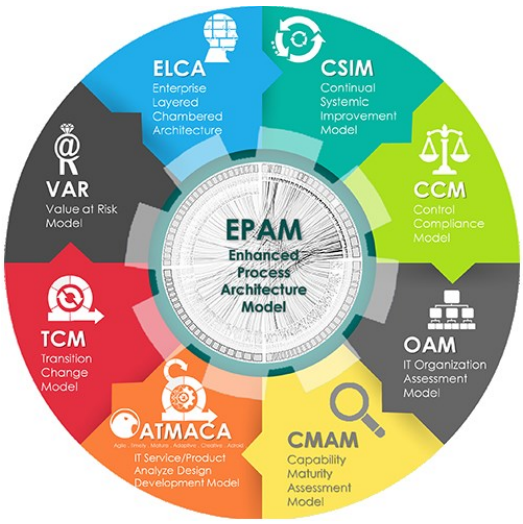


Figure 2.54. CONIG® (Converged Information Governance) by TAC

(Source: TAC A.S. CONIG®, 2021**)**

They define “CONIG® (Converged Information Governance) as a reference framework that consists of components of various models, best practices, frameworks and standards. All of the underlying frameworks and best practices are widely accepted in the industry. While they might bring different perspectives and differ in nuances the common goal of all these frameworks and best practices is the assurance of provisioning of IT services, business services, and other enabler services” (TAC A.S., 2021).

2.9. Literate Review Final Evaluation

In the literature study, first of all, corporate governance, IT governance, IT governance frameworks, IT risk management and risk management frameworks, IT compliance management and all IT-related regulations of the Turkish banking sector are given. In national and international publications, these fields have been evaluated together, as well as individually, and their relations with each other have been investigated. After these explanations, the concepts of GRC, and IT GRC are explained in the thesis. These pre-definitions can be considered as prerequisites to introducing the concept of GRC. Because the concept of GRC does not envisage the management of governance, risk and compliance alone, but the management of each one in harmony. GRC frameworks and related IT GRC frameworks could not be found together in the reviewed articles and theses. In this sense, GRC and related IT GRC frameworks are explained in the study.

The literature review results, which were carried out with keyword searches and content analyzes by scanning the journals that make selected publications in the field of management information systems, revealed that an increasing number of academic studies were conducted on the concepts of GRC, IT GRC, IT governance, IT risk and IT compliance. When compared with the study of Racz et al., which covers a 10-year period, it has been concluded that governance models have been started to be studied specifically for the IT GRC concept, and GRC studies have been studied by both academic and corporate firms, apart from large audit and consultancy firms. It has been determined that intensive studies have been carried out, especially in the field of IT risk, and it has been determined that they mostly refer to cyber security risks. After the IT risk issue, it has been observed that especially IT governance subject has been studied. The number of articles dealing directly with GRC and IT GRC subjects was found to be quite low compared to IT Governance, IT risk, or IT Compliance. There are studies that introduce IT compliance studies, such as compliance with local regulations and their importance, and report developments or reveal

the practices of different countries. After the keyword searches, the results of the 103 articles selected for analysis were compared with the 2000-2010 and 2010-2020 observations, and the change reflected in the literature was compared. As a result, no literature study has been found in which the IT GRC concept has been evaluated together with other relevant key concepts, and the relevant frameworks and international good practices that can be reached, have not been found, and the literature gap in this field has been filled with the study. Starting from corporate governance to IT governance, GRC and IT GRC relations have been tried to be explained as a whole. In the thesis literature section "corporate governance", "IT governance" and governance subjects, topics are covered in detail. This relation is depicted in Figure 2.55., all other related subjects studied are summarized in the picture.

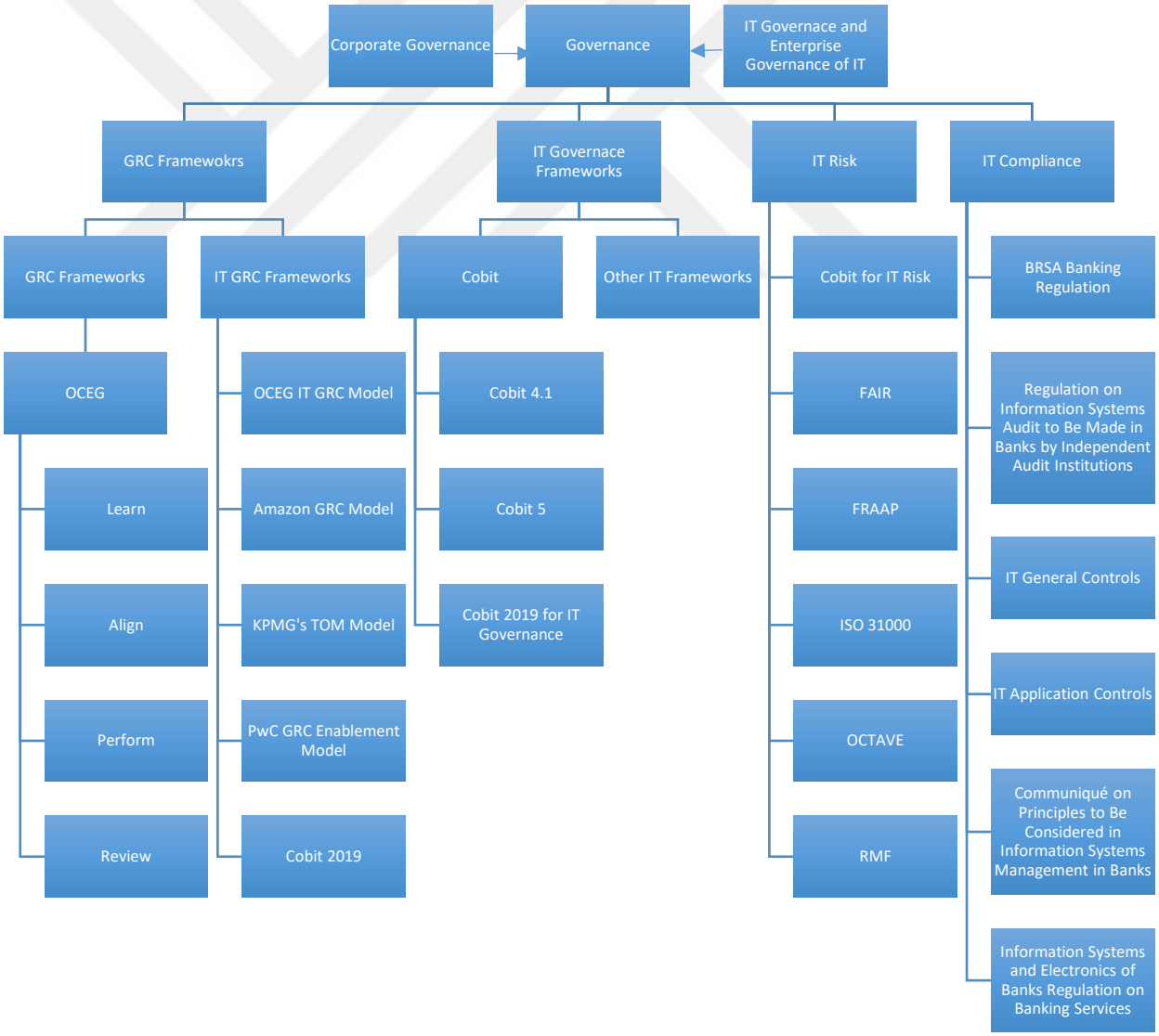


Figure 2.55. Literature structure that worked in the thesis

3. RESEARCH METHODOLOGY

In this section the research design of the thesis, design factors, the method of the creation process of proposed IT GRC model, and the results of the latent semantic analysis of the selected regulation and Cobit relatedness studies are given.

3.1. Designing the Research

This thesis development process is based on 3 phases. GRC literature review, IT GRC model creation, LSA-based compliance map creation. Every phase and it is major works are listed in Figure 3.1.

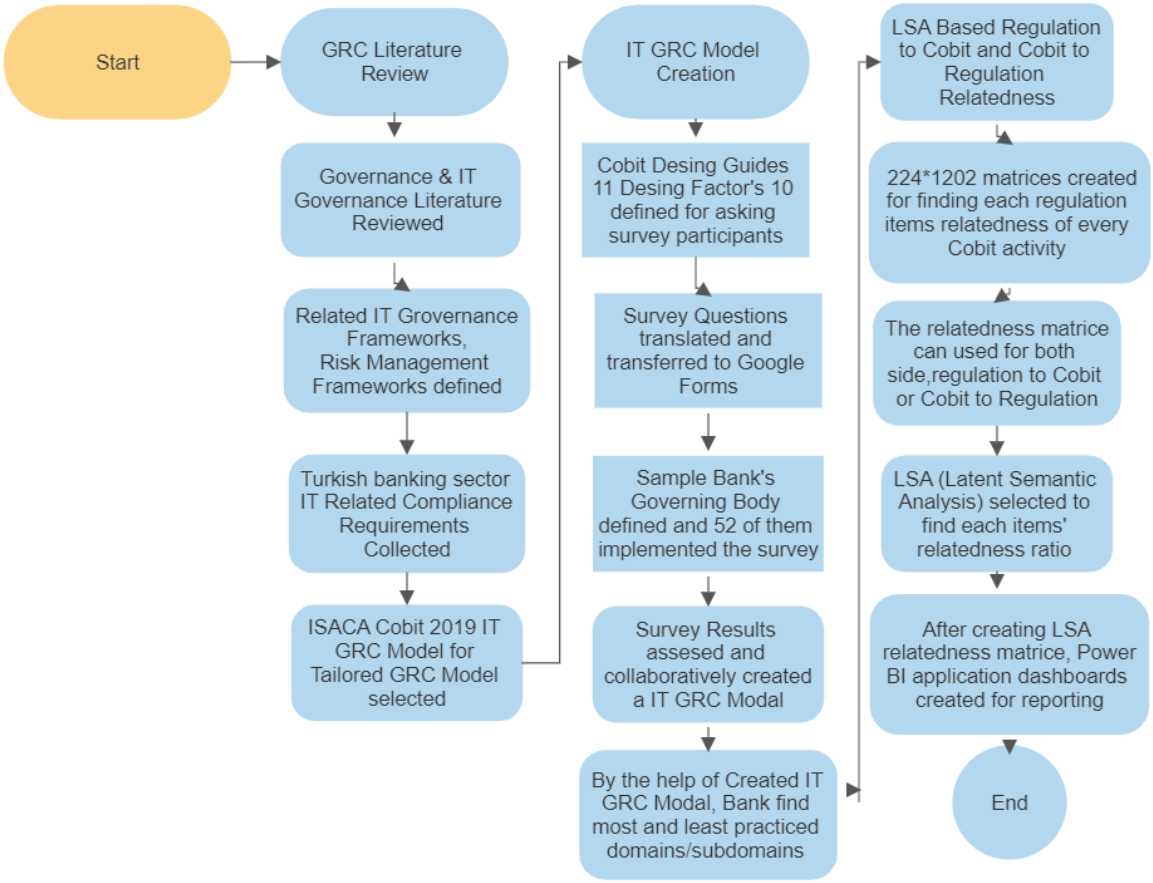


Figure 3.1. Research process

GRC literature review is based on academic papers and governance and risk frameworks information gathered from best practices and standards but compliance requirements are created along with the sample countries' banking sector IT-related regulations.

IT GRC model creation process is mentioned in Figure 3.2. based on Cobit 2019 with the help of a quantitative survey. This survey was made with Google Forms questionnaire. Question set based on "Cobit 2019 Design an Information and Technology Governance

Solution Guide". The created questionnaire is given in Appendix A. Cobit's proposed model creation method is based on 4 foundational steps. Firstly, the businesses' enterprise strategy, goals, risk profile and I&T-related issues are understood by governors. Secondly, with the help of the first four design factors of Cobit 2019 design guide (explained in the following pages) governance system's initial scope was determined. Third, threat landscape, the role of IT, sourcing model of IT, IT implementation methods, adoption strategy and enterprise size (other 6 design factors of Cobit 2019) were used to refine the scope of the model. The final step is to conclude the model, Cobit proposes approaches for a resolution to conclude the design.

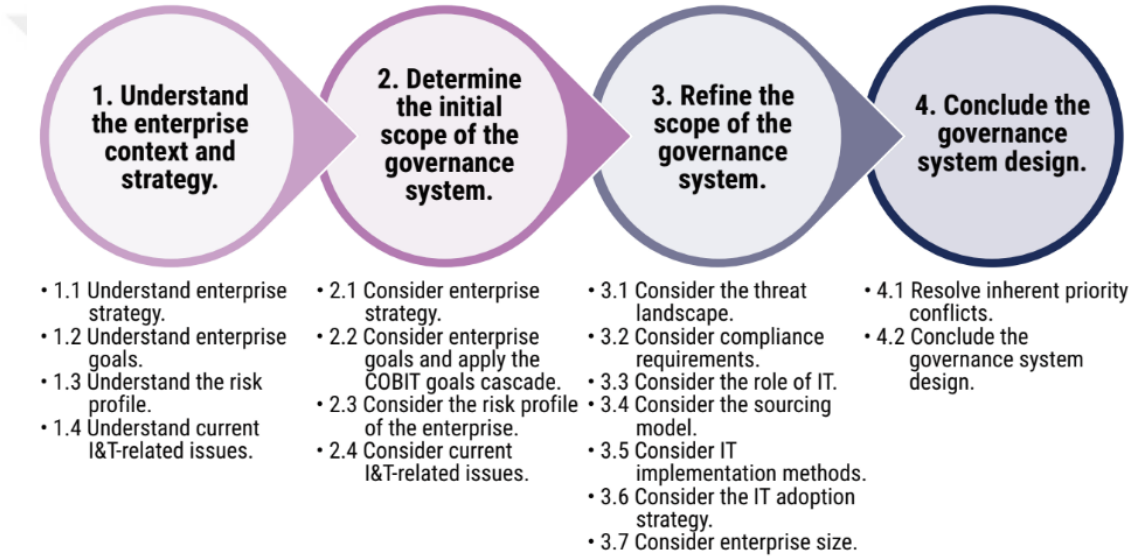


Figure 3.2. Tailored IT governance risk and compliance mechanism by Cobit 2019 design guide

(**Source**: ISACA Cobit 2019, 2018)

After completion of the quantitative survey, a canvas was created about Cobit 2019 domain system design and defined the GRC model's most important processes. 11 of 10 Cobit design factors were used to create survey results as a canvas and a Cobit process importance map. One of the design factor is "Enterprise Size", it is constant in the survey and did not ask to survey participants.

The survey considers the most relevant governance and management objectives for the values of each factor of design. After initial design and design refinement steps, a qualitative decision is made on the priorities of the governance and management objectives. The initial scope of the tailored GRC system is based on enterprise strategy, enterprise goals, the risk

profile of the enterprise and I&T related issues. To refine the scope of a tailored governance system, to the participants answered about sample banks' threat landscape, compliance requirements, role of IT, implementation methods of IT, IT adoption strategy. The quantitative approach involves numerical mapping tables created for each design factor. The tables' assignment variables quantify the descriptive values associated with each design factor to indicate their correlation with governance and management objectives.

The questionnaire contains and implements this 10-design factor, Cobit 2019 mapping tables typically contain values between one to five. Five indicates the maximum relevance of a governance or management objective with that value of the determined design factor; zero indicates that it is not relevant.

Translating the values of the design factor to the importance of a governance and management objective involves the calculation of matrices that are derived in a score for each governance and management objective. At the end of steps 2 (determining the initial scope) and 3 (refining the scope of governance system), the results of several of these calculations should be consolidated. Again, there is no objectively necessary and fixed method for its consolidation; however, it is usually best achieved by using a sum.

3.1.1. Design Factors and Research Results

Cobit design guide creates a model for a tailored system. It has risk management and related compliance management in related domains. GRC model creation needs 10 selected design factors. ISACA defined these factors as "Design factors (DF) are factors that can influence the design of an enterprise's governance system and position it for success in the use of I&T" Design Factors are listed in Figure 3.3. ISACA created these factors and future factors would be created. Every DF has a unique number and is used to give survey results.

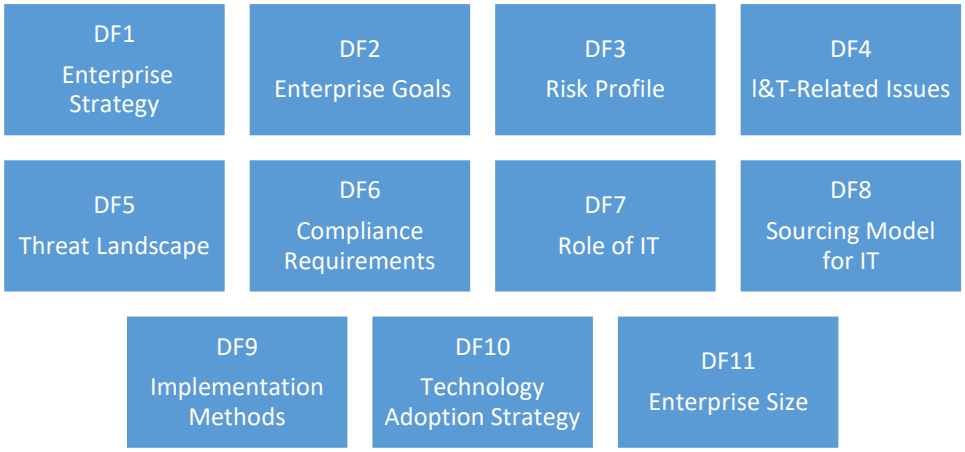


Figure 3.3. Cobit 2019 design factors
(**Source**: ISACA Cobit 2019, 2018)

In this thesis, an example from the banking sector, where IT governance, IT risk management and regulatory compliance are of high importance, was chosen to create the IT GRC model as an exemplary business. The widespread use of Cobit in the Turkish banking sector, its mandatory selection by the regulatory authority, and the fact that the current version of Cobit proposes a tailored IT GRC model supported the study of a bank from the Turkish banking sector. The selected bank is a company that has been serving in Turkey for more than 30 years, has branches in all cities of Turkey, develops almost all of its information technologies and software with its own IT organization and operates complex IT processes. The sample bank in which the research was conducted sold its core banking software to other banks and also provides maintenance and support services with its subsidiary. Complex IT service procurement processes are also operated between the bank and its technology subsidiary. All systems and infrastructures of the sample bank are run on its own established data center, and critical infrastructure management processes are also managed. The established data center is in Turkey and it uses cloud technology to the extent permitted by the regulation.

It is among the prerequisites of Cobit that the research can be carried out together with this bank's IT governing body. The proposed model was created by filling in a quantitative survey created by experts in the subject. Research survey was completed by 52 bank personnel. They are all related to governance, risk and compliance management in the sample bank. In literature, this mass is mentioned as governing body of the sample bank.

The questionnaire reached the %94 of the main mass surveyed. The participant's role in the sample bank to control their relatedness to the thesis subject and total experience in the banking sector was evaluated. It is aimed to ensure that those who contribute to the

research define the sample bank and make the right guidance by setting a minimum 5-year experience requirement. 3 of the completed survey did not evaluate for this reason. Survey participants were selected directly by personnel lists and sent the survey link prepared on Google Forms. Also, one on one meetings were made to gather sample bank's executives' assessment results. Before sending the survey a group of related department's G-R or C related personnel, a presentation had given about GRC, IT GRC and its importance. With the help of this presentation participation rate increased. After completing the presentation, survey links were sent directly to related participants or to executive managers an interview is made to fill the survey form.

The mean of survey participants' experience is 7.6 years. Personnel's role when participating in the survey is diverse. The roles of survey participants are mentioned in Table 3.1. Participant's roles and counts for the survey.

Table 3.1. Participant's roles and counts for the survey

Role	**Count**
CIO, CTO, CHrO and CFO and the chief executives	4
Head of IT and IT Vice Presidents	6
IT Project and Strategy Project managers	7
IT Auditors (Auditor and Internal Controller)	4
IT Service Managers	19
IT G-R-C related heads, managers and inspectors	12
Total	52

3.1.1.1.Enterprise strategy (DF 1)

Companies can have different strategies, which can be expressed as one or more prototypes shown in Table 3.22. Organizations often have primary and secondary strategies. Design factor values (strategy archetypes) come from Cobit 2019 design guide. The first design factor value "growth/acquisition" is related to APO 02 "Managed Strategy", APO03 "Managed Enterprise Architecture", APO05 "Managed Portfolio", BAI 01 "Managed Programs", BAI 05 "Managed Organizational Change", BAI11 "Managed Projects", these are components of organizational structure which supports the portfolio management and investment office, also related with the services, infrastructures and applications to facilitate businesses growth and realize economies of scale. "Innovation/differentiation" value is related to APO 02 "Managed Strategy", APO 04 "Managed Innovation", APO 05 "Managed

Portfolio", BAI 08 "Managed Knowledge", BAI 11 "Managed Projects" has an important influence on "of culture and behavior component for innovation". Cost leadership value focused on IT costing and budgeting skills, it has an important influence of culture and behavior of spending on IT budget. It is related with Cobit's EDM 04 "Ensured Resource Optimization", APO 06 "Managed Budget & Costs", APO 10 "Managed Vendors" processes. Client service/stability value is directly related to customer satisfaction and business client centricity. This value is related to Cobit's EDM 02 "Ensured Benefits Delivery", APO 08 "Managed Relationships", APO 09 "Managed Service Agreements", APO 11 "Managed Quality", BAI 04 "Managed Availability & Capacity", DSS 02 "Managed Service Requests & Incidents", DSS 03 "Managed Problems", DSS 04 "Managed Continuity" (ISACA, 2018).

Table 3.2. DF 1, enterprise strategy design factor details

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues)[2]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients[3]
Cost Leadership	The enterprise has a focus on short-term cost minimization[4]
Client Service/Stability	The enterprise has a focus on providing a stable and client-oriented service.[5]

(**Source**: ISACA Cobit 2019, 2018)

To gather enterprise strategy information from participants the survey has a question about getting strategy archetype importance level inputs from participants. Inputs, calculation methods and outputs are given in Table 3.33.

Table 3.3. DF 1 inputs, calculation methods and outputs

Input	• Each of the four possible values for the enterprise strategy design factor—growth/acquisition, innovation/differentiation, cost leadership, client services/stability—must be rated between 1 (not important) and 5 (most important). • It is recommended to maintain sufficient spread between values.
Calculation	• The toolkit performs a matrix calculation of the entered values for Design Factor 1 *Enterprise strategy* with the mapping table for design factor 1, resulting in a score for each governance/management objective. • The toolkit performs a second matrix calculation of a baseline set of values for design factor 1 with the mapping table for design factor 1, resulting in a baseline score for each governance/management objective. • The toolkit then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

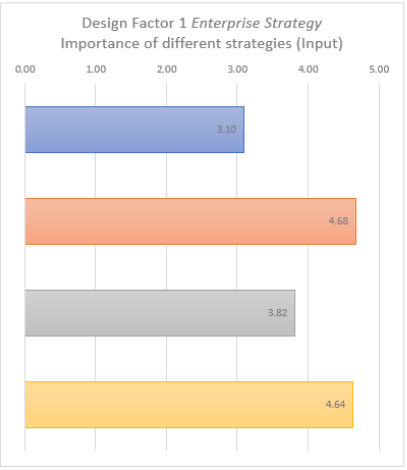
(**Source**: ISACA Cobit 2019, 2018)

Proposed collaborative approach gets inputs and calculates as defined in the design book. But, in the end 52 of these results were summed and divided by the participants' count and

get the mean of all these enterprise strategies' importance scores. Design factor 1 mapping table is given in Appendix B. Total unique strategy archetype results are calculated and then divided by the participants' count. For DF 1 calculation method is explained detailly for EDM 01 process. All other 39 Cobit processes' relative importance levels calculated as this method. For DF 1, calculation details for EDM 01 results calculated with this formula; "MMULT(DF1map!B2:E41;'DF1'!D7:D10)", MMULT formula multiplies two matrices, "DF1 map" and "DF1" are two different Excel sheet and in B2 to E41 in DF1 and D7 to D10 there are two different matrices. In all other design factors this MMULT formula affects in the same way. DF1 sheet contains means of 52 survey participants' results in D7 to D10 cells in excel sheet, DF 1 map is another sheet which has constant values defined in Appendix B. In DF 1 map sheet B2 to E 41 cells contain another matrix to multiply with collaboratively created strategy archetypes final result. Matrix calculation results create "Result" of each Cobit domain presented in Table 4.6. Another baseline result was calculated again for the changing possibility of the baseline of each archetype. In the survey participants did not change these baselines. The calculation formula is the same way of the individual "Result" score; "MMULT(DF1map!B2: E41;'DF1'!E7:E10)". After calculating the average, standard deviation and correction factor by "AVERAGE(D7:D10)"; baseline scores average of strategy archetype, "STDEVP(D7:D10)"; standard deviation of them, and "AVERAGE(E7:E10)/ STDEVP(D7:D10)" ; for correction factor. The final score is calculated with the formula of; "IFERROR(MROUND(E14*100*B22/C22;5)-100;0)"; E14 cell contains correction factor, B22 contains "Result" and C22 contains "Baseline Score". "IFERROR" stand in this formula to prevent calculation errors. This formula gives -10 to +10, (increased by 5) final results for each of Cobit processes.

The sample bank's primary focus is on innovation and differentiation and a secondary focus on client service and stability are depicted in Figure 3.4.

Strategy Archetype	Importance (1-5)
Growth/Acquisition	**3.10**
Innovation/Differentiation	**4.68**
Cost Leadership	**3.82**
Client Service/Stability	**4.64**



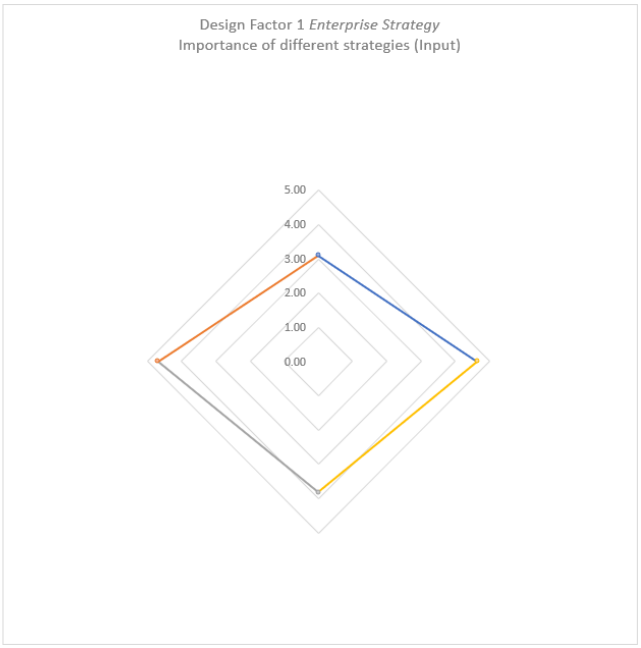


Figure 3.4. Design factor 1, sample bank's strategy archetype

Governance/management objectives' importance result is depicted in Figure 3.5. spider map. To show an overview of all Cobit, ISACA used spider maps and in this thesis after every design factor evaluated related factors spider map was created to assess each of DF's special contributions to the relative importance of each Cobit process. Detail for Design Factor 1 for Enterprise Strategy is given in Table 3.4.

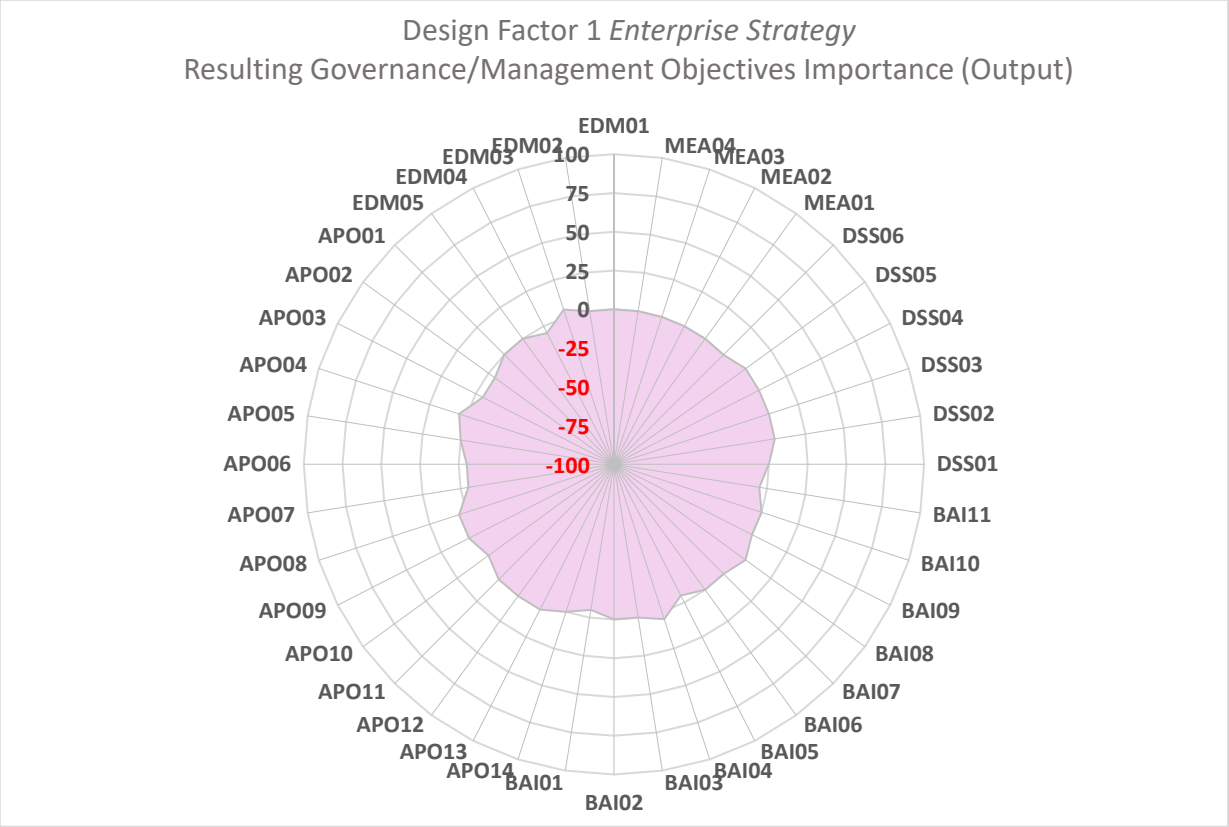


Figure 3.5. DF1 results for Cobit domains

DF1 adds total and final spider map positive effect on EDM 03, "Ensured Risk Optimization", APO 04 "Managed Innovation", APO 08 "Managed Relationships", APO 09 "Managed Service Agreements", APO 11 "Managed Quality", APO 12 "Managed Risk", APO 13 "Managed Security", BAI 04 "Managed Availability and Capacity", BAI 08 "Managed Knowledge", DSS 02 "Managed Service Requests and Incidents", DSS 03 "Managed Problems", DSS 04 "Managed Continuity", DSS 05 "Managed Security Services" and negative effect and negative effect on EDM 04 "Ensured Resource Optimization", APO 02 "Managed Strategy", APO 03 "Managed Enterprise Architecture", APO 06 "Managed Budget and Costs", APO 07 "Managed Human Resources", BAI 01 "Managed Programs", BAI 05 "Managed Organizational Change", BAI 11 "Managed Projects". Negative results can be found in modal selected processes, final importance or maturity level calculated by the cumulative results of each DF's results. DF 1 outputs changes between -10 to +10 relative importance given detailly in Table 3.4.

Table 3.4. DF 1, Enterprise strategy governance/management objective importance results

Governance / Management Objective	Result	Baseline Score	Relative Importance
"EDM01 Ensured Governance Framework Setting and Maintenance"	20.47	15	**0**
"EDM02 Ensured Benefits Delivery"	33.21	24	**0**
"EDM03 Ensured Risk Optimization"	20.88	15	**5**
"EDM04 Ensured Resource Optimization"	29.25	22.5	**-5**
"EDM05 Ensured Stakeholder Engagement"	24.77	18	**0**
"APO01 Managed I&T Management Framework"	16.24	12	**0**
"APO02 Managed Strategy"	37.6	28.5	**-5**
"APO03 Managed Enterprise Architecture"	30.22	24	**-5**
"APO04 Managed Innovation"	30.28	21	**5**
"APO05 Managed Portfolio"	43.76	33	**0**
"APO06 Managed Budget and Costs"	29.25	22.5	**-5**
"APO07 Managed Human Resources"	19.34	15	**-5**
"APO08 Managed Relationships"	30.18	21	**5**
"APO09 Managed Service Agreements"	32.07	22.5	**5**
"APO10 Managed Vendors"	28.11	21	**0**
"APO11 Managed Quality"	30.16	21	**5**
"APO12 Managed Risk"	25.54	18	**5**
"APO13 Managed Security"	23.2	16.5	**5**
"APO14 Managed Data"	16.24	12	**0**
"BAI01 Managed Programs"	34.45	27	**-5**
"BAI02 Managed Requirements Definition"	18.15	13.5	**0**
"BAI03 Managed Solutions Identification and Build"	18.15	13.5	**0**
"BAI04 Managed Availability and Capacity"	25.52	18	**5**
"BAI05 Managed Organizational Change"	32.54	25.5	**-5**
"BAI06 Managed IT Changes"	26.34	19.5	**0**
"BAI07 Managed IT Change Acceptance and Transitioning"	24.79	18	**0**
"BAI08 Managed Knowledge"	27.94	19.5	**5**
BAI09 Managed Assets"	16.24	12	**0**
"BAI10 Managed Configuration"	16.24	12	**0**
"BAI11 Managed Projects"	35.26	27	**-5**
"DSS01 Managed Operations"	18.56	13.5	**0**
"DSS02 Managed Service Requests and Incidents"	30.16	21	**5**
"DSS03 Managed Problems"	25.52	18	**5**
"DSS04 Managed Continuity"	30.16	21	**5**
"DSS05 Managed Security Services"	23.2	16.5	**5**
"DSS06 Managed Business Process Controls"	18.56	13.5	**0**
"MEA01 Managed Performance and Conformance Monitoring"	16.24	12	**0**
"MEA02 Managed System of Internal Control"	16.24	12	**0**
"MEA03 Managed Compliance with External Requirements"	16.24	12	**0**
"MEA04 Managed Assurance"	16.24	12	**0**

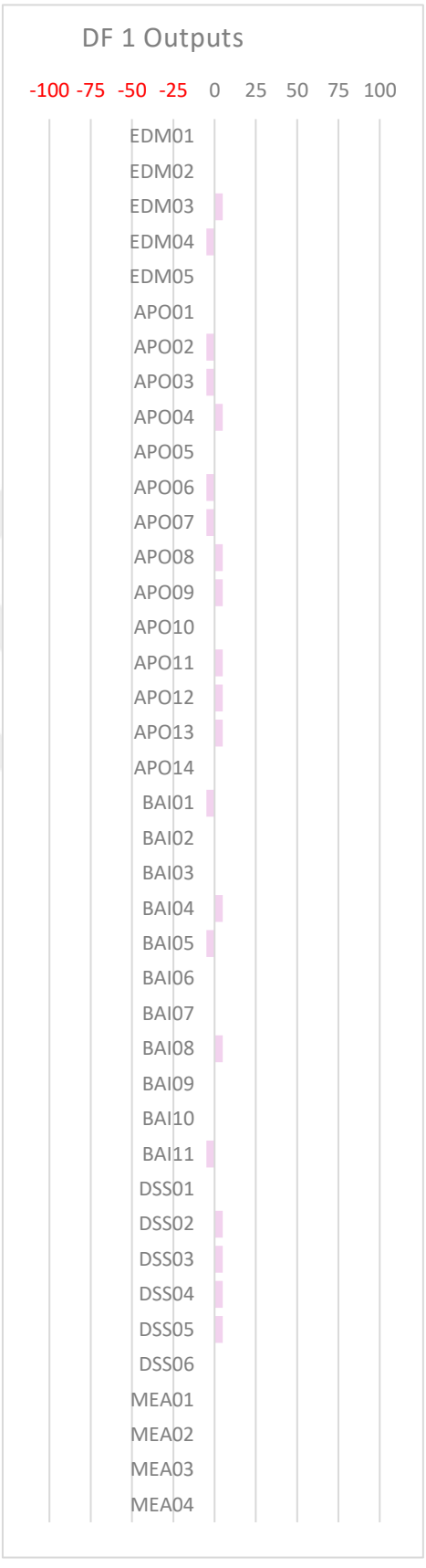


Table 3.4. shows that the sample bank's most important processes for DF 1 are;

- APO 05, "Managed Portfolio" (43.76 %)
- APO 02, "Managed Strategy" (37.6 %)
- BAI 11, "Managed Projects" (35.26 %)
- BAI 01, "Managed Programs" (34.45 %)
- EDM 02, "Ensured Benefits Delivery" (33.21 %)
- BAI 05, "Managed Organizational Change" (32.54 %)
- APO 09, "Managed Service Agreements" (32.07 %)

The sample bank's primarily focused on strategy-related domains are generally about project and portfolio management domain.

- APO 04, "Managed Innovation" (30.28 %)
- APO 03, "Managed Enterprise Architecture" (30.22 %)
- APO 08, "Managed Relationships" (30.18%)
- APO 11, "Managed Quality" (30.16%)
- DSS 02, "Managed Service Requests and Incidents" (30.16 %)
- DSS 04, "Managed Continuity" (30.16 %)

Secondarily important strategy-related processes are diverse but related to innovation and technology infrastructure.

3.1.1.2. Enterprise goals (DF 2)

Enterprise goals support business strategy; business strategy is achieved through the achievement of business goals. These objectives are defined in the Cobit framework, they are structured around the dimensions of the balanced scorecard and are defined in Table 3.55. A balanced scorecard categorization made in this DF by ISACA. Balanced scorecard is defined by Quesado et al. as "The BSC is an adequate tool to select a balanced set of indicators and objectives that reflect the strategic vision of the organization, helping organizations to meet their stakeholders' expectations, to articulate and communicate strategic objectives and to evaluate their implementation, i.e., it transforms the mission and strategic objectives into actions, allows members to communicate with each other and perceive their contribution in the scope of the organizational mission, enables improvements in the quality of the services provided and continuous feedback and learning."(Quesado et al., 2018). Kaplan and Norton created BSC and it is "a strategic management tool that links a company's current actions with its long-term goals." (Kaplan and Norton, 1993). Cobit 2019 used BSC's enterprise goals directly to its governance model. 4 dimensions and 13 goals were defined and their importance level was asked the participants in a 1-5 scaled-importance level.

Table 3.5. DF 2, enterprise goals design factor details

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

(**Source**: ISACA Cobit 2019, 2018)

Enterprise goal design factor inputs, calculation methods and outputs are given in Table 3.66.

Table 3.6. Design factor 2 inputs, calculation methods and outputs

Input	• Each of the thirteen enterprise goals must be rated between 1 (not important) and 5 (most important). • Using the generic enterprise goals, determine the most important goals for the enterprise. It is advisable to select the top three to five most important enterprise goals; too many high-priority goals will lead to less meaningful goals cascade results. • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a double matrix calculation between (1) the rated enterprise goals and the mapping table between enterprise goals and IT alignment goals, and (2) the result of the first matrix calculation and the mapping table between IT alignment goals and governance/management objectives. • The tool performs a second set of matrix calculations of a baseline set of values for Design Factor 2 *Enterprise goals*, resulting in a baseline score for each governance/management objective. • The tool then calculates the relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this sheet contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

In the proposed collaborative approach, all participants' scores were evaluated. 52 of enterprise goals results summed and calculate the mean of all of them. The design factor 2 mapping table is given in Appendix C. For DF 2 calculation method is explained detailly for EDM 01 process. All other 39 Cobit processes' relative importance levels are calculated as this method.

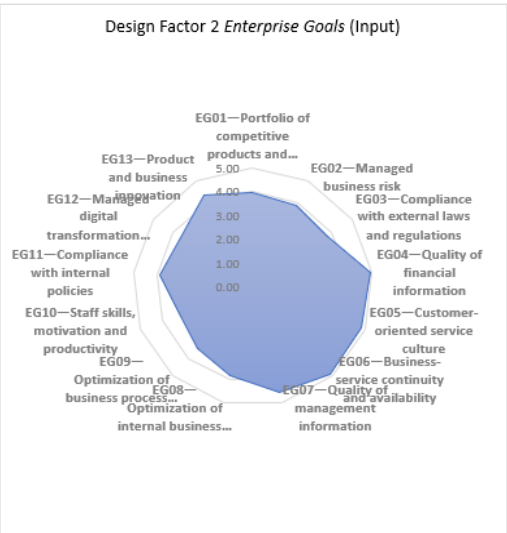
For DF 2, calculation details for example EDM 01 results are calculated with this formula; in DF2 sheet contains means of 52 survey participants' results in E6 to E18 cells in excel sheet, DF 2 map is another sheet which has constant 2 matrices defined in Appendix C detailly. In DF 2 map sheet, 2 mapping tables were created for "Mapping Table-Enterprise

Goals to Alignment Goals" and "Mapping Table-Alignment Goals to Governance and Management Objectives". The first table has 13 enterprise goals "EG" and 13 alignment goals "AG". If there is no relation with EG to AG cell got 0, it has a primary relation got 2 or "P", else secondary cell got 1 or "S". These two matrices multiplied to create final baseline matrices for calculating relevance for each Cobit process. Firstly "Mapping Table EG-GA" multiplied with EG final results. Second, this result matrices multiplied with "Mapping Table AG-GMO", this AG-GMO table contains each of "Alignment Goal" primary or secondary relation definitions. Final baseline created and inserted each Cobit processes' individual baseline score. Matrix calculation results create "Result" of each Cobit domain presented in Table 4.9. Another baseline result was calculated again for changing the possibility of the baseline of each enterprise goal. In the survey, participants did not change these baselines. The calculation formula is the same way as the individual "Result" score. After the calculating average, standard deviation and correction factor by "AVERAGE (E6:E18)"; baseline scores average of enterprise goals, "STDEVP (E6:E18)"; the standard deviation of them, and "AVERAGE (F6:F18)/ STDEVP (E6:E18)"; for correction factor. The final score is calculated with the formula of EDM 01;

"IFERROR(MROUND((F22*100*B33/C33);5)-100;0)"; F22 cell contains correction factor, B33 contains "Result" and C33 contains "Baseline Score". IFERROR stands in this formula to prevent calculation errors. This formula gives -15 to +10, (increased by 5) final results for each of Cobit processes. Importance percentage is calculated by the formula of "TRUNC(100*C48/C49)-100" with TRUNC function cell numbers truncate to get the nearest integer number in C48 cell multiplied "Mapping Table—Enterprise Goals to Alignment Goals" result for EDM 01 and C49 has baseline score. This final result shows which enterprise goals are most important for the business.

Figure 3.6 shows the results of enterprise goals collaboratively assessment. EG 04 "Quality of financial information" (4.88) and EG 05 "Customer oriented service culture" (4.84) is the most important goals.

Value	Importance (1-5)
EG01—Portfolio of competitive products and services	3.95
EG02—Managed business risk	3.86
EG03—Compliance with external laws and regulations	3.75
EG04—Quality of financial information	4.92
EG05—Customer-oriented service culture	4.84
EG06—Business-service continuity and availability	4.88
EG07—Quality of management information	4.54
EG08—Optimization of internal business process functionality	3.82
EG09—Optimization of business process costs	3.46
EG10—Staff skills, motivation and productivity	3.24
EG11—Compliance with internal policies	3.86
EG12—Managed digital transformation programs	3.66
EG13—Product and business innovation	4.36



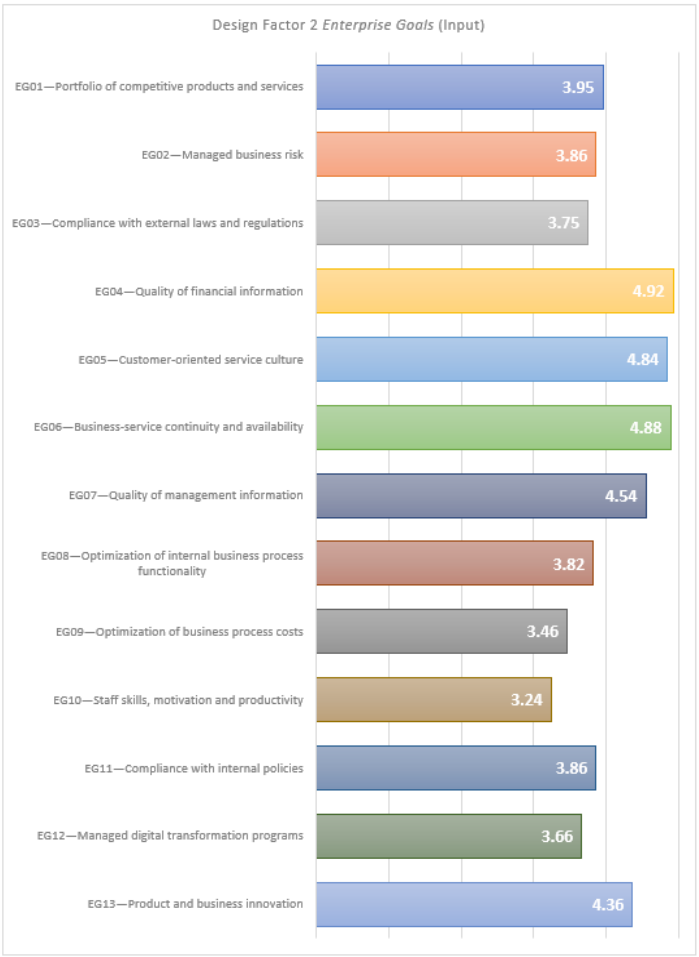


Figure 3.6. DF 2, sample bank's enterprise goals results

The sample bank's most important enterprise goal is "Quality of financial information" as a finance company is a natural result to meet. The second most important goal is "Business-service continuity and availability" to continue with a "Customer-oriented service culture". Bank's IT-related business continuity is essential, customers need 7 days and 24 hours of stable financial service in every channel. Mobile branch or ATM service stability is crucial due to the needs of customers interchangeable.

Other goals over 4 are "quality of management information" and "product and business innovation" information related to all enterprise goal is over 4, and again in design factor 1 innovation and differentiation strategy are seeing a product and business innovation is an important goal for the sample bank. Figure 3.7 shows added total effect on Cobit processes.

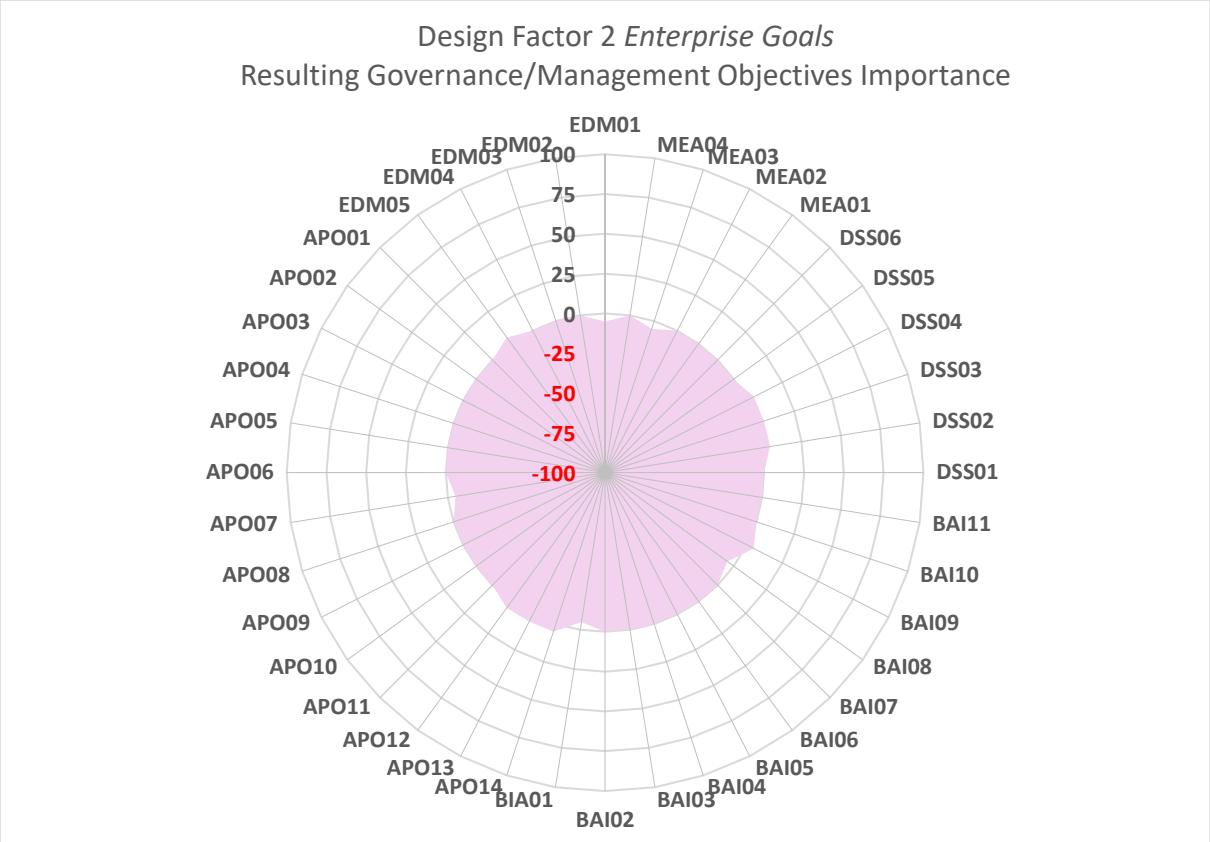


Figure 3.7. Bank's design factor 2 results for Cobit domains

Design factor 2 adds final spider map positive effect on EDM 05 "Ensured Stakeholder Engagement", APO 12 "Managed Risk", APO 13 "Managed Security", APO 14 "Managed Data", BAI 09 "Managed Assets", DSS 02 "Managed Service Requests and Incidents", DSS 03 "Managed Problems", DSS 04 "Managed Continuity" and negative effect on EDM 01 "Ensured Governance Framework Setting and Maintenance", APO 07 "Managed Human Resources", BAI 01 "Managed Programs", BAI 08 "Managed Knowledge", MEA 03 "Managed Compliance with External Requirements".

Table 3.7. DF 2, Enterprise goals governance/management objective importance results

Governance / Management Objective	Result	Baseline Score	Importance Percentage	Relative Importance
"EDM01 Ensured Governance Framework Setting and Maintenance"	130	99	41.27	-5
"EDM02 Ensured Benefits Delivery"	153.06	114	48.59	0
"EDM03 Ensured Risk Optimization"	86.74	63	27.54	0
"EDM04 Ensured Resource Optimization"	172.79	129	54.85	
"EDM05 Ensured Stakeholder Engagement"	89.68	63	28.47	5
"APO01 Managed I&T Management Framework"	241.88	180	76.79	0
"APO02 Managed Strategy"	177.31	132	56.29	-5
"APO03 Managed Enterprise Architecture"	183.91	135	58.38	-5
"APO04 Managed Innovation"	160.75	120	51.03	5
"APO05 Managed Portfolio"	189.58	141	60.18	0
"APO06 Managed Budget and Costs"	160.85	117	51.06	0
"APO07 Managed Human Resources"	143.39	108	45.52	5
"APO08 Managed Relationships"	253.97	189	80.63	5
"APO09 Managed Service Agreements"	86.52	63	27.47	5
"APO10 Managed Vendors"	106.48	78	33.8	0
"APO11 Managed Quality"	182.49	132	57.93	0
"APO12 Managed Risk"	52.44	36	16.65	5
"APO13 Managed Security"	55.06	39	17.48	5
"APO14 Managed Data"	112.04	78	35.57	5
"BAI01 Managed Programs"	171.08	129	54.31	-5
"BAI02 Managed Requirements Definition"	233.79	174	74.22	0
"BAI03 Managed Solutions Identification and Build"	222.47	165	70.63	0
"BAI04 Managed Availability and Capacity"	95.52	69	30.32	5
"BAI05 Managed Organizational Change"	243.82	183	77.4	-5
"BAI06 Managed IT Changes"	123.18	90	39.1	0
"BAI07 Managed IT Change Acceptance and Transitioning"	93.46	69	29.67	0
"BAI08 Managed Knowledge"	179.19	135	56.89	-5
"BAI09 Managed Assets"	74.06	51	23.51	5
"BAI10 Managed Configuration"	25.1	18	7.97	0
"BAI11 Managed Projects"	184.44	138	58.55	-5
"DSS01 Managed Operations"	86.52	63	27.47	0
"DSS02 Managed Service Requests and Incidents"	76.42	54	24.26	5
"DSS03 Managed Problems"	76.42	54	24.26	5
"DSS04 Managed Continuity"	76.42	54	24.26	5
"DSS05 Managed Security Services"	111.84	81	35.5	5
"DSS06 Managed Business Process Controls"	143.04	105	45.41	0
"MEA01 Managed Performance and Conformance Monitoring"	184.35	135	58.52	0
"MEA02 Managed System of Internal Control"	184.62	135	58.61	0
"MEA03 Managed Compliance with External Requirements"	49.52	39	15.72	-5
"MEA04 Managed Assurance"	152.92	111	48.55	0

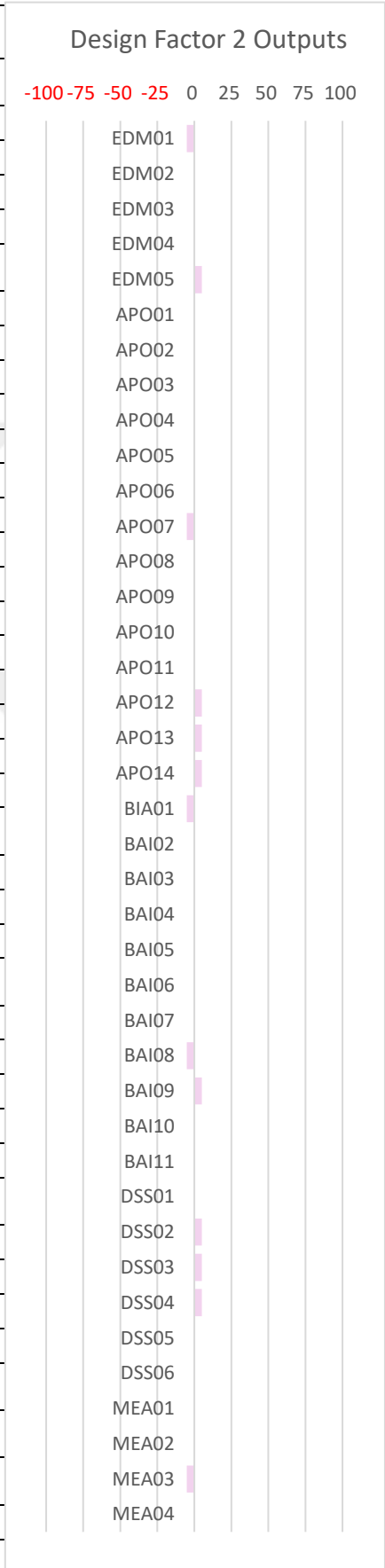


Table 3.7. shows the sample Bank's most important enterprise goal-related processes are;

1. APO 08, "Managed Relationships" (80.63 %)
2. BAI 05, "Managed Organizational Change" (77.40 %)
3. APO 01, "Managed I&T Management Framework" (76.79 %)
4. BAI 02, "Managed Requirements Definition" (74.22 %)
5. BAI 03, "Managed Solutions Identification and Build" (70.63 %)

The sample bank primarily focused on enterprise goal-related domains are generally in "Build Acquire and Implementation" domain (3 of 5). The highest-ranked "Evaluate, Direct and Monitor" domain-based process is, EDM 04 "Ensured Resource Optimization", (54.85%). Other top processes are mentioned below.

1. APO 05, "Managed Portfolio" (60.18%)
2. MEA 02, "Managed System of Internal Control" (58.61%)
3. BAI 11, "Managed Projects" (58.55%)
4. MEA 01, "Managed Performance and Conformance Monitoring" (58.52%)
5. APO 03, "Managed Enterprise Architecture" (58.38%)

Project and portfolio management processes and their monitoring is all related and aligns with the strategy again.

3.1.1.3. Risk Profile and Importance of Each Generic IT Risk Category (DF 3)

Companies define current issues and risk profiles related to I&T. IT risk profiles identify the types of risks related to I&T risks to which the company is currently exposed and indicates which areas of risk outweigh the risk appetite. Cobit evaluates 19 generic IT-related risk scenarios. Example risk scenarios about each related IT risk are given in Appendix D. Design factor 3 evaluation method is given in Table 3.8.

Table 3.8. Design factor 3 inputs, calculation methods and, outputs

Input	• Each of the 19 risk categories contained in the risk profile design factor must be rated as follows:
	  ▪ Impact of the risk should it occur, as a value between 1 (not important) and 5 (critical)
	  ▪ Likelihood of the risk to occur, as a value between 1 (very unlikely) and 5 (very likely)
	• The tool assigns a risk rating (very high, high, normal, low) to each risk category, based on the combination of the impact and likelihood ratings.
	• It is recommended to maintain sufficient spread between values.

Calculation	• The tool performs a matrix calculation of the risk ratings with the mapping table for Design Factor 3 *Risk profile*, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of risk ratings for design factor 3 with the mapping table for design factor 3, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tool contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The proposed collaborative approach gets a total score of 52 for impact and likelihood results and finding the mean of each of them. The design factor 3 mapping table is given in Appendix E Table 2. The total risk rating value is summed and then divided by the participants' count. The calculation of the final risk rating method is based on the Cobit toolkit. This gives the overall risk level of this scenario. The final results are given in Table 3.99. For DF 3 calculation method is explained detailly for EDM 01 process. All other 39 Cobit processes' relative importance levels were calculated as this method.

For DF 3, calculation details for EDM 01 results are calculated with this formula; "MMULT(DF3map! B3:T42;'DF3'!G6:G24)" DF3 sheet contains means of 52 survey participants' results in G6 to G24 cells in excel sheet, G6 calculated by E6*F6 which is the risk result of each impact and likelihood result multiplication. DF 3 map is another sheet that has constant values defined in Appendix E. In DF 3 map sheet B3 to T42 cells contains another matrix to multiply with the collaboratively created risk category's final result. Matrix calculation results create "Result" of each Cobit domain presented in Table 3.10. Another baseline result was calculated again for changing the possibility of the baseline of each risk

category. In the survey participants did not change these baselines. The calculation formula is the same way of the individual "Result" score; "MMULT(DF3map! B3:T42;'DF3'!H6:H24)" after calculating the average, standard deviation and correction factor by "AVERAGE(G6:G24)"; baseline scores average of risk category, "STDEVP(G6:G24)"; the standard deviation of them, and "AVERAGE(G6:G24)/ STDEVP(G6:G24)" ; for correction factor. The final score is calculated with the formula of;

"IFERROR(MROUND((G28*100*B35/C35);5)-100;0)"; G28 cell contains correction factor, B35 contains "Result" and C35 contains "Baseline Score". IFERROR stands in this formula to prevent calculation errors. This formula gives -30 to +30, (increased by 5) final results for each of Cobit processes.

Table 3.9. DF 3, Cobit 2019 generic risk categories and bank's impact and likelihood results

	Risk Scenario Category	Impact (1-5)	Likelihood (1-5)	Risk Rating
1	IT investment decision making, portfolio definition & maintenance	4.22	2.64	
2	Program & projects life cycle management	3.26	3.44	
3	IT cost & oversight	3.28	2.56	
4	IT expertise, skills & behavior	3.04	2.62	
5	Enterprise/IT architecture	4.42	2.84	
6	IT operational infrastructure incidents	4.46	2.96	
7	Unauthorized actions	3.46	2.60	
8	Software adoption/usage problems	4.12	3.86	
9	Hardware incidents	4.16	2.68	
10	Software failures	4.26	3.56	
11	Logical attacks (hacking, malware, etc.)	4.74	2.86	
12	Third-party/supplier incidents	3.48	3.28	
13	Noncompliance	4.64	2.84	
14	Geopolitical Issues	3.25	2.28	
15	Industrial action	1.34	1.32	
16	Acts of nature	4.25	3.26	
17	Technology-based innovation	3.36	3.38	
18	Environmental	2.30	1.54	
19	Data & information management	4.28	3.26	

	Very High Risk
	High Risk
	Normal Risk
	Low Risk

The sample bank's generic risk list consists of 2 very high risks, 11 high risks, 4 normal risks and only 2 low risks. This shows that threat landscape of the selected sector is high. Although the likelihood of all generic risks is not higher than 3.86, the impact score can be 4.74 in logical attack risk.

Software adoption and usage problems and logical attacks (hacking, malware etc.) risks are the most important generic risks in the sample bank. The least important risks are industrial action and environmental risks. Bank's design factor 3 results for Cobit domains spider map given in Figure 3.8.

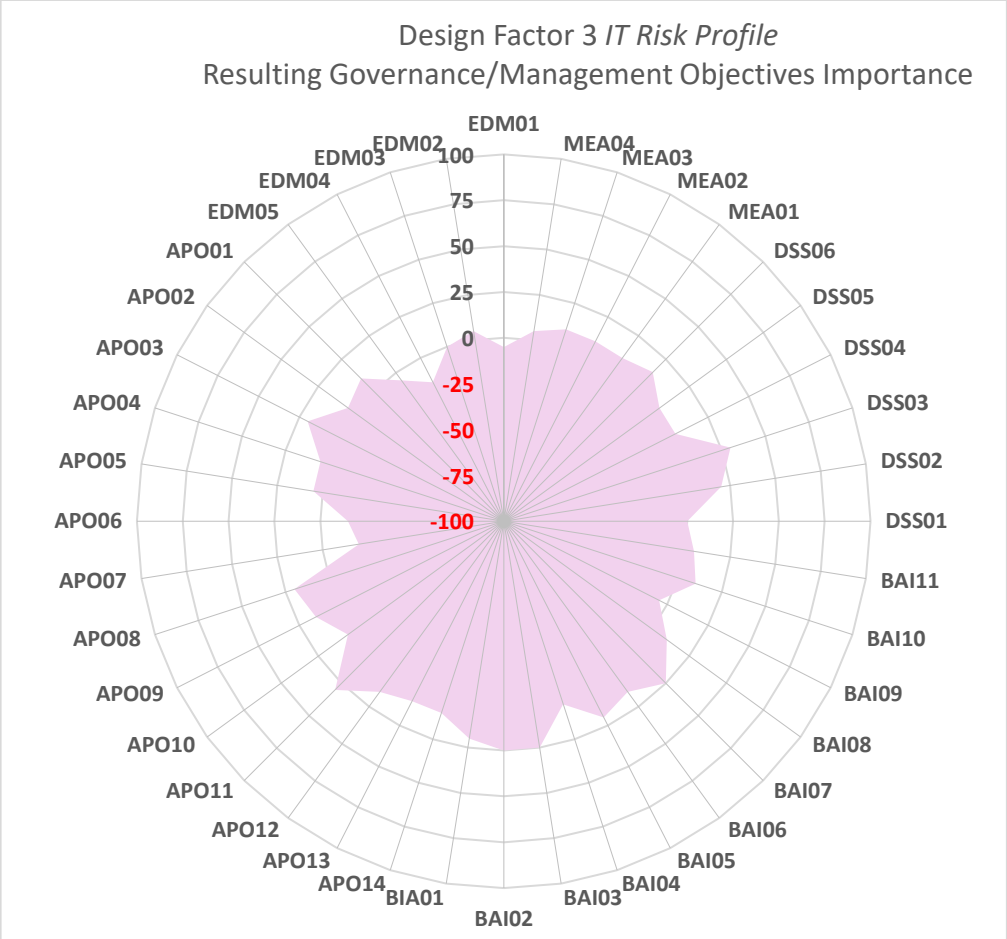
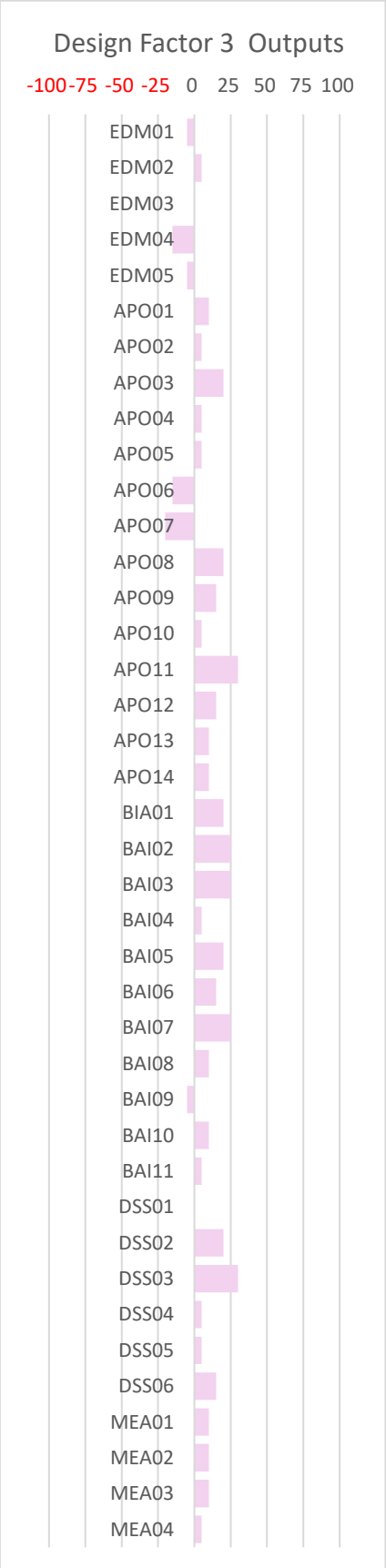


Figure 3.8. Bank's design factor 3 results for Cobit domains

DF3 adds a final spider map positive effect on every process except EDM 01 "Ensured Governance Framework Setting and Maintenance", EDM 05 "Ensured Stakeholder Engagement", BAI 09 "Managed Assets", EDM 04 "Ensured Resource Optimization", APO 06 "Managed Budget and Costs", APO 07 "Managed Human Resources". The most value-added processes are APO 11 "Managed Quality", DSS 03 "Managed Problems" by 30 points. BAI 02 "Managed Requirements Definition", BAI 03 "Managed Solutions Identification and Build", BAI 07 "Managed IT Change Acceptance and Transitioning" by 25 points. Details are given in Table 3.10.

Table 3.10. DF 3, IT risk profile governance/management objective importance results

Governance / Management Objective	Result	Baseline Score	Relative Importance
"EDM01 Ensured Governance Framework Setting and Maintenance"	211.09	189	-5
"EDM02 Ensured Benefits Delivery"	173.61	135	5
"EDM03 Ensured Risk Optimization"	197.69	162	0
"EDM04 Ensured Resource Optimization"	204.5	198	-15
"EDM05 Ensured Stakeholder Engagement"	211.15	189	-5
"APO01 Managed I&T Management Framework"	419.81	324	10
"APO02 Managed Strategy"	183.03	144	5
"APO03 Managed Enterprise Architecture"	249.14	171	20
"APO04 Managed Innovation"	57.98	45	5
"APO05 Managed Portfolio"	185.71	144	5
"APO06 Managed Budget and Costs"	156.96	153	-15
"APO07 Managed Human Resources"	211.77	216	-20
"APO08 Managed Relationships"	216.57	153	20
"APO09 Managed Service Agreements"	159.02	117	15
"APO10 Managed Vendors"	275.14	216	5
"APO11 Managed Quality"	154.02	99	30
"APO12 Managed Risk"	125.7	90	15
"APO13 Managed Security"	129.74	99	10
"APO14 Managed Data"	262.92	198	10
"BAI01 Managed Programs"	117.67	81	20
"BAI02 Managed Requirements Definition"	174.97	117	25
"BAI03 Managed Solutions Identification and Build"	176.72	117	25
"BAI04 Managed Availability and Capacity"	11.214	9	5
"BAI05 Managed Organizational Change"	101.97	72	20
"BAI06 Managed IT Changes"	188.45	135	15
"BAI07 Managed IT Change Acceptance and Transitioning"	172.97	117	25
"BAI08 Managed Knowledge"	180.18	135	10
"BAI09 Managed Assets"	40.19	36	-5
"BAI10 Managed Configuration"	133.39	99	10
"BAI11 Managed Projects"	44.858	36	5
"DSS01 Managed Operations"	158.59	135	0
"DSS02 Managed Service Requests and Incidents"	212.16	144	20
"DSS03 Managed Problems"	171.27	108	30
"DSS04 Managed Continuity"	269.25	216	5
"DSS05 Managed Security Services"	266.52	216	5
"DSS06 Managed Business Process Controls"	202.72	144	15
"MEA01 Managed Performance and Conformance Monitoring"	285.38	216	10
"MEA02 Managed System of Internal Control"	314.99	243	10
"MEA03 Managed Compliance with External Requirements"	201.34	153	10
"MEA04 Managed Assurance"	288.71	225	5



3.1.1.4. I&T Related Issues (DF 4)

Cobit 2019 defined an associated method for an I&T risk assessment and issue definition of the company, to consider what problems will occur or occurred in the past related to I&T. The most common problems/issues are defined in Table 3.111.

Table 3.11. DF 4, I&T related issues design factor

Reference	Description
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT related incidents, such as data loss, security breaches, project failure, application errors, etc. linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives or other forms of wasting resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or lack of committed business sponsors for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementations of new initiatives or innovations caused by the current IT architecture and system
O	Gap between business and technical knowledge which leads to business users and IT and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department [8]
S	Ignorance and/or noncompliance with security and privacy regulations
T	Inability to exploit new technologies or to innovate using I&T

(**Source**: ISACA Cobit 2019, 2018)

Design factor 4, I&T related issue evaluation method is given in Table 3.122.

Table 3.12. Design factor 4 inputs, calculation methods, and outputs

Input	• Each of the 20 I&T-related issues for the I&T-related issues design factor must be rated between 1 (no issue) and 3 (serious issue). Numbers 1, 2 or 3 should be keyed into the tool; the tool will then automatically translate values into a symbol, based on the tool's key for this rating. • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 4 *I&T-Related Issues* with the mapping table for design factor 4, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 4 with the mapping table for design factor 4, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The proposed collaborative approach gets 52 participants' individual issue results and scored them collectively. The importance level and participants' answer count were multiplied and added together. After calculating the total score, the mean of them is calculated. Evaluation method can be defined as if the issue has not occurred, they marked no issues, but if occurred marked as it is an issue if these occurred many times, they asses as a serious issue. The results are given in Table 3.13. DF 4 calculation method is explained detailly for the EDM 01 process. All other 39 Cobit processes' relative importance levels were calculated as this method. The cells and values differ for the related Cobit process. For DF 4, calculation details for EDM 01 results are calculated with this formula; "MMULT(DF4map!B2:U41;'DF4'!F6:F25)" DF4 sheet contains means of 52 survey participants' results in F6 to F25 cells in excel sheet, F6 is the importance level of specific IT-related issue. F6 calculation detail is given in Table 4.15. DF 4 map is another sheet that has constant values defined in Appendix F. In DF 4 map sheet B2 to U41 cells contains another matrix to multiply with collaboratively created IT-related issues' final result. Matrix calculation result creates "Result" of each Cobit domain presented in Table 3.14. Another baseline result was calculated again for changing the possibility of the baseline of each risk category. In the survey, participants did not change these baselines. The calculation formula is the same way of individual "Result" score; "MMULT(DF4map!B2:U41;'DF4'!G6:G25)" after calculating average, standard deviation and correction factor by "AVERAGE(G6:G25)"; baseline scores average of risk category, "STDEVP(G6:G25)"; the standard deviation of them, and "AVERAGE(G6:G25)/ STDEVP(G6:G25)"; for correction factor. The final score is calculated with the formula of;

"IFERROR(MROUND((J25*100*B31/C31);5)-100;0)" J25 cell contains correction factor, B31 contains "Result" and C31 contains "Baseline Score". IFERROR stands in this formula to prevent calculation errors. This formula gives -10 to +10, (increased by 5) final results for each of the Cobit processes.

Table 3.13. DF 4, I&T related issues, and bank's responses

I&T-Related Issue	No Issue	Issue	Serious Issue	Mean
Frustration between different IT entities across the organization because of a perception of low contribution to business value	14	18	20	2.11538
Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	6	22	24	2.34615
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	2	12	38	2.69231
Service delivery problems by the IT outsourcer(s)	17	32	3	1.73077
Failures to meet IT-related regulatory or contractual requirements	34	12	6	1.46154
Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	8	23	21	2.25
Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	12	22	18	2.11538
Duplications or overlaps between various initiatives, or other forms of wasted resources	11	27	14	2.05769
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	8	13	31	2.44231
IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	7	22	23	2.30769
Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	33	16	3	1.42308
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	12	28	12	2
Excessively high cost of IT	24	22	6	1.65385
Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	15	27	10	1.90385
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	29	14	9	1.61538
Regular issues with data quality and integration of data across various sources	4	14	34	2.57692
High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	22	21	9	1.75
Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)	19	24	9	1.80769
Ignorance of and/or noncompliance with privacy regulations	37	7	8	1.44231
Inability to exploit new technologies or innovate using I&T	35	12	5	1.42308

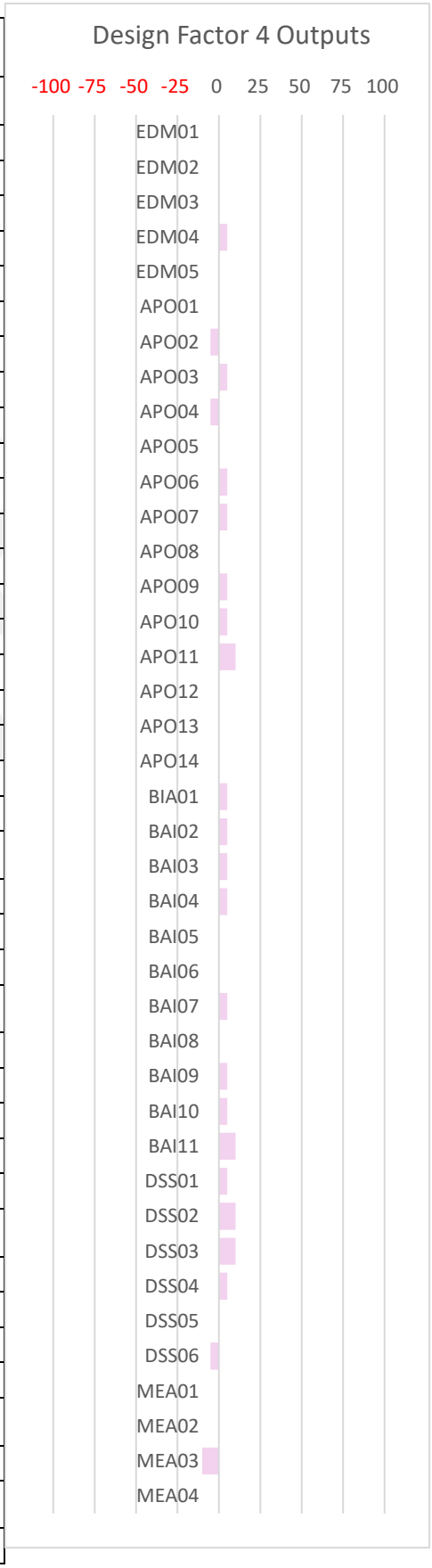
The results show that the sample bank has 2 serious issues which are "Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT" and "Regular issues with data quality and integration of data across various sources".

The banking sector gets attention from hackers. These hackers' attack types are various, they can be a denial of distributed service attacks or a malware that aims to steal information or money from banks' accounts. They can use lots of techniques to gather information like phishing, SQL Injection or cross-site scripting (XSS) attacks. There are more sophisticated attack types to go into a network and gather an administration authorization. The other important issue is data management, data quality is an important issue in every sector, especially in the finance sector. Data integration is a complex and hard issue because complex information systems have big databases and these databases have sometimes thousands of tables. These million lines of information are used to generate meaningful information or wisdom. Sometimes in this process complexity creates lots of integration problems. The value of data could be various in different tables and if this occurs the reports which are about this data cannot be integrated with other data sources. Data integration is crucial to creating effective customer relationship management, reporting mechanisms and effective oversight of governing body. Bank has 8 other issues. They are listed with the importance level;

- "Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction"
- "Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or perception of low contribution to business value"
- "IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget"
- "Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems"
- "Frustration between different IT entities across the organization because of a perception of low contribution to business value"
- "Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets"
- "Duplications or overlaps between various initiatives, or other forms of wasted resources"
- "Complex IT operating model and/or unclear decision mechanisms for IT-related decisions" (ISACA, 2018).

Table 3.14. DF 4, I&T related issues governance/management objective importance results

Governance / Management Objective	Result	Baseline Score	Relative Importance
"EDM01 Ensured Governance Framework Setting and Maintenance"	68.06	70	**0**
"EDM02 Ensured Benefits Delivery	68.54	70	**0**
"EDM03 Ensured Risk Optimization"	45.465	47	**0**
"EDM04 Ensured Resource Optimization"	67.205	67	**5**
"EDM05 Ensured Stakeholder Engagement"	39.48	41	**0**
"APO01 Managed I&T Management Framework"	54.86	56	**0**
"APO02 Managed Strategy"	47.595	50	**-5**
"APO03 Managed Enterprise Architecture"	66.37	66	**5**
"APO04 Managed Innovation"	29.45	32	**-5**
"APO05 Managed Portfolio"	66.99	68	**0**
"APO06 Managed Budget and Costs"	63.175	62	**5**
"APO07 Managed Human Resources"	47.77	47	**5**
"APO08 Managed Relationships"	67.365	70	**0**
"APO09 Managed Service Agreements"	45.01	43	**5**
"APO10 Managed Vendors"	39.415	39	**5**
"APO11 Managed Quality"	45.525	43	**10**
"APO12 Managed Risk"	50.83	52	**0**
"APO13 Managed Security"	32.825	33	**0**
"APO14 Managed Data"	59.915	60	**0**
"BAI01 Managed Programs"	36.31	35	**5**
"BAI02 Managed Requirements Definition"	51.205	51	**5**
"BAI03 Managed Solutions Identification and Build"	42.855	41	**5**
"BAI04 Managed Availability and Capacity"	23.875	23	**5**
"BAI05 Managed Organizational Change"	27.835	28	**0**
"BAI06 Managed IT Changes"	41.955	42	**0**
"BAI07 Managed IT Change Acceptance and Transitioning"	39.005	38	**5**
"BAI08 Managed Knowledge"	30.145	31	**0**
"BAI09 Managed Assets"	23.29	23	**5**
"BAI10 Managed Configuration"	25.185	25	**5**
"BAI11 Managed Projects"	48.415	45	**10**
"DSS01 Managed Operations"	28.025	27	**5**
"DSS02 Managed Service Requests and Incidents"	35.48	33	**10**
"DSS03 Managed Problems"	33.85	32	**10**
"DSS04 Managed Continuity"	21.375	21	**5**
"DSS05 Managed Security Services"	28.675	29	**0**
"DSS06 Managed Business Process Controls"	26.845	29	**-5**
"MEA01 Managed Performance and Conformance Monitoring"	60.01	61	**0**
"MEA02 Managed System of Internal Control"	46.865	48	**0**
"MEA03 Managed Compliance with External Requirements"	26.06	29	**-10**
"MEA04 Managed Assurance"	57.785	58	**0**



These I&T-related issues add relative importance to Cobit domains as shown in Table 4.9. Positive 10 points affects APO 11 “Managed Quality” and BAI 11 “Managed Projects” processes. Other affected processes can be seen in the table. Fist 4 domains’ final results are mentioned in Figure 3.9. Scores give the importance level of Cobit’s related processes. Detailed information is given in the final canvas.

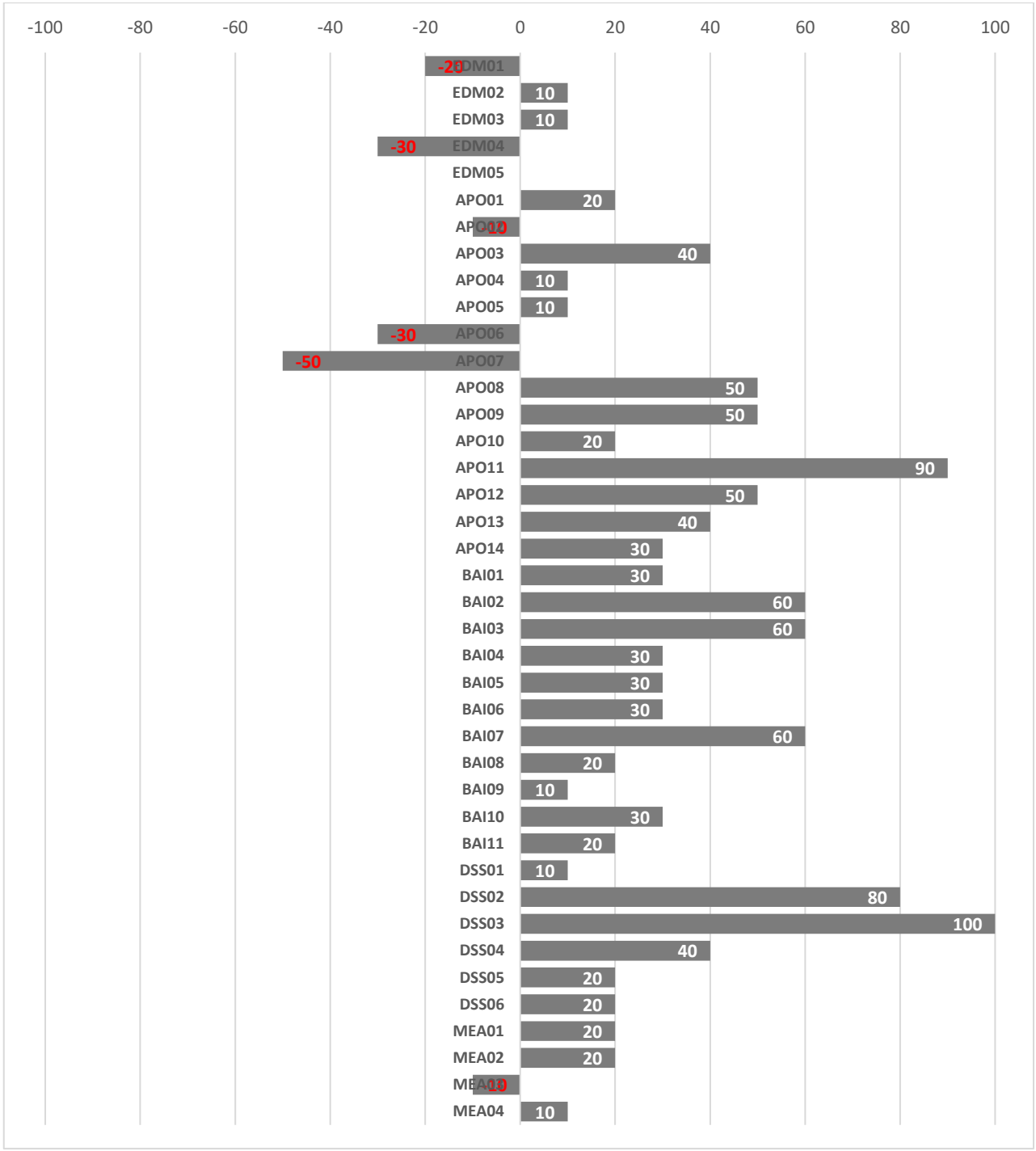


Figure 3.9. The initial design for governance and management objectives importance

3.1.1.5. Threat Landscape (DF 5)

After designing the first four design factors, this results created the initial scope of tailored the governance system. With DF 5 and other next design factors, Cobit refined the scope of governance system. The threat landscape is like a sector and geography in which the company operates under the rule. These can be classified as shown in Table 3.155.

Table 3.15. DF 5, threat landscape design factor

Threat Landscape	Explanation
Normal	The enterprise is operating under what are considered normal threat levels
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

(**Source**: ISACA Cobit 2019, 2018)

Threat landscape inputs, calculation methods and outputs are given in Table 3.166.

Table 3.16. Design factor 5 inputs, calculation methods, and outputs

Input	• Each of the two possible values (high and normal) for the threat landscape design factor must be rated between 0% and 100%. The sum of both values must be 100%. • For many enterprises, 100% will be assigned to one of the categories. The option is available to assign percentages where a portion of enterprise operations is subject to a high threat landscape, while others are subject to a more normal threat landscape.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 5 *Threat landscape* with the mapping table for design factor 5, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 5 with the mapping table for design factor 5, resulting in a baseline score for each governance/management objective. • The tool then calculates the relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The sample bank's results for the IT threat landscape are depicted in Figure 3.10. This figure shows that sample bank's IT threat landscape is high 82%, normal 18%.

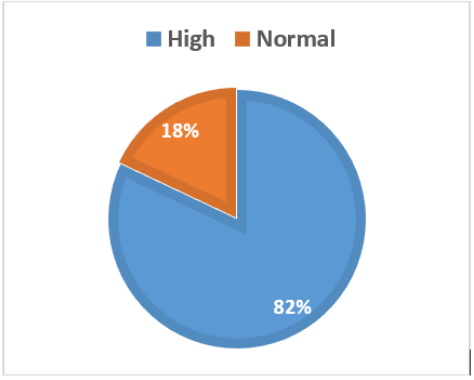


Figure 3.10. DF 5, IT threat landscape results

For DF 5, calculation details for EDM 1 results are calculated with this formula; “MMULT(DF5map!B2:C41;'DF5'!B7:B8)” DF5 sheet contains means of 52 survey participants’ results in C7 and C8 cells in excel sheet, C7 is high-level threat landscape ratio, C8 is normal level threat landscape ratio. DF 5 map is another sheet that has constant values defined in Appendix G. In DF 5 map sheet B2 to C41 cells contains another matrix to multiply with collaboratively created IT threat landscape’s final result. Matrix calculation results create baseline calculation formula in the same way as individual “Result” score; “MMULT(DF5map!B2:C41;'DF5'!D7:D8)” In DF 5 again average, standard deviation and correction factor calculated. Final relative importance is calculated with the formula; “IFERROR(MROUND((100*B30/C30);5)-100;0))” B30 cell contains the “Score”, C30 contains “Baseline Score”. IFERROR stands in this formula to prevent calculation errors. This formula gives -10 to +10, (increased by 5) final results for each of Cobit processes.

Final relative results -10 points of 17 different Cobit processes and -5 points for 7 processes are affected. There are no positive effects on other processes.

3.1.1.6. Compliance Requirements (DF 6)

The compliance requirements to which the company is subject may be classified according to the categories listed in Table 3.17.

Table 3.17. DF 6, compliance requirements design factor

Regulatory Environment	Explanation
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher than average compliance requirements, most often related to industry sector or geopolitical conditions.

(**Source**: ISACA Cobit 2019, 2018)

Compliance Requirements design factor inputs, calculation methods and outputs are given in Table 3.18.

Table 3. 18. Design factor 6 inputs, calculation methods, and outputs

Input	• Each of the three possible values for the compliance requirements design factor must be rated between 0% and 100%. The sum of all three values must be 100%. • For many enterprises, 100% will be assigned to one of the categories. However, the option is available to assign different percentages, if the enterprise's IT landscape is quite vast, and certain parts are subject to strict compliance regulation, while other parts are subject to less strict regulation.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 6 *Compliance Requirements* with the mapping table for design factor 6, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 6 with the mapping table for design factor 6, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

In the proposed collaborative approach, every participant's result percentage is added for each compliance requirements level. All score levels of every category percentage calculated by the mean of them. The final total level percentage score is again 100%.

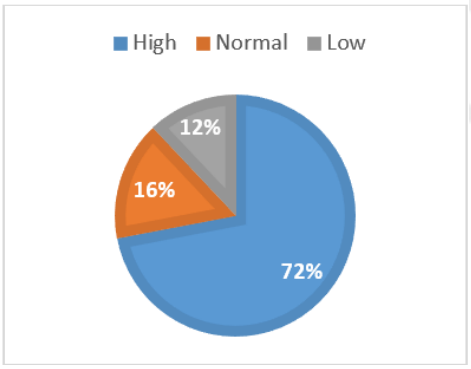


Figure 3. 11. DF 6, compliance requirements result

The sample bank's results for design factor 6 compliance requirements are depicted in Figure 3. **11**1. This figure shows the selected bank's compliance requirement is high at 72%, normal at 16%, and low at 12%.

For DF 6, calculation details for EDM 1 results are calculated with this formula; "MMULT(DF6map!B2:D41;'DF6'!B7:B9) DF6 sheet contains means of 52 survey participants' results in C7, C8, and C9 cells in excel sheet, C7 is high Importance level of compliance requirements ratio, C8 is normal, C9 is low level. DF 6 map is another sheet that has constant values defined in Appendix H. In DF 6 map sheet B2 to D41 cells contain another matrix to multiply with collaboratively created IT threat landscape's final result matrices. Matrix calculation results create baseline calculation formula in the same way as

individual “Result” score; “MMULT(DF6map!B2:D41;'DF6'!D7:D9)” in DF 6 again average, standard deviation and correction factor calculated. Final relative importance is calculated with the formula; “IFERROR(MROUND((100*B30/C30);5)-100;0)” B30 cell contains the “Score”, C30 contains “Baseline Score”. IFERROR stands in this formula to prevent calculation errors. This formula gives 0 to +50, (increased by 5) final results for each of the Cobit processes.

Final relative results show 12 different Cobit processes increase more than 15 percent, others are not affected. There are no negative effects on other processes. DSS 05 “Manage Security Services” process increased relatively +50 in this step.

3.1.1.7. Role of IT (DF 7)

The role of IT in the company can be classified as shown in Table 3.19. DF 7, the role of IT design factor details.

Table 3.19. DF 7, the role of IT design factor details

Role of IT[9]	Explanation
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency of IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

(**Source**: ISACA Cobit 2019, 2018)

The role of IT design factor inputs, calculation methods, and outputs are given in Table 3.20. In the proposed collaborative approach, every participant’s result is added for each role of its type. All score levels of every role in IT category are calculated by the mean them.

Table 3.20. Design factor 7 inputs, calculation methods, and outputs

Input	• Each of the four possible values for the role of IT design factor—support, factory, turnaround and strategic—must be rated between 1 (not important) and 5 (most important). • It is recommended to maintain sufficient spread between values.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 7 *Role of IT* with the mapping table for design factor 7, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 7 with the mapping table for design factor 7, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The role of IT results is given in Figure 3.12. It can be seen that every role is evaluated as important but the most important role is strategic, second important role is the factory. It can be implied that IT organizations create values for the business itself and are critical for innovating the organization's processes. In the banking sector If IT fails there is an immediate impact as service continuity disruption, the IT processes must keep running to maintain all other processes of the bank.

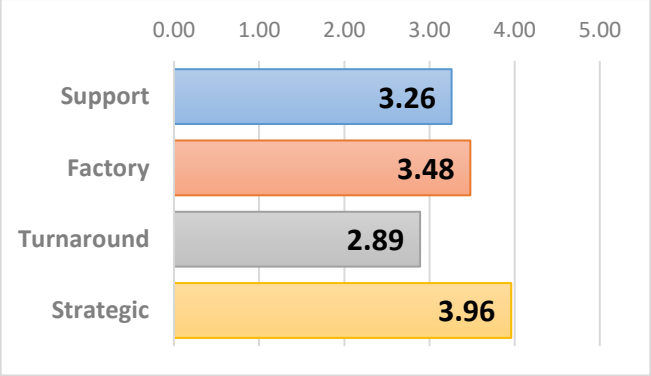


Figure 3.12. DF 7, the role of IT results

For DF 7, calculation details for EDM 1 results are calculated with this formula; "MMULT(DF7map!B2:E41;'DF7'!B6:B9)" DF7 sheet contains means of 52 survey participants' results in C6, C7, C8 and C9 cells in excel sheet, C6 is support, C7 factory, C8 turnaround, and C9 is the strategic role of IT levels ratio. DF 7 map is another sheet that has constant values defined in Appendix I. In DF 7 map sheet B2 to E41 4* 41 matrix cells contain another constant to multiply with collaboratively created IT role final result matrix. Baseline calculation formula creation is the same way as individual "Result" score; "MMULT(DF7map!B2:E41;'DF7'!D6:D9)" in DF 7 again average, standard deviation, and correction factor calculated. Final relative importance is calculated with the formula; "IFERROR(MROUND((B13*100*B32/C32);5)-100;0)" B32 cell contains the "Score", C32 contains; "Baseline Score". IFERROR stands in this formula to prevent calculation errors. This formula gives 0 to +50, (increased by 5) final results for each of the Cobit processes.

Final relative results show all the Cobit processes increase more than 5 percent. There are no negative effects on any processes. APO 04 "Managed Innovation", APO 12 "Managed Risk" and APO 13 "Managed Security" increased by more than 20%.

3.1.1.8. Sourcing Model for IT (DF 8)

The sourcing model for IT is the supplier supply model (sourcing) that the company adopts can be classified as shown in Table 3.21.

Table 3.21. DF 8, sourcing model for IT design factor details

Sourcing Model	Explanation
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for their own IT staff and services.
Hybrid	A mixed model is applied, combining the three models above in varying degrees.

(**Source**: ISACA Cobit 2019, 2018)

The sourcing model for IT design factor inputs, calculation methods, and outputs are given in Table 3.22. In this design factor, the exact values of sourcing ratios are used.

Table 3.22. Design factor 8 inputs, calculation methods, and outputs

Input	• Each of the three possible values for the sourcing model for IT design factor—outsourcing, cloud and insourcing—must be rated between 0% and 100%. The sum of all three values must be 100%. • Note that there is a fourth category—the hybrid classification. This is not denoted in the tool, because, by definition, assigning percentages to more than one of the other three values creates a hybrid model.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 8 *Sourcing Model for IT* with its corresponding mapping table, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 8 with the mapping table for design factor 8, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The sample banks sourcing model is insourced 90%, outsourcing is only 10%. There is no cloud or hybrid type sourcing. Results are depicted in Figure 3.13.

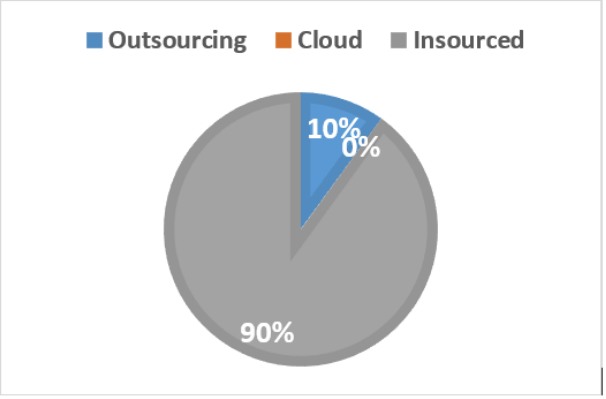


Figure 3.13. DF 8, IT sourcing model results

For DF 8, calculation details for EDM 1 results are calculated with this formula; “MMULT(DF8map!B2:D41;'DF8'!B6:B8)” DF8 sheet contains means of 52 survey participants’ results in C6, C7, C8 cells in excel sheet, C6 is outsourcing, C7 cloud, C8 insourced version of sourcing model of IT. DF 8 map is another sheet that has constant values defined in Appendix J. In DF 8 map sheet B2 to D41 3* 40 matrix cells contain another constant to multiply with collaboratively created IT role final result matrix. Baseline calculation formula creation is the same way of individual “Result” score; “MMULT(DF7map!B2:E41;'DF7'!D6:D9)” in DF 8 again average, standard deviation and correction factor calculated. Final relative importance is calculated with the formula of; “IFERROR(MROUND((100*B32/C32);5)-100;0) B32 cell contains the “Score”, C32 contains “Baseline Score”. IFERROR stands in this formula to prevent calculation errors.

Final relative results show 5 of Cobit process decrease by more than 15 percent. There are no positive effects on any processes. APO 09 “Managed Service Agreements”, APO 10 “Managed Vendors” decreased by more than 15%.

3.1.1.9. IT Implementation Methods (DF 9)

IT implementation methods are the company’s working style that can be adaptable in every process. These can be classified as shown in Table 3.23.

Table 3.23. DF 9, IT implementation methods design factor details

IT Implementation Method	Explanation
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach towards software development (waterfall) and separates software development and operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as “bimodal IT.”

(**Source**: ISACA Cobit 2019, 2018)

IT Implementation Methods design factor inputs, calculation methods and outputs are given in Table 3.24.

Table 3.24. Design factor 9 inputs, calculation methods, and outputs

Input	• Each of the three possible values for the IT implementation methods design factor—Agile, DevOps and traditional—must be rated between 0% and 100%. The sum of all three values must be 100%. • Note that there is a fourth category—the hybrid classification. This is not denoted in the tool, because, by definition, assigning percentages to more than one of the other three values creates a hybrid model.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 9 *IT Implementation Methods* with the mapping table for design factor 9, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 9 with the mapping table for design factor 9, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output section of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

In the proposed collaborative approach every participant's result percentage was added for each implementation method's level and then calculated the mean of them. The final total level percentage score is again 100%.

The sample bank's results for IT implementation methods are depicted in Figure 3.14. This figure shows that sample bank mostly using traditional - waterfall 74%, devops 16% and agile only 10%.

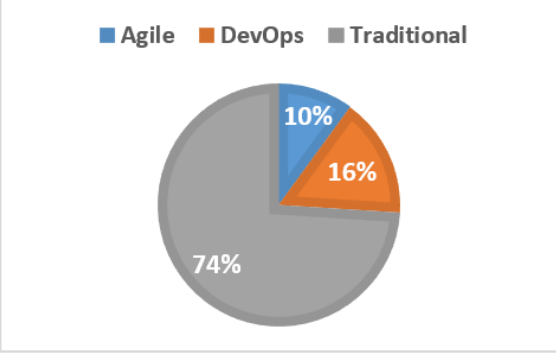


Figure 3.14. DF 9, IT implementation methods results

Nowadays, IT implementation methods evolve from traditional to agile. Also, DevOps (development operations) and DevSecOps (Development security operations) methods started to use. These methods create efficiency and creativity in processes. Waterfall or traditional processes still creates values but to adapt to compliance or emerging risks it is important to be agile. For DF 9, calculation details for EDM 1 results are calculated with this formula; "MMULT(DF9map! B2:D41;'DF9'!B6:B8)" DF9 sheet contains means of 52 survey participants' results in C6, C7, C8 cells in excel sheet, C6 is agile, C7 devops, C8

traditional version of IT implementation methods. DF 9 map is another sheet that has constant values defined in Appendix K. In “DF 9 map” sheet B2 to D41 3* 40 matrix cells contain another constant to multiply with collaboratively created IT implementation methods final result matrix. Baseline calculation formula creation is the same way as individual “Result” score; “MMULT(DF9map!B2:D41;'DF9'!D6:D8)” in DF 9 again average, standard deviation and correction factor calculated. Final relative importance is calculated with the formula of; “IFERROR(MROUND((100*B29/C29);5)-100;0)” B29 cell contains the “Score”, C29 contains “Baseline Score”. IFERROR stands in this formula to prevent calculation errors.

Final relative results show 15 of Cobit process increase more than 10 percent. There are no negative effects on any processes. BAI 03 “Managed Solutions Identification & Build”, DSS 01 “Managed Operations” increased by more than 20%.

3.1.1.10. Technology Adoption Strategy (DF 10)

Technology adoption strategies can be classified as shown in Table 3.25.

Table 3.25. DF 10, technology adoption strategy design factor details

Technology Adoption Strategy	Explanation
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technology to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with their adoption of new technologies.

(**Source**: ISACA Cobit 2019, 2018)

Technology adoption strategy design factor inputs, calculation methods and outputs are given in Table 3.26. In the proposed collaborative approach, every participant’s result percentage was added for each technology adoption strategies level and then calculated the mean of them. The final total level percentage score is again 100%.

Table 3.26. Design factor 10 inputs, calculation methods, and outputs

Input	• Each of the three possible values for the technology adoption strategy design factor—first mover, follower, slow adopter—must be rated between 0% and 100%. The sum of all three values must be 100%. • For many enterprises, 100% may be assigned to one of the categories. However, the option is available to assign different percentages, if the enterprise's IT landscape is quite vast, and different areas adopt technology at difference paces.
Calculation	• The tool performs a matrix calculation of the entered values for Design Factor 10 *Technology Adoption Strategy* with the mapping table for design factor 10, resulting in a score for each governance/management objective. • The tool performs a second matrix calculation of a baseline set of values for design factor 10 with the mapping table for design factor 10, resulting in a baseline score for each governance/management objective. • The tool then calculates a relative importance for each governance/management objective as the relative difference between both sets of values, expressed as a percentage and rounded to 5. This number can be positive or negative, indicating that a governance/management objective is more or less important when compared to the baseline score.
Output	• The output of this tab contains the calculated relative importance of each of the 40 COBIT® 2019 governance and management objectives. • The results are represented in table format, as a bar chart and as a spider diagram.

(**Source**: ISACA Cobit 2019, 2018)

The sample bank's results for the technology adoption strategy are depicted in Figure 3.15. This figure shows that sample bank adapts technology as a "follower" 44%, "slow adopter" 24% and "first mover" 32%.

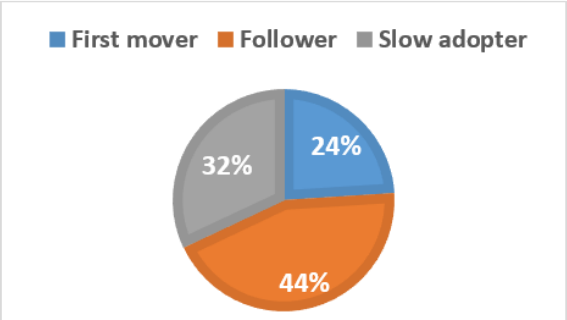


Figure 3.15. DF 10, technology adoption strategy results

This design factor result shows that the sample bank technology adoption strategy is based mostly on "follower" 44%. Other strategies are total score higher than "follower", second high percentage is "slow adapter". As a bank, being a first mover in technology is not possible for some reasons. Technology changes fast and it needs some stability before wide usage. For example, cloud technologies started to use in lots of sectors but in the banking sector due to some compliance requirements, cloud usage is limited or requires permission from a regulation authority.

Another example of slow adoption can be related to infrastructure needs. System stability and security are important issues as mentioned before. Some technologies create fast transactions or glad customers but they may be insecure or unstable. There are lots of

samples to be a slow adapter or a follower. Due to these conditions, the sample bank's first-mover strategy is 24%. For DF 10, calculation details for EDM 1 results are calculated with this formula; "MMULT(DF10map!B2:D41;'DF10'!B6:B8)" DF10 sheet contains means of 52 survey participants' results in C6, C7, C8 cells in excel sheet, C6 is first mover, C7 follower, C8 slow adapter version of technology adoption strategy. "DF 10 map" is another sheet that has constant values defined in Appendix L. In "DF 10 map" sheet B2 to D41 3* 40 matrix cells contains constants to multiply with collaboratively created IT implementation methods final result matrix. Baseline calculation formula creation is the same way as individual "Result" score; "MMULT(DF10map!B2:D41;'DF10'!D6:D8)" in DF 10 again average, standard deviation and correction factor calculated. Final relative importance is calculated with the formula of; "=IFERROR(MROUND((100*B22/C22);5)-100;0)" B22 cell contains the "Score", C22 contains "Baseline Score". IFERROR stands in this formula to prevent calculation errors.

Final relative results show 28 of Cobit process increase more than 5 percent. There is only 1 negative effects on a process (APO 06 "Managed Budget & Costs"). 11 of 40 processes are not affected by this factor. APO 07 "Managed Human Resources", APO 08 "Managed Relationships", APO 03 "Managed Enterprise Architecture" increased by more than 10%.

3.1.2. All Design Factors (Final Evaluation)

After assessing all DFs results a relative importance score was added to every Cobit process and these created a final importance map depicted in Figure 3.16. A final canvas was created for every DF's importance factor and its relativity to the final map and these three figures are assessed together. Figure 3.17 and 3.18. shows figure 3.16's details.

The final figure explained the critical sequence of processes. Sample bank's most important (need to be more mature) processes are;

- DSS 05—"Managed Security Services", 100%*
- DSS 04—"Managed Continuity", 95%
- APO 12—"Managed Risk", 90%
- APO 13—"Managed Security", 90%*
- EDM 03—"Ensured Risk Optimization", 85%
- MEA 03—"Managed Compliance with External Requirements", 80%
- MEA 04—"Managed Assurance", 80%

* DSS05 "Managed Security Services" and APO 13 "Managed Security" are different processes in Cobit. DSS 05 "Managed Security" is about "Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance

with the security and privacy policy. Establish and maintain information security and privacy roles and access privileges. Perform security monitoring." and APO 13 "Managed Security" define, operate and monitor a system for information security and privacy management." Its objective is "Keep the impact and occurrence of information security and privacy incidents within the enterprise's risk appetite levels." (ISACA, 2018) DSS domain processes are generally about the operations or service detail, APO domain is more about planning, organizing, and governance.

In every domain design factor were processed to build the GRC model. Sample bank defined "Deliver Service and Support" domains' two processes are evaluated for the most important processes to govern. Security services and continuity related to other processes followed by other domains. ISACA defines "Managed Security Services" processes' main objective as "Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security and privacy policy. Establish and maintain information security and privacy roles and access privileges. Perform security monitoring." And "Managed Continuity" processes objective is "Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain the availability of resources, assets and information at a level acceptable to the enterprise." (ISACA, 2018) These two processes are the most important processes and need to be more mature.

"Align, plan and organize" domain's two related processes are defined as 90% percent important. Results are aligned and mutually support each other. Risk management and security operation management processes cover all compliance requirements and security policies/baselines to implement, this governs banks as more secure and stable. These domains' main objectives are, "Managed Risk"; "Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management." and "Managed Security"; "Define, operate and monitor a system for information security and privacy management." (ISACA, 2018)

After these 4 processes an "Evaluate, Direct and Monitor" domain process "Ensured Risk Optimization" comes in a queue, in this process the bank governs risks and levels of ensured risk levels are within a tolerable limit. This EDM process' main objective is "Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed." (ISACA,

2018) Finally, there are 2 “Monitor Evaluate and Assess” processes with the importance of 80%. These processes are important to highly regulated sectors like the sample bank’s compliance domain. ISACA defined “Managed Compliance with External Requirements” processes objective as “Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance.” and “Managed Assurance” as “Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities” (ISACA, 2018).

Also, the least important processes for the sample bank were defined, this does not mean these processes are not important, this means they have managed these processes and they are mature enough and there are little or no gap between the desired level and as it is. These processes are;

- APO 06—"Managed Budget & Costs”, -15%
- EDM 04—"Ensured Resource Optimization”, -5%
- APO 02—"Managed Strategy”, -5%
- APO 04—"Managed Innovation”, -5%
- APO 05—"Managed Portfolio”, 0%
- APO 09—"Managed Service Agreements”, 0%
- BAI 11—"Managed Projects”, 0%

These processes and other all 40 process objectives are given in Appendix M. Negative values, relative importance values from design factors, and in some cases, negative results can result in a negative total score. This situation is normal and it is stated that adjustments can be made by the Cobit design guide and toolkit. All the results in the final canvas by stating the reasons can be passed through the adjustment (between -100 and +100) process. It was considered that it would be more reasonable to maintain the negative results instead of operating this process, which is a subjective approach and can be carried out by a single IT governor. The survey participants were asked whether they wanted to make adjustment by conveying the final canvas results, and they were asked not to change the results. Only 4 participants wanted to update their results for 2 design factors. The updated factors were DF 5 "IT threat landscape" and DF 7 "Importance of Role of IT".

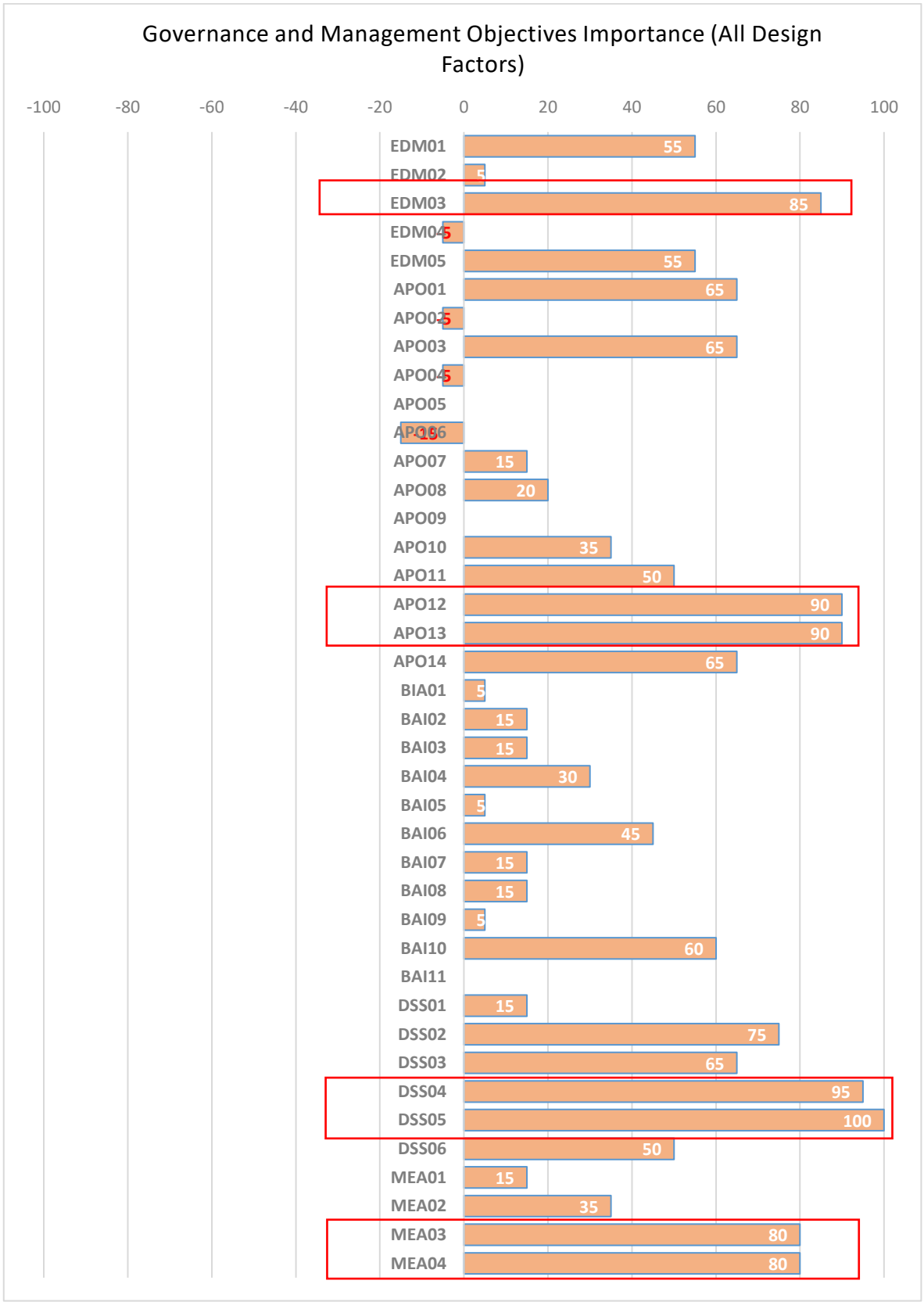


Figure 3.16. All design factors governance and management objectives importance (Highest scored processes are enclosed in red boxes)

	DF1	DF2	DF3	DF4		DF5	DF6	DF7	DF8	DF9	DF10	
	Step 2: Determine the initial scope of the Governance System					Step 3: Refine the scope of the Governance System						
Design Factors:	Enterprise Strategy	Enterprise Goals	Risk Profile	IT-Related Issues	Initial Scope: Governance/ Management Objectives Score	Threat Landscape	Compliance Req's	Role of IT	Sourcing Model for IT	IT Implementation Methods	Technology Adoption Strategy	Refined Scope: Governance/ Management Objectives Score
Weight	1	1	1	1		1	1	1	1	1	1	
EDM01—Ensured Governance Framework Setting & Maintenance	0	-5	-5	0	-20	60	30	5	0	0	-5	55
EDM02—Ensured Benefits Delivery	0	0	5	0	10	0	0	0	0	0	0	5
EDM03—Ensured Risk Optimization	5	0	0	0	10	75	65	5	-25	0	5	85
EDM04—Ensured Resource Optimization	-5	0	-15	5	-30	0	0	5	0	0	0	-5
EDM05—Ensured Stakeholder Engagement	0	5	-5	0	0	35	35	5	0	0	5	55
APO01—Managed I&T Management Framework	0	0	10	0	20	60	20	5	0	0	0	65
APO02—Managed Strategy	-5	0	5	-5	-10	0	0	0	0	0	-5	-5
APO03—Managed Enterprise Architecture	-5	0	20	5	40	60	0	0	0	5	10	65
APO04—Managed Innovation	5	0	5	-5	10	0	0	0	0	0	-10	-5
APO05—Managed Portfolio	0	0	5	0	10	0	0	0	0	0	-5	0
APO06—Managed Budget & Costs	-5	0	-15	5	-30	0	0	5	0	0	-10	-15
APO07—Managed Human Resources	-5	-5	-20	5	-50	35	0	0	0	5	10	15
APO08—Managed Relationships	5	0	20	0	50	0	0	0	0	0	5	20
APO09—Managed Service Agreements	5	0	15	5	50	35	0	0	-55	0	-5	0
APO10—Managed Vendors	0	0	5	5	20	60	35	0	-55	0	0	35
APO11—Managed Quality	5	0	30	10	90	35	0	0	0	0	-5	50
APO12—Managed Risk	5	5	15	0	50	75	65	5	-35	5	-5	90
APO13—Managed Security	5	5	10	0	40	75	35	5	0	0	0	90
APO14—Managed Data	0	5	10	0	30	60	20	5	0	0	-5	65

Figure 3.17. Cobit total DF's canvas result for "Evaluate Direct & Monitor" (EDM) and "Align, Plan and Organize" (APO) domains

	DF1	DF2	DF3	DF4		DF5	DF6	DF7	DF8	DF9	DF10	
	Step 2: Determine the initial scope of the Governance System					Step 3: Refine the scope of the Governance System						
Design Factors:	Enterprise Strategy	Enterprise Goals	Risk Profile	IT-Related Issues	Initial Scope: Governance/ Management Objectives Score	Threat Landscape	Compliance Req's	Role of IT	Sourcing Model for IT	IT Implementation Methods	Technology Adoption Strategy	Refined Scope: Governance/ Management Objectives Score
Weight	1	1	1	1		1	1	1	1	1	1	
BAI01—Managed Programs	-5	-5	20	5	30	0	0	0	0	0	-5	5
BAI02—Managed Requirements Definition	0	0	25	5	60	0	0	0	0	-5	-5	15
BAI03—Managed Solutions Identification & Build	0	0	25	5	60	0	0	0	0	0	-5	15
BAI04—Managed Availability & Capacity	5	0	5	5	30	35	0	0	0	0	-5	30
BAI05—Managed Organizational Change	-5	0	20	0	30	0	0	5	0	-5	-5	5
BAI06—Managed IT Changes	0	0	15	0	30	60	0	5	0	-5	-5	45
BAI07—Managed IT Change Acceptance and Transitioning	0	0	25	5	60	0	0	0	0	0	-5	15
BAI08—Managed Knowledge	5	-5	10	0	20	0	0	5	0	0	5	15
BAI09—Managed Assets	0	5	-5	5	10	0	0	5	0	0	0	5
BAI10—Managed Configuration	0	0	10	5	30	60	0	5	0	5	5	60
BAI11—Managed Projects	-5	0	5	10	20	0	0	0	0	-5	-5	0
DSS01—Managed Operations	0	0	0	5	10	0	0	5	0	10	0	15
DSS02—Managed Service Requests & Incidents	5	5	20	10	80	60	0	5	0	5	0	75
DSS03—Managed Problems	5	5	30	10	100	35	0	5	0	5	5	65
DSS04—Managed Continuity	5	5	5	5	40	75	35	5	0	0	5	95
DSS05—Managed Security Services	5	0	5	0	20	60	70	5	0	0	5	100
DSS06—Managed Business Process Controls	0	0	15	-5	20	60	0	5	0	0	0	50
MEA01—Managed Performance and Conformance Monitoring	0	0	10	0	20	60	0	5	-50	0	-5	15
MEA02—Managed System of Internal Control	0	0	10	0	20	35	0	5	0	0	0	35
MEA03—Managed Compliance with External Requirements	0	-5	10	-10	-10	60	65	0	0	0	0	80
MEA04—Managed Assurance	0	0	5	0	10	60	50	5	0	0	0	80

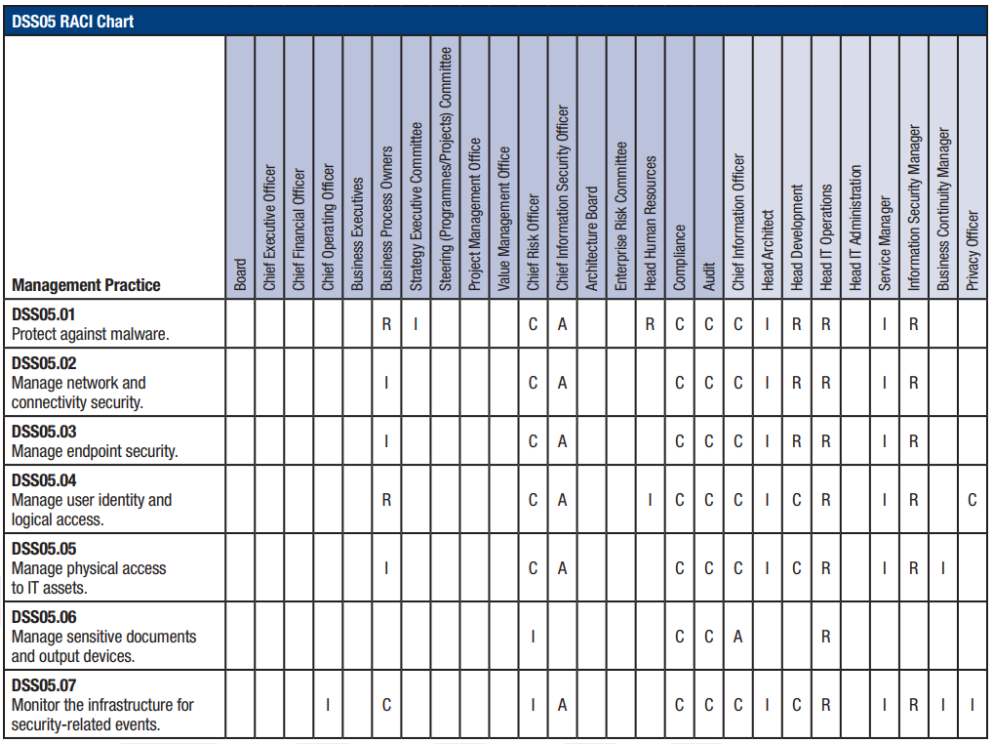
Figure 3.18. Cobit total DF's canvas result for Build, "Acquire and Implement" (BAI), "Deliver Service and Support" (DSS) and "Monitor Evaluate and Assess" (MEA) domains

To create a GRC model, Cobit's 40 processes importance heat map was created. After coloring all processes, due to each processes' importance score Figure 3.21. GRC model for the sample bank created. The coloring schema is based on Microsoft Excel heat map property. Scales or colors can differentiate and importance level of each process which is required to evaluate depending on the specific business governing body's decision. In the sample bank regulation related to any Cobit practices taken into account due to regulation, obligation comes from the regulatory authority. According to the created model sample bank can evaluate which processes or process groups are more mature, or need to be more mature. In addition, Cobit makes another comment about this result as the importance level of the related Cobit process is in a higher score or vice versa. Cobit has 1202 practices spread over 40 processes for businesses (mentioned actions in Cobit) to gain more maturity in IT processes. DSS 05's details are given from Cobit 5 for the sample bank's most important process to be mature as an example. DSS 05 IT-related goals and their related metrics are defined by ISACA and depicted in Figure 3.19.

DSS05 Manage Security Services	**Area: Management** **Domain: Deliver, Service and Support**
Process Description Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.	
Process Purpose Statement Minimise the business impact of operational information security vulnerabilities and incidents.	
The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
04 Managed IT-related business risk	• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Percent of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
10 Security of information, processing infrastructure and applications	• Number of security incidents causing financial loss, business disruption or public embarrassment • Number of IT services with outstanding security requirements • Time to grant, change and remove access privileges, compared to agreed-on service levels • Frequency of security assessment against latest standards and guidelines

Figure 3.19. DSS 05 IT-related goals and its metrics
(**Source**: ISACA Cobit 2019, 2018)

Cobit's every process has this type of process description, objectives, goals, metrics and also responsibility assignment matrix (RACI charts) to implement in their business. The figure shows DSS 05's all related sub-processes and their RACI ("R" for responsible, "A" for accountable, "C" for consulted, "I" for informed) chart as a sample depicted in Figure 3.20.



DSS05 RACI Chart																									
Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Figure 3.20. DSS 05's subprocesses and RACI chart
(**Source**: ISACA Cobit 2019, 2018)

Also, every Cobit domain has actions to implement, DSS 05'has 50 actions. To give an example DSS 05.01 has 5 actions given in Table 3.27.

Table 3.27. DSS 05.01 action list

Action no	Action Detail
DSS 05.01.1	"Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically)."
DSS 05.01.2	"Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails)."
DSS 05.01.3	"Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software."
DSS 05.01.4	"Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management."
DSS 05.01.5	"Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories)."

(**Source**: ISACA Cobit 2019, 2018)

The final IT GRC model is depicted in Figure 3.21 and with the help of it, the bank can create an action plan. To show an example DSS 05's action list is given in Appendix N. After creating this model, the relations with IS regulation with the help of LSA analysis are defined.

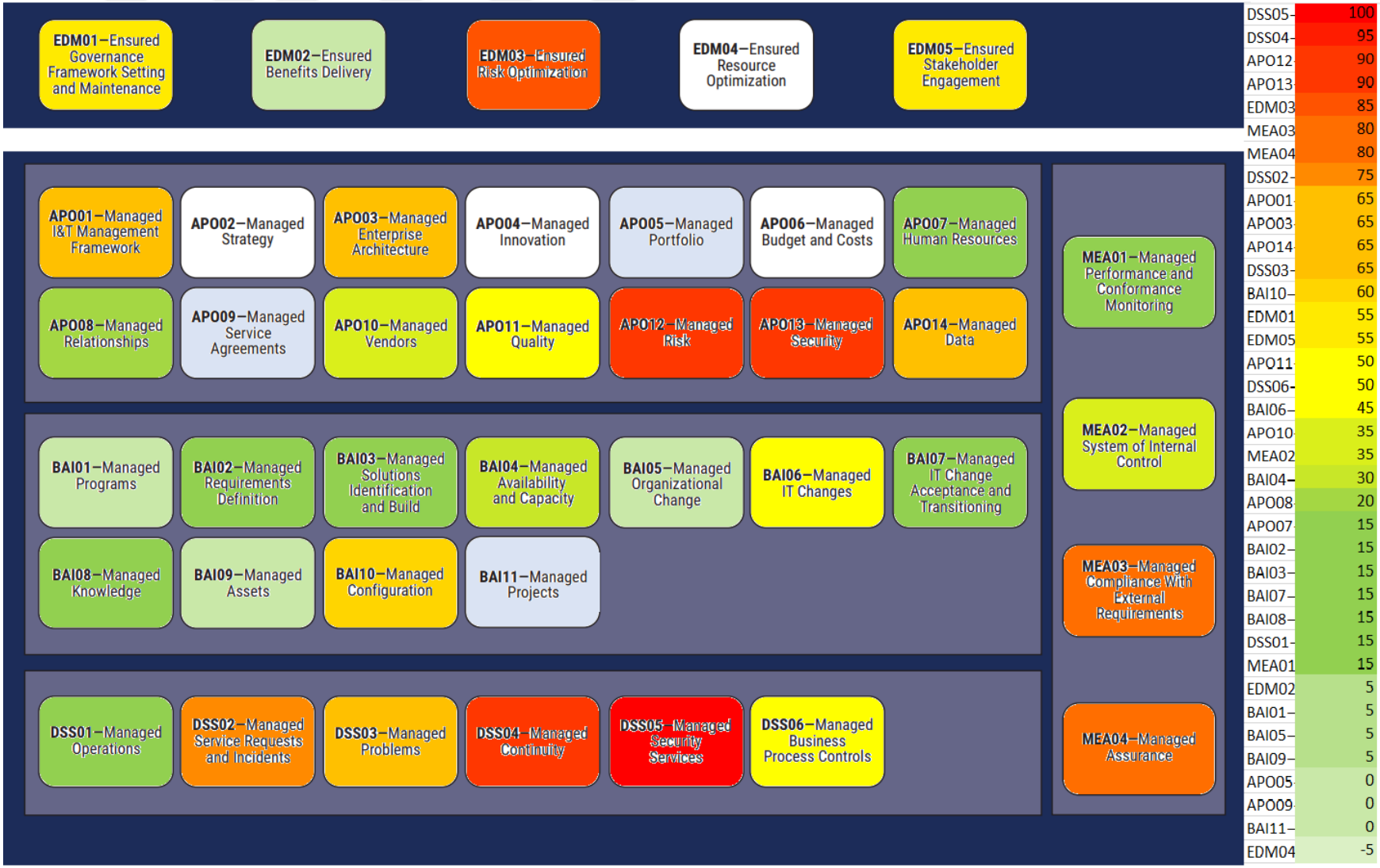


Figure 3.21. Final IT GRC model for the sample bank based on Cobit 2019

3.2. Latent Semantic Analysis

In the third phase latent semantic analysis was made to an IT regulation's compliance requirements to defined Cobit activities. To create a relatedness map, semantic word meaning finding and creating relatedness percentage creation method LSA was used (Kurniawan and Surendro, 2018). Finding relations between two texts is semantic analysis. There are various ways to find relatedness between texts or paragraphs but the most meaningful and scientific method is LSA- "Latent Semantic Analysis". (Bellegarda and Jerome, 2006; Ampazis and Perantonis, 2004, Dumanis, 1993; Dumanis 1995)

LSA is kind of a neural language processing subset of automatic language processing methods based on a predefined word-to-word relatedness maps which named corpus. According to Landauer and Foltz "Latent Semantic Analysis (LSA) is a theory and method for extracting and representing the contextual-usage meaning of words by statistical computations applied to a large corpus of text. The underlying idea is that the totality of information about all the word contexts in which a given word does and does not appear provides a set of mutual constraints that largely determines the similarity of meaning of words and set of words to each other. The adequacy of LSA's reflection of human knowledge has been established in a variety of ways." (Landauer and Foltz 1998). Another definition is "LSA is a mathematical/statistical technique for extracting and representing the similarity of meaning of words and passages by analysis of large bodies of text. It uses singular value decomposition, a general form of factor analysis, to condense a very large matrix of word-by-context data into a much smaller, but still large-typically 100-500 dimensional-representation" (Deerwester et al., 1990).

For a computer to be able to evaluate texts in terms of content, it should have a sufficient degree of verbal intelligence and semantic knowledge. This is an unsolved problem research in the field of artificial intelligence, but various methods have been developed whose goal is the representation of text content on the computer (Lemaire and Denhière, 2004; Landauer et al., 2007). The most prominent way is latent semantic analysis (LSA) (Deerwester et al., 1990). This is an automatic language processing technique with regard to the content comparison of text content, partial aspects of word meanings. LSA can simulate semantic knowledge sufficiently well. It enables the relationship to be analyzed between words based on their common occurrence. It is a pure one statistical approach, the word relationships based on co-occurrences are automatically extracted without specifying rule systems in

advance or entering dictionaries. Generation of semantic spaces; the starting point of the LSA is text collections, with the text material usually in paragraphs split up (hereinafter referred to as the document). The ones saved in the documents Information about word relationships can be represented abstractly in a frequency matrix, where the columns contain the individual documents and the lines contain the different words. In the research regulations, every action and Cobit practice would be documents and terms. In this thesis, one to many approaches were used which is stated on Colorado University LSA website. (“Latent Semantic Analysis at CU”, 2021)

The frequency of occurrence of a word in a specific document specifies the relatedness, this uses large corpora of natural language, then this frequency matrix is very sparse. The Frequency matrix already contains all information about word relationships. It has been defined by Colorado University. In selected documents, texts there are usually too big to be able to carry out unnecessary information ("noise"). To eliminate the "background noise", reducing the information contained in the frequency matrix to the core content there is a necessary step. It is needed to create a filter of potentially superfluous words, application of weighting functions the cell frequencies, singular value decomposition, and determination of the optimal number Dimensions (Lenhard et al., 2007).

In the first step, potentially unnecessary words are excluded. These include high-frequency words that do not convey any specific information ("stop words", e.g. Prepositions, conjunctions, articles, etc.), as well as words that appear very rarely, for example, less than three times in the entire text corpus. This reduces the number of different one’s words clearly.

In documents, there are lots of IT-related abbreviations, they needed to be completely changed with the help of a word-by-word processor. For example, required changes to all “IT” abbreviated words changed to “information technology”. Cobit has lots of prepositions on it like, “eg.”, “ex.”, “aka.” or abbreviations like “I&T”, “decision-making”, “IT-enabled or (IT-something else)”, “enterprise’”, “stakeholder’”, apostrophe or hyphen words are converted. Cobit gives examples on bracelets, these are deleted. Also, sometimes the example of a topic may be related to the document but it can affect the main area or direction and relatedness. So, the data was cleared with these examples from actions and Cobit practices. This data cleaning process and evaluation of all related data increase the similarity ratio if any.

Next, LSA has a weighting function and it is applied to the cell frequencies. These results with log-entropy and weighting, probably produce the best results (Nakov, Popova, and Mateev, 2001), when a word is clumped locally occurs and is therefore specific to a particular context. Equally common words that are spread out, there are weakened the relation because they are not specific to transport information. In the sample, there are lots of special IT terms, so if they can be cleared or deleted, the meaning would not change. Lastly, the filtered and weighted matrix becomes one singular value decomposition (SVD), similar to factor analysis. While If the covariance matrix is broken down during a factor analysis, the matrix is taken with the LSA the weighted frequencies of occurrence. In both cases, there are two orthogonal matrices and a diagonal matrix, which again result in the starting matrix by multiplication. Factor analysis is applied to the various variables of a sample of objects, so a matrix is created with the factor values of the individual objects on the various extracted dimensions (factors) (Lenhard et al., 2007).

Furthermore, a diagonal matrix with the sorted eigenvalues of the Dimensions and a matrix of the factor loading of the variables. In the LSA, one is created in the same way Word matrix with the factor values of the words, a matrix of the sorted singular values and a document matrix (Figure. 3.22, for a mathematical description, see Berry, Dumais, and O'Brien, 1995; Martin, and Berry, 2007).

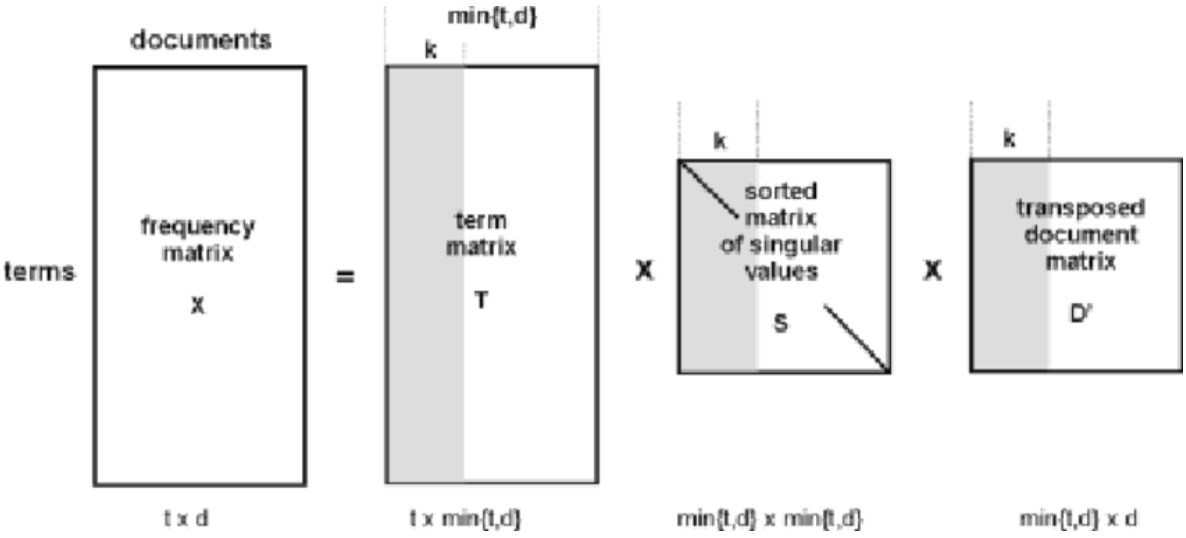


Figure 3.22. LSA method

(**Source**: Berry, Dumais, and O'Brien, 1995)

By reducing the number of dimensions of the sub-matrices, "background noises" go to the raw matrix are lost and a simple structure with the essential information of the output matrix is created. Since the singular value decomposition in the LSA on weighted raw values, the level of the singular values cannot be interpreted, so a priori no meaningful criterion for the number of dimensions can be established. Values around the 300 dimensions have proven to be optimal, with the recommendations being different authors vary between 100 and 1500 dimensions (Dumais, 1990; Graesser et al., 1999; Nakov, 2000; Wild, Stahl, Stermsek, and Neumann, 2005).

By reducing the dimensions, space is ultimately established in which words after their common occurrences with other words are distributed. The “place” of a word in space (to be vector) represents that part of its content that is related to its common use manifested in other words (hence latent semantic analysis). Accordingly, are not only represented adjacent words that are often used together, but also words that are never directly together but often together with the same other words can be used (higher-order relationships), (Lemaire, and Denhière, 2004; Kontostathis, and Pottenger, 2002). This applies to synonyms, for example, most of which are not occur together, but are usually used in the same context. The same goes for Single and plural nouns and inflections of verbs. (Lenhard et al., 2007)

A semantic space can be called n-dimensional Vector representation of word and text meanings are viewed: Each word gets through its factor values a coordinate in this space and thus a vector with a certain direction and length. The direction is an analog to the subject matter of the word, whereas the Length of the vector reflects its semantic content.

Finding synonyms or distinguishing between subordinate and generic terms and capture negations. It is therefore also inadmissible for LSA-based similarity calculations to be equated with human association structures (Landauer, Foltz, and Laham, 1998). There are numerous fields of application in which they are successful in simulation human language comprehension skills that could be applied. These include the;

- automatic evaluation of articles (Landauer, Laham, Rehder and Schreiner, 1997),
- evaluation of the coherence and comprehensibility of texts (Foltz, Kintsch, and Landauer, 1998),
- prediction of the Learning success when reading a text based on the prior knowledge of the reader and selection of suitable learning material (Wolfe et al., 1998),

- successful passing of multiple-choice knowledge tests such as B. the "Test of English as a Foreign Language" (Landauer and Dumais, 1997),
- intelligent learning systems that provide feedback on the content of text summaries (Wade-Stein and E. Kintsch, 2004).

The LSA does not provide a valid semantic simulation of knowledge and verbal intelligence, but it is a good approximation of a number of application areas. (Lenhard, Baier, Hoffmann, and Schneider, 2007)

Other fields that LSA can implement; (Dumais, 2004) Information discovery (eDiscovery, Government/Intelligence Community, 2007).

- Automated document classification (eDiscovery, Government/Intelligence community, Publishing) (Sedona, 2007)
- Text summarization (eDiscovery, Publishing) (Gong and Lui, 2001)
- Relationship discovery (Government, Intelligence community, Social Networking) (Bradford, 2005)
- Automatic generation of link charts of individuals and organizations (Government, Intelligence community) (Bradford, 2005)
- Matching technical papers and grants with reviewers (Government) (Yarowsky and Florian, 1999)
- Online customer support (Customer Management) (Caron, 2000)
- Determining document authorship (Education) (Soboroff, 1997)
- Automatic keyword annotation of images (Monay, Gatica-Perez, 2003)
- Understanding software source code (Software Engineering) (Maletic and Marcus, 2000)
- Filtering spam (System Administration) (Gee, K, 2003)
- Information visualization (Landauer, Laham, 2004)
- Essay scoring (Education) (Foltz et al.,1999)
- Literature-based discovery (Gordon and Dumais, 1998)
- Stock returns prediction (Ramiro et al., 2017)
- Dream Content Analysis (Psychology) (Altszyler, et al., 2017)

This approach can also implement in the compliance relatedness finding side. A compliance or regulation relatedness map can also use to show which articles are related to which domains. As a result, in which actions were taken by the management created beneficial improvements in which domains. The process flow of latent semantic analysis can be illustrated as shown in Figure 3.23.

Figure 3.23. LSA method flowchart

Final similarity scores are between 0,00 -1,00, a score, such 0,78 represents two inputs similarity is 78%. Determining the lower limit of the sample that can be examined may differ according to the examiner and his purpose. In this similarity display, there is no inference that a certain threshold above or below is low similarity. The focus is on the excess or the low similarity ratio (Gomaa and Fahmy, 2013; Sarkar et al. 2014; Islam and Hoque, 2010).

3.2.1. Compliance Map with Latent Semantic Analysis

In literature, Cobit 5 mapped to lots of IT-related standards like ISO 27001, ITIL, TOGAF ("The Open Group Architecture Framework") or NIST series by different methods. Some uses manual text search ways to compare all the clauses and their meanings. This way is suitable for a lightweight standard. In Table 3.28 NIST Cyber Security standard mapped by Cobit by manually.

Table 3.28. Cobit-NIST cyber security framework map

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

(Source: NIST Cyber Security Framework and other References Map by Nicole Keller, 2018)

Cobit 2019 and ITIL v4 map were created manually by two dimensions. Well covered 60% and above and less than this percentage. They mapped only main domains to each other, they do not assess their objectives or practices to each other. Figure 3.24. is a sample. ITIL is a widely using another best practice in the IT management area. Especially in IT service management has lots of good practices. General, service management and technical domains have 34 processes to govern IT with the business. This mapping is important for Cobit or ITIL implemented businesses. If they needed to comply with Cobit or ITIL and they have already used one of these, they can use such a relation map to understand their domain or process relation.

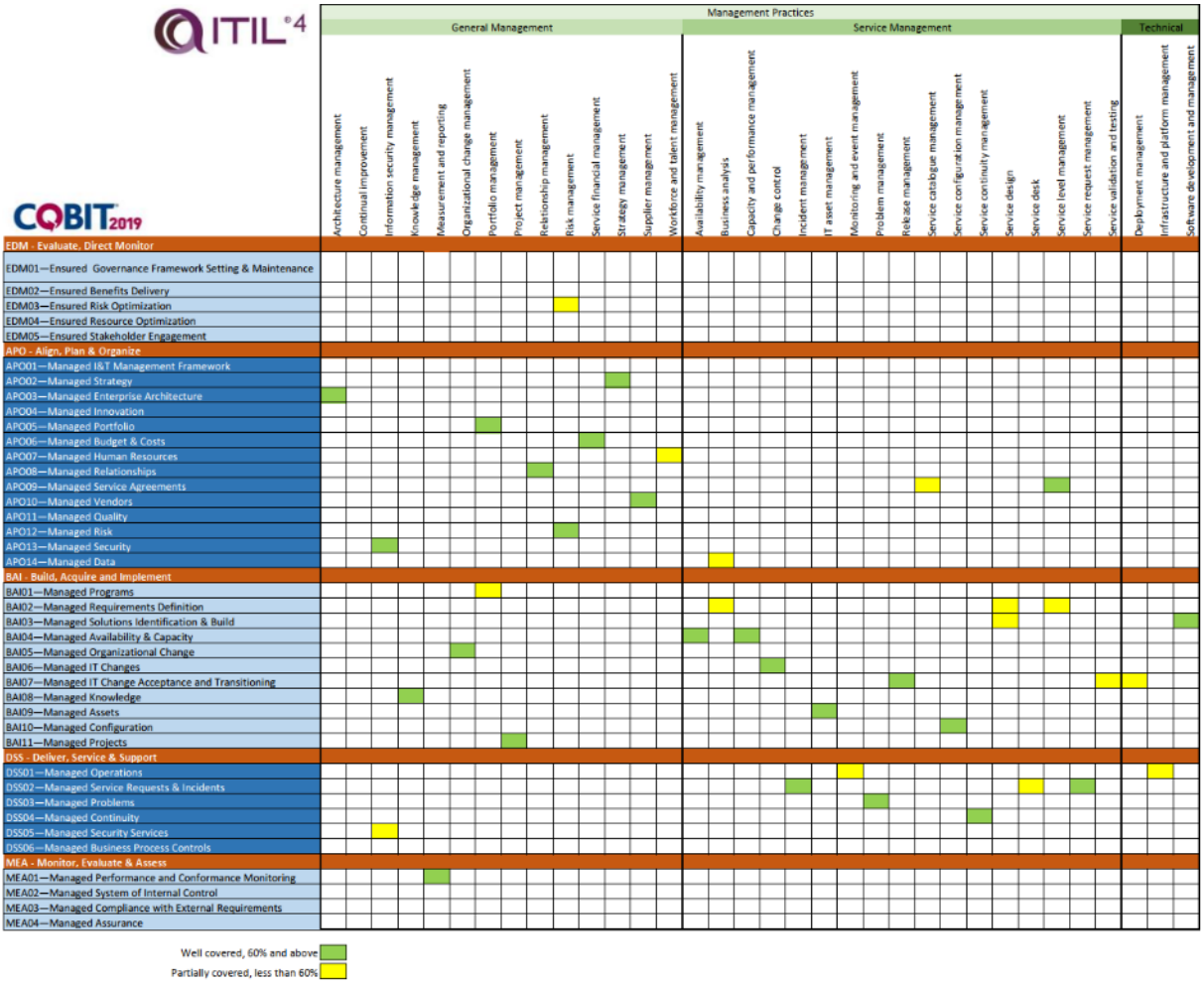


Figure 3.24. Cobit 2019 to ITIL v4 relatedness map
(**Source:** Glenfis ITIL4-COBIT2019 Mapping v1.0, 2020)

Another way to map standards is to use a definition language and semantic analysis to find the relatedness of all the clauses, especially ArchiMate is an UML-like algorithmic modelling language used in some researches. ArchiMate samples for ISO standards relatedness with Cobit are given in Figure 3.25 and Figure 3.26. In literature, it is seen that some domain-to-domain relatedness map too. Not a whole standard relatedness map but a partial status to research. Figure 3.26. is a sample of Cobit DSS02 to ISO 33072 map made by ArchiMate. Also, Balanced Score Card (BSC) is used to map best practices. With financial, customer, internal business, learning and growth categories/perspectives, IT BSC dimension information and technology-related goals are mapped with a selected best practice's IT related goals. For example, Cobit 5 to ISO 27001 mapped with this technique (Oparaugo, 2014). Each goals categorized subjectively and matrices each cell ranked with zero relation, primary or secondary level relation. Calculation method has not published on a scientific paper, only shared via ISACA's website.

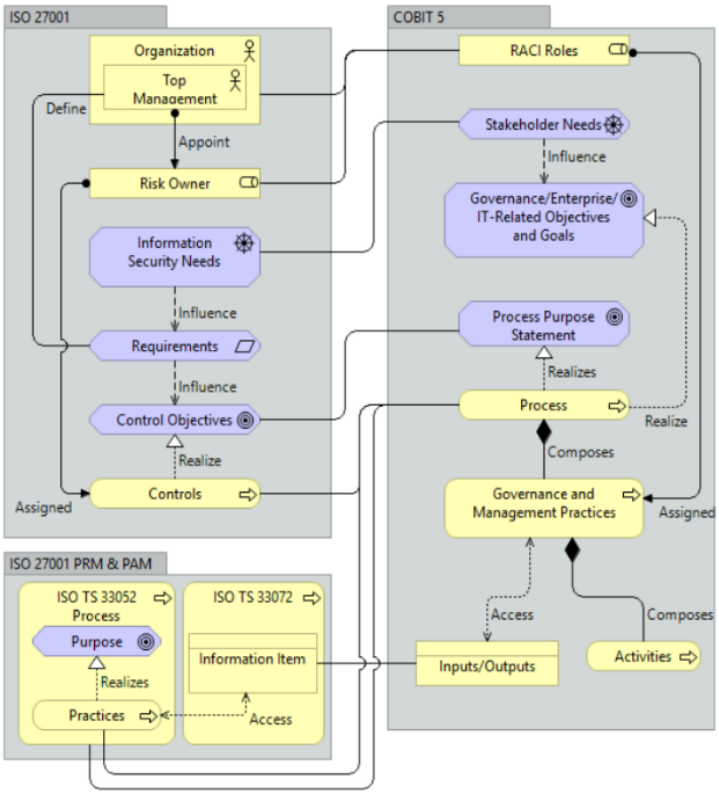


Figure 3.25. Cobit-ISO 27001 maps with ArchiMate

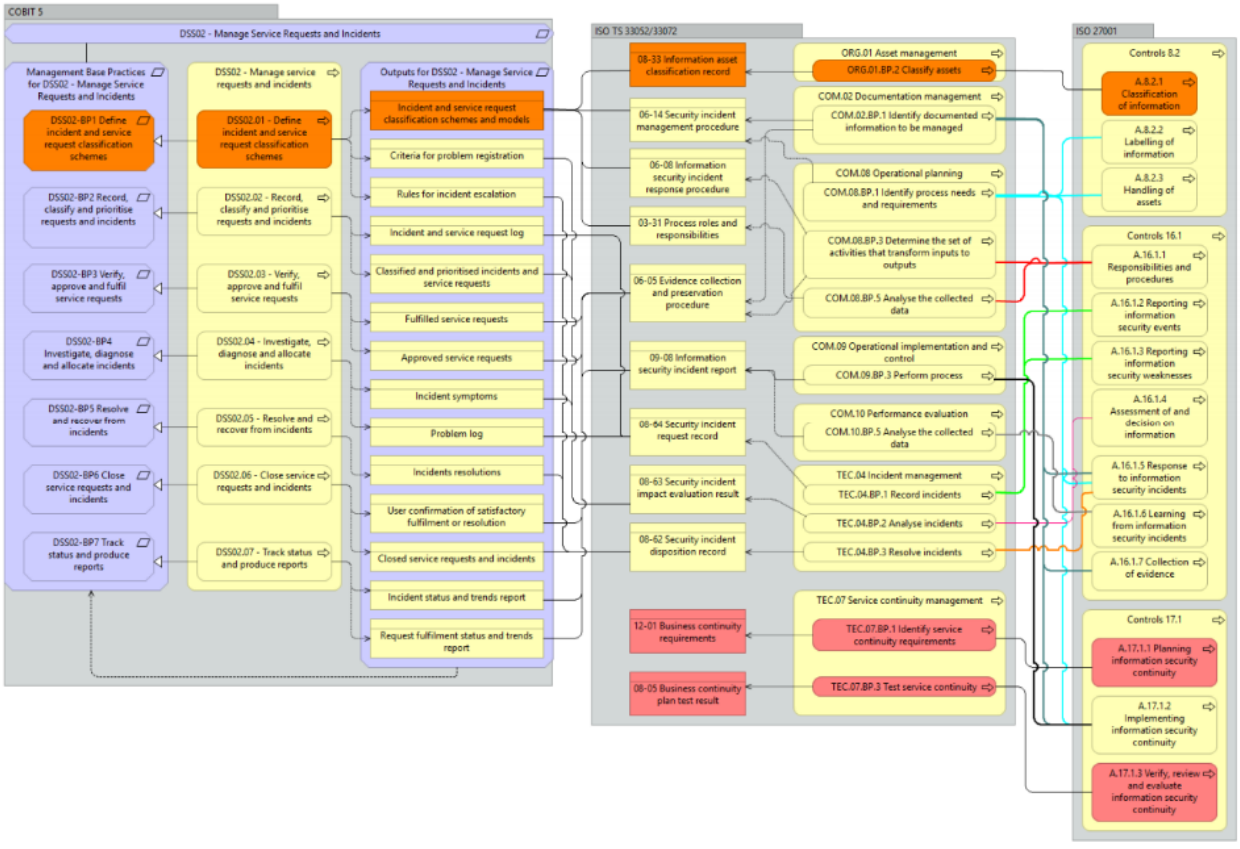


Figure 3.26. Cobit DSS02-ISO 33072 map with ArchiMate

Another way to find relations is semantic analysis. Mapping between two text information is required to define how to be compliant. By making this relatedness map users (IT governors or process owners) can prioritize the Cobit actions to comply with the related selected regulation. (Magerman et al., 2011)

3.2.2. Mapping Cobit Activities to BRSA's IS and Electronic Banking Regulation

The proposed mapping process published as an journal paper. In this paper, it has been revealed that the consistency of the relationship matrices, relatedness ratios that is specified in the relationship matrix created with LSA is very high. Since some of the information in this part of the thesis was published exactly in the article, the information needed to cited with a reference. "Cobit has 5 domains and 40 processes, these 40 processes have 231 practices and every practice has actions as a piece of advice to comply with Cobit. Totally, Cobit has 1202 actions. In thesis 1202 actions and BRSA's "Information Systems and Electronics of Banks Regulation on Banking Services" regulation has 224 articles together and made a one-to-many latent semantic analysis to gather a relatedness map. With this map, it is intended to have two ways to evaluate. First is finding Cobit's related article on regulation, second from the regulation side which Cobit domains are covered and which Cobit actions can be done to comply with the regulation" (Huyut, Kocaoğlu and Meram, 2022) Figure 3.27 shows which way to use on a relatedness map.

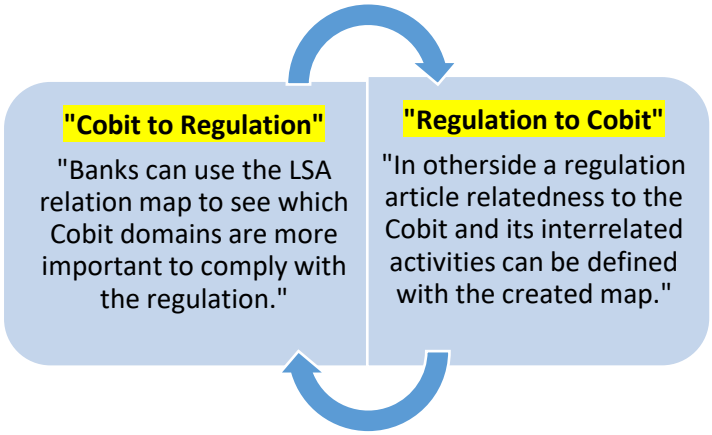


Figure 3.27. Map's purpose; Cobit to regulation and regulation to Cobit

Table 3.29. shows a sample of EDM 01 "Evaluate Direct and Monitor" domain's 01 numbered "Evaluate Governance Framework Setting and Maintenance" process. In this table, ISACA defined these objectives description and its practices and these practices related actions. This table consists of 231 total practices.

Table 3.29. Sample domain, process, and practices for Cobit

Area	Domain	Objective ID	Objective	Objective Description	Objective Purpose Statement	Practice_ID	Practice Name	Practice Description
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.	EDM01.01	Evaluate the governance system.	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.
						EDM01.02	Direct the governance system.	Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.
						EDM01.03	Monitor the governance system.	Monitor the effectiveness and performance of the enterprise's governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.
Governance	Evaluate, Direct and Monitor	EDM02	Ensured Benefits Delivery	Optimize the value to the business from investments in business processes, I&T services and I&T assets.	Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.	EDM02.01	Establish the target investment mix.	Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.

5 Domain **40 Processes** **231 practices and this practices have 1202 Actions**

In Table 4.32 Cobit actions and related Cobit process has a key to map with identification numbers. In “Area” field, Cobit groups its domain with governance and management. “Evaluate, Direct and Monitor” process group or domain is in “Governance” area, other 4 domains are in “Management” area. Domains or process groups are “Evaluate, Direct and Monitor”, “Align, Plan and Organize”, “Build, Acquire and Implement”, “Deliver, Service and Support”, “Monitor, Evaluate and Assess”. Cobit has 40 processes (sometimes mentioned as a subdomain) and each of them belongs to a process group aka domain. Every process has a unique process number that starts with the name of the domain and continuing with the specific number of its own code. Cobit named this “Objective ID” and each of them has an objective detail, objective description and objective purpose statement. For example, EDM 01 process has 3 practices; “EDM 01.01”, “EDM 01.02” and “EDM 01.03" and these practices have their own actions. In Table 3.30. “EDM 01.01”’s 8 actions, “EDM 01.02”’s 7 actions and “EDM 01.03”’s 6 actions are shown. For EDM 01 process total of 21 actions are defined by ISACA.

Table 3.30. Cobit actions and practices in relation

Area	Domain	Objective ID	Objective	Objective Description	Objective Purpose Statement	Practice_ID	Practice Name	Practice Description
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.	EDM01.01	Evaluate the governance system.	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.

Action No comes from Objective ID+Practice ID and its unique code

ACTION_NO	ACTION_DETAIL
EDM01.01.1	Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.
EDM01.01.2	Determine the significance of I&T and its role with respect to the business.
EDM01.01.3	Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise I&T.
EDM01.01.4	Determine the implications of the overall enterprise control environment with regard to I&T.
EDM01.01.5	Align the ethical use and processing of information and its impact on society, the natural environment, and internal and external stakeholder interests with the enterprise's direction, goals and objectives.
EDM01.01.6	Articulate principles that will guide the design of governance and decision making of I&T.
EDM01.01.7	Determine the optimal decision-making model for I&T.
EDM01.01.8	Determine the appropriate levels of authority delegation, including threshold rules, for I&T decisions.
EDM01.02.1	Communicate governance of I&T principles and agree with executive management on the way to establish informed and committed leadership.
EDM01.02.2	Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.
EDM01.02.3	Establish an I&T governance board (or equivalent) at the board level. This board should ensure that governance of information and technology, as part of enterprise governance, is adequately addressed; advi
EDM01.02.4	Allocate responsibility, authority and accountability for I&T decisions in line with agreed-on governance design principles, decision-making models and delegation.
EDM01.02.5	Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.
EDM01.02.6	Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.
EDM01.02.7	Direct the establishment of a reward system to promote desirable cultural change.
EDM01.03.1	Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise I&T.
EDM01.03.2	Periodically assess whether agreed-on governance of I&T mechanisms (structures, principles, processes, etc.) are established and operating effectively.
EDM01.03.3	Assess the effectiveness of the governance design and identify actions to rectify any deviations found.
EDM01.03.4	Maintain oversight of the extent to which I&T satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.
EDM01.03.5	Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.
EDM01.03.6	Monitor regular and routine mechanisms for ensuring that the use of I&T complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.
EDM02.01.1	Create and maintain portfolios of I&T-enabled investment programs, IT services and IT assets, which form the basis for the current IT budget and support the I&T tactical and strategic plans.
EDM02.01.2	Obtain a common understanding between IT and the other business functions on the potential opportunities for IT to enable and contribute to enterprise strategy.
EDM02.01.3	Identify the broad categories of information systems, applications, data, IT services, infrastructure, I&T assets, resources, skills, practices, controls and relationships needed to support the enterprise strategy.
EDM02.01.4	Agree on I&T goals, taking into account the interrelationships between the enterprise strategy and the I&T services, assets and other resources. Identify and leverage synergies that can be achieved.
EDM02.01.5	Define an investment mix that achieves the right balance among a number of dimensions, including an appropriate balance of short- and long-term returns, financial and nonfinancial benefits, and high- and lo
EDM02.02.1	Understand stakeholder requirements; strategic I&T issues, such as dependence on I&T; and technology insights and capabilities regarding the actual and potential significance of I&T for the enterprise's strate
EDM02.02.2	Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new I&T services, assets and resources.
EDM02.02.3	Understand and regularly discuss the opportunities that could arise for the enterprise from changes enabled by current, new or emerging technologies, and optimize the value created from those opportunities
EDM02.02.4	Understand what constitutes value for the enterprise, and consider how well it is communicated, understood and applied throughout the enterprise's processes.

The selected LSA tool and algorithm is Colorado University's LSA tool. This tool can be reachable from the website (http://lsa.colorado.edu/cgi-bin/LSA-one2many.html) one-to-many algorithms, which works only in the English language. So, the selected regulation was translated from Turkish to English. After translating, data cleaning process was made. In this process, some special terms (IT, I&T, eg., ex. etc. et al.) cleared, punctuations or pointing, abbreviations and special characters such apostrophes or hyphens and Cobit or selected regulation's special names abbreviations, domain-process need-regulation article numbers to be cleared article names and numbers stayed on a different table field to have a valid reference between regulation articles and Cobit actions. The regulation consists of 4 main sections, 7 parts, and 48 articles. In Table 3.31. main parts are given.

Table 3.31. Translated regulation's main parts and its articles

Kısım No	Kısım Adı	Bölüm No	Bölüm Adı	Madde No	Madde Adı	Fıkra Sayısı
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	4	Sistem Geliştirme ve Değişiklik Yönetimi	21	Proje yönetimi	5
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	4	Sistem Geliştirme ve Değişiklik Yönetimi	22	Sistem geliştirme, taşıma ve kurulum	10
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	4	Sistem Geliştirme ve Değişiklik Yönetimi	23	Uygulama kontrolleri	1
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	4	Sistem Geliştirme ve Değişiklik Yönetimi	24	Değişiklik yönetimi	4
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	5	Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi	25	Birincil ve ikincil sistemler	5
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	5	Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi	26	BT operasyon yönetimi	5
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	5	Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi	27	Erişilebilirlik yönetimi ve yedekleme	5
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	5	Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi	28	Bilgi sistemleri sürekliliğinin sağlanması	10
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	6	Dış Hizmet Alımı	29	Dış hizmet alımı sürecinin yönetimi	11
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	7	BS İç Kontrol ve İç Denetim Faaliyetleri	30	BS iç kontrol faaliyetleri	3
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	7	BS İç Kontrol ve İç Denetim Faaliyetleri	31	BS iç denetim faaliyetleri	5
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	7	BS İç Kontrol ve İç Denetim Faaliyetleri	32	Bulguların takibi ve güvence sağlanması	4
2	Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi	7	BS İç Kontrol ve İç Denetim Faaliyetleri	33	Personelin eğitilmesi ve kaynak tahsisi	2
3	Elektronik Bankacılık Hizmetleri	1	Ortak Hükümler	34	Kimlik doğrulama ve işlem güvenliği	15
3	Elektronik Bankacılık Hizmetleri	1	Ortak Hükümler	35	İnkâr edilemezlik ve sorumluluk atama	1
3	Elektronik Bankacılık Hizmetleri	1	Ortak Hükümler	36	İşlemlerin takibi	2
3	Elektronik Bankacılık Hizmetleri	1	Ortak Hükümler	37	Müşterilerin bilgilendirilmesi	8
3	Elektronik Bankacılık Hizmetleri	2	İnternet Bankacılığı	38	İnternet bankacılığında kimlik doğrulama ve işlem güvenliği	5
3	Elektronik Bankacılık Hizmetleri	3	Mobil Bankacılık	39	Mobil bankacılıkta kimlik doğrulama ve işlem güvenliği	3
3	Elektronik Bankacılık Hizmetleri	4	Telefon Bankacılığı	40	Telefon bankacılığında kimlik doğrulama, işlem güvenliği ve hizmet kalitesi	7
3	Elektronik Bankacılık Hizmetleri	5	Açık Bankacılık Servisleri	41	Açık bankacılık servislerinde kimlik doğrulama ve işlem güvenliği	2
3	Elektronik Bankacılık Hizmetleri	6	ATM Bankacılığı	42	ATM'lerde kimlik doğrulama ve işlem güvenliği	10
4	Çeşitli ve Son Hükümler	1	Çeşitli Hükümler	43	Uzaktan kimlik tespiti ve üçüncü tarafa güven	1
4	Çeşitli ve Son Hükümler	1	Çeşitli Hükümler	44	Mesleki tecrübeye ilişkin alanlar ve süreler	1
4	Çeşitli ve Son Hükümler	1	Çeşitli Hükümler	45	İstisna hükmü	1
4	Çeşitli ve Son Hükümler	2	Son Hükümler	46	Yürürlükten kaldırılan tebliğ	1
4	Çeşitli ve Son Hükümler	2	Son Hükümler	47	Yürürlük	1
4	Çeşitli ve Son Hükümler	2	Son Hükümler	48	Yürütme	1

Totally 48 article has 224 clauses (significant substances, sometimes mentioned as article as a unique numbered text with article master number and its related clause special number) and these 224 clauses are coded as Text1 to Text 224 to identify them on the relatedness map. Table 3.32. shows a sample of the coded texts.

Table 3.32. Coded regulation articles' clauses

Total 224 Article Translated Turkish to English

Fıkra	ARTICLE_NO	ARTICLE
etim kurulu, bilgi sistemlerinin yönetiminin kurumsal yönetim uygulamalarının bir parçası olarak ele almakla, bilgi in doğru yönetimi için gerekli finansman ve insan kaynağını tahsis etmekle, bilgi varlıklarının gizliliği, bütünlüğü ve ğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlamakla ve gelişen yeni teknolojileri inde bulundurarak bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmekle r. Bu amaçla, yönetim kurulu tarafından onaylanacak şekilde bir BS strateji planı, BS Strateji Komitesi ve BS Yönlendirme luşturulur. Banka yönetim kurulu bankanın ölçeği, bilgi sistemlerine bağımlılığı, personel sayısı ve bilgi sistemleri alınan dış hizmetler gibi kriterleri esas alarak strateji ve yönlendirme komitelerini birleştirebilir. Bu komitelerin görev e çalışma esasları yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilir.	Text 1	The Board of Directors of the Bank considers the management of information systems as a part of management practices, allocates the necessary financial and human resources for the correct mar information systems, ensures the establishment of effective controls on information systems in or confidentiality, integrity and accessibility of information assets, and It is responsible for conductin oversight in order to manage the risks arising from the use of information systems. For this purpos plan, IS Strategy Committee and IS Steering Committee are established to be approved by the boa board of directors of the bank can combine strategy and steering committees based on criteria su the bank, dependency on information systems, number of personnel and external services receive systems. Job descriptions and working principles of these committees are put in writing to be app of directors.
Komitesi, yönetim kurulu adına, BS strateji planı doğrultusunda BS yatırımlarının uygun bir şekilde kullanılıp dığının ve bankanın iş hedefleri ile BS hedeflerinin birbiriyle uyumluluğunun gözetimini yürütmekle; bu hususlarda yönetim loğrudan ve düzenli olarak raporlama yapmakla; BS strateji planını yılda en az bir defa olmak üzere gözden geçirerek gerekli rumlarda revize ederek yönetim kurulu onayına sunmakla ve BS Yönlendirme Komitesinin faaliyetlerini gözetmekle r.	Text 2	The IS Strategy Committee, on behalf of the board of directors, oversees whether IS investments a appropriately in line with the IS strategy plan and that the business objectives of the bank and IS o compatible with each other; reporting directly and regularly to the board of directors on these ma responsible for reviewing the IS strategy plan at least once a year, revising it when necessary, subm board of directors and overseeing the activities of the IS Steering Committee.
Komitesinde en az bir yönetim kurulu üyesinin bulunması ve bilgi sistemlerinden sorumlu üst düzey yönetici ile bankanın mlerinden üst düzey yöneticilerin bu komiteye üye olması esastır. BS Strateji Komitesi, BS strateji planının düzgün bir şekilde uygulanmadığını gözden geçirmek ve önemli BS yatırım kararlarını değerlendirmek üzere yılda en az iki defa bir araya gelir az bir defa yönetim kuruluna rapor sunar.	Text 3	It is essential that there is at least one board member in the IS Strategy Committee and that the se responsible for information systems and senior managers from the relevant business units of the b of this committee. The IS Strategy Committee meets at least twice a year and reports to the board to review the proper implementation of the IS strategy plan and evaluate key IS investment decisio
inin yönetim kurulu onayı doğrultusunda uygulanmasında, BS Strateji komitesine ve üst düzey yönetime yardımcı olmak bir BS Yönlendirme Komitesi oluşturulur. BS Yönlendirme Komitesi, BS yatırımlarının ve projelerinin öncelik sırasını , devam eden BS projelerinin durumunu takip etmek, projeler arasındaki kaynak çatışmalarını çözüme kavuşturmak, BS e BS projelerinin mevzuata uyumluluğunu sağlamak üzere gerekli yönlendirmeleri yapmak ve BS servislerine ilişkin hizmet izlemekten sorumludur. BS Yönlendirme Komitesinde BS, insan kaynakları, bankanın ilgili iş birimlerinden temsilcilerin ve nizasyonunda bulunması durumunda uyum ve hukuk ile ilgili birim ya da pozisyonlardan temsilcilerin bulunması esastır. dirme Komitesi, yılda en az iki defa bir araya gelir ve yılda en az bir defa BS Strateji Komitesine rapor sunar.	Text 4	An IS Steering Committee is established to assist the IS Strategy committee and senior manageme implementation of the IS strategy in line with the approval of the board of directors. The IS Steerin responsible for determining the prioritization of IS investments and projects, monitoring the status projects, resolving resource conflicts between projects, making necessary guidance to ensure com architecture and IS projects with legislation, and monitoring service levels for IS services. In the IS S Committee, it is essential to have representatives from IS, human resources, relevant business unit if present, from the units or positions related to compliance and law. The IS Steering Committee m a year and reports to the IS Strategy Committee at least once a year.
asyonu ve bilgi sistemlerinin kapsamlılık düzeyinin, bankanın büyüklüğü ve faaliyetlerinin karmaşıklığı ile orantılı olması ve asyon şemasının da bu doğrultuda oluşturulması esastır. BS organizasyon şeması kapsamındaki birimlerin görev ve kları ile bu birimlerdeki personelin görev tanımları açık bir şekilde yazılı hale getirilir, yönetim kurulu ya da yönetim bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanır, bu görev tanımlarının uygunluğu düzenli olarak gözden	Text 5	It is essential that the level of comprehensiveness of the IS organization and information systems i the size of the bank and the complexity of its activities, and that the IS organization chart is formed duties and responsibilities of the units within the scope of the IS organizational chart and the job d personnel in these units are clearly written, and the board of directors or senior executives who ha authority in this direction are approved, and the appropriateness of these job descriptions is regula
elinin kendilerine atanan görev ve sorumluluklar hakkında farkındalığa sahip olması ve kendilerine ait görev ve klarda değişiklik yapılması halinde bu değişikliklerden haberdar olmaları sağlanır.	Text 6	It is ensured that IS personnel are aware of the duties and responsibilities assigned to them, and ar changes in case of changes in their duties and responsibilities.
i sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken ıslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanlarını oluşturur.	Text 7	The Bank creates IS policy, procedure and process documents describing the procedures and princ and the controls to be established in order to manage the risks arising from the use of information protect information assets.

Articles coded as Text 1 to Text 224

After coding the regulation, every article was analyzed with 1202 actions from Cobit and created a matrix of 224*1202. LSA created every article's relatedness ratio with Cobit's selected domains' practices' action's similarity percentage. Values are varied from 0 to 1, 0 shows relatedness is not found and 1 shows they are the same. After analyzing all article's

relatedness, the data was stored in Excel and created the relatedness matrices. In excel a heat map was created and its small part is depicted in Table 3.33. these matrices show easily which action is mostly related to specific articles.

Table 3.33. Regulation articles and Cobit actions relatedness map sample

ARTICLE_NO	EDM01.01	EDM01.01	EDM01.01	EDM01.01	EDM01.01	EDM01.01	EDM01.01	EDM01.01	EDM01.02	EDM01.02	EDM01.02	EDM01.02	EDM01.02	EDM01.02	EDM01.02	EDM01.03	EDM01.03	EDM01.03	EDM01.03	EDM01.03	EDM01.03	EDM02.01	EDM02.01	EDM02.01
Text 1	0.73	0.76	0.79	0.69	0.82	0.76	0.69	0.74	0.83	0.73	0.90	0.73	0.84	0.76	0.67	0.77	0.83	0.77	0.73	0.74	0.77	0.80	0.83	0.84
Text 2	0.67	0.78	0.78	0.64	0.73	0.74	0.68	0.72	0.80	0.76	0.90	0.76	0.72	0.73	0.59	0.76	0.79	0.77	0.70	0.64	0.75	0.78	0.81	0.69
Text 3	0.67	0.77	0.74	0.61	0.74	0.73	0.69	0.74	0.82	0.67	0.88	0.74	0.78	0.72	0.60	0.74	0.76	0.72	0.70	0.66	0.72	0.76	0.80	0.73
Text 4	0.73	0.79	0.79	0.66	0.76	0.72	0.68	0.76	0.84	0.75	0.88	0.76	0.73	0.76	0.63	0.80	0.80	0.74	0.79	0.68	0.80	0.82	0.83	0.75
Text 5	0.70	0.76	0.79	0.66	0.79	0.75	0.67	0.76	0.83	0.76	0.87	0.73	0.78	0.75	0.66	0.80	0.85	0.78	0.74	0.69	0.76	0.76	0.83	0.75
Text 6	0.69	0.71	0.78	0.66	0.71	0.72	0.66	0.69	0.76	0.69	0.78	0.69	0.69	0.75	0.69	0.75	0.79	0.76	0.69	0.60	0.72	0.71	0.76	0.64
Text 7	0.68	0.69	0.75	0.64	0.81	0.75	0.68	0.71	0.75	0.71	0.82	0.71	0.84	0.69	0.64	0.70	0.81	0.73	0.71	0.70	0.74	0.71	0.74	0.83
Text 8	0.63	0.70	0.75	0.56	0.67	0.69	0.60	0.68	0.72	0.69	0.83	0.68	0.68	0.69	0.55	0.72	0.73	0.68	0.66	0.55	0.70	0.69	0.72	0.66
Text 9	0.67	0.73	0.81	0.67	0.76	0.78	0.71	0.77	0.84	0.76	0.86	0.78	0.73	0.76	0.66	0.81	0.83	0.78	0.77	0.67	0.78	0.77	0.78	0.70
Text 10	0.69	0.72	0.78	0.67	0.76	0.78	0.71	0.74	0.80	0.76	0.83	0.76	0.75	0.75	0.64	0.77	0.85	0.78	0.75	0.69	0.74	0.76	0.78	0.73
Text 11	0.64	0.68	0.76	0.63	0.73	0.77	0.72	0.70	0.77	0.72	0.80	0.74	0.71	0.74	0.61	0.73	0.81	0.77	0.72	0.61	0.73	0.73	0.72	0.67
Text 12	0.64	0.75	0.73	0.60	0.72	0.67	0.62	0.63	0.70	0.67	0.81	0.65	0.70	0.66	0.60	0.69	0.75	0.71	0.64	0.60	0.67	0.73	0.76	0.71
Text 13	0.70	0.85	0.66	0.57	0.69	0.58	0.55	0.57	0.63	0.59	0.80	0.57	0.68	0.59	0.51	0.63	0.70	0.61	0.55	0.55	0.58	0.71	0.85	0.75
Text 14	0.55	0.61	0.58	0.50	0.70	0.58	0.55	0.54	0.56	0.57	0.72	0.56	0.72	0.57	0.45	0.54	0.63	0.62	0.50	0.47	0.57	0.60	0.63	0.80
Text 15	0.64	0.73	0.77	0.62	0.70	0.67	0.61	0.64	0.73	0.68	0.80	0.65	0.64	0.68	0.62	0.73	0.75	0.72	0.70	0.63	0.73	0.75	0.77	0.66
Text 16	0.68	0.73	0.78	0.62	0.77	0.73	0.65	0.71	0.76	0.69	0.85	0.68	0.81	0.73	0.61	0.75	0.80	0.76	0.74	0.63	0.77	0.76	0.78	0.76
Text 17	0.61	0.63	0.66	0.58	0.73	0.61	0.60	0.60	0.61	0.62	0.72	0.60	0.67	0.65	0.54	0.64	0.71	0.68	0.61	0.54	0.64	0.64	0.67	0.79
Text 18	0.66	0.69	0.66	0.61	0.78	0.68	0.63	0.63	0.70	0.63	0.81	0.64	0.81	0.65	0.54	0.65	0.72	0.68	0.62	0.60	0.66	0.70	0.72	0.76
Text 19	0.71	0.76	0.78	0.67	0.79	0.74	0.70	0.72	0.76	0.70	0.86	0.71	0.82	0.75	0.61	0.76	0.81	0.78	0.69	0.63	0.72	0.76	0.80	0.78
Text 20	0.74	0.82	0.81	0.68	0.77	0.74	0.71	0.73	0.78	0.72	0.86	0.72	0.77	0.75	0.62	0.78	0.83	0.78	0.72	0.64	0.74	0.78	0.85	0.76
Text 21	0.69	0.72	0.81	0.69	0.75	0.79	0.72	0.73	0.76	0.74	0.82	0.74	0.71	0.76	0.63	0.77	0.83	0.81	0.71	0.64	0.74	0.77	0.77	0.68
Text 22	0.77	0.85	0.83	0.72	0.79	0.77	0.72	0.75	0.83	0.75	0.89	0.75	0.79	0.78	0.68	0.81	0.86	0.80	0.77	0.72	0.79	0.79	0.88	0.77
Text 23	0.70	0.74	0.77	0.69	0.77	0.73	0.68	0.68	0.73	0.72	0.83	0.69	0.74	0.73	0.66	0.72	0.82	0.78	0.67	0.67	0.71	0.80	0.77	0.74
Text 24	0.72	0.75	0.76	0.67	0.80	0.69	0.63	0.71	0.78	0.70	0.85	0.68	0.82	0.73	0.61	0.78	0.81	0.74	0.73	0.67	0.73	0.78	0.81	0.80
Text 25	0.73	0.77	0.78	0.69	0.81	0.74	0.69	0.70	0.77	0.73	0.88	0.71	0.79	0.73	0.65	0.74	0.84	0.78	0.71	0.70	0.74	0.79	0.82	0.81
Text 26	0.76	0.81	0.81	0.71	0.82	0.74	0.69	0.76	0.82	0.74	0.91	0.73	0.82	0.77	0.69	0.82	0.85	0.79	0.77	0.75	0.78	0.83	0.86	0.83
Text 27	0.66	0.69	0.73	0.63	0.78	0.72	0.64	0.70	0.77	0.67	0.83	0.70	0.82	0.68	0.68	0.72	0.77	0.70	0.72	0.74	0.72	0.73	0.74	0.79
Text 28	0.69	0.76	0.76	0.63	0.78	0.72	0.65	0.73	0.85	0.70	0.89	0.73	0.81	0.74	0.61	0.77	0.78	0.74	0.74	0.68	0.76	0.78	0.82	0.77
Text 29	0.68	0.71	0.78	0.66	0.80	0.76	0.69	0.71	0.79	0.72	0.85	0.73	0.80	0.75	0.67	0.74	0.81	0.78	0.73	0.64	0.74	0.76	0.77	0.76
Text 30	0.66	0.72	0.75	0.64	0.76	0.69	0.63	0.69	0.77	0.72	0.85	0.70	0.79	0.69	0.63	0.73	0.81	0.73	0.70	0.70	0.72	0.75	0.77	0.76
Text 31	0.73	0.78	0.77	0.66	0.81	0.73	0.67	0.73	0.81	0.74	0.89	0.74	0.84	0.76	0.62	0.79	0.81	0.78	0.74	0.66	0.75	0.79	0.82	0.80
Text 32	0.68	0.68	0.73	0.67	0.79	0.68	0.63	0.62	0.65	0.70	0.79	0.64	0.70	0.67	0.59	0.65	0.78	0.74	0.62	0.61	0.70	0.68	0.72	0.79
Text 33	0.68	0.73	0.80	0.67	0.79	0.78	0.70	0.67	0.73	0.74	0.84	0.70	0.73	0.74	0.64	0.73	0.84	0.82	0.67	0.64	0.75	0.78	0.79	0.76
Text 34	0.64	0.67	0.71	0.62	0.78	0.68	0.64	0.62	0.66	0.70	0.79	0.65	0.73	0.65	0.57	0.63	0.79	0.73	0.61	0.60	0.68	0.70	0.74	0.81
Text 35	0.70	0.75	0.78	0.63	0.78	0.74	0.68	0.70	0.74	0.71	0.82	0.70	0.78	0.71	0.63	0.74	0.81	0.77	0.73	0.65	0.77	0.74	0.79	0.79
Text 36	0.59	0.64	0.66	0.54	0.67	0.66	0.60	0.56	0.65	0.59	0.75	0.60	0.77	0.61	0.51	0.64	0.66	0.67	0.59	0.57	0.63	0.65	0.70	0.70
Text 37	0.61	0.65	0.76	0.55	0.66	0.71	0.64	0.65	0.68	0.64	0.75	0.66	0.72	0.65	0.52	0.66	0.71	0.70	0.70	0.55	0.75	0.64	0.70	0.64
Text 38	0.72	0.77	0.81	0.69	0.82	0.77	0.69	0.73	0.79	0.75	0.87	0.73	0.82	0.76	0.69	0.78	0.85	0.79	0.74	0.73	0.77	0.77	0.83	0.82
Text 39	0.64	0.67	0.74	0.64	0.82	0.72	0.64	0.66	0.71	0.71	0.82	0.67	0.82	0.68	0.73	0.69	0.81	0.73	0.66	0.77	0.70	0.68	0.73	0.82
Text 40	0.68	0.72	0.75	0.63	0.79	0.69	0.62	0.66	0.72	0.69	0.83	0.67	0.81	0.69	0.65	0.72	0.78	0.74	0.69	0.67	0.74	0.73	0.76	0.80
Text 41	0.65	0.72	0.81	0.65	0.74	0.75	0.69	0.68	0.76	0.73	0.83	0.70	0.71	0.74	0.66	0.74	0.82	0.82	0.69	0.66	0.76	0.72	0.77	0.69
Text 42	0.74	0.77	0.87	0.72	0.78	0.78	0.72	0.76	0.81	0.79	0.86	0.76	0.75	0.79	0.69	0.81	0.90	0.82	0.78	0.72	0.82	0.78	0.83	0.74

In the sample relatedness matrix EDM domain and selected regulation's first 42 articles relatedness heat map can be seen. Red areas mean that relatedness between Cobit's action and regulation's related article has a strong relevance or high similarity. So, a governor can choose this pair and evaluate them together. On the other hand, green areas show that there is a low correlation and similarity between the Cobit action and the related regulation item. The governor can see that these couples do not have (or have very little) a relationship. In the biggest picture, the governor can see all the areas that are above the defined similarity percentage that has been chosen. With the help of this matrix, governors can easily detect if there are gaps between the regulation and Cobit. For example, it can be evaluated that all Cobit columns or related regulation items, in rows, whose similarity ratio is between 0 and 30 percent, generally shown in heat map as green, do not have a high relation with any action. Thus, it can be determined that there are articles that cannot be associated with Cobit in the regulation or that cannot be included in the regulation even though Cobit is studied.

3.2.3. Creating an Application

To show the results a Power BI application with a power query was created. The static dataset comes from the latent semantic analysis result of the regulation articles and Cobit actions relation map. To evaluate this data, two dashboards were created; one for a regulation's article related Cobit actions to show and another for a Cobit actions most related regulation article. These two dashboards visualize the data and easy access to each side to evolve the IT GRC model.

Model's most important processes selected to show created Power BI dashboard result. This application query relation map is given in a data model, in Figure 3.28.

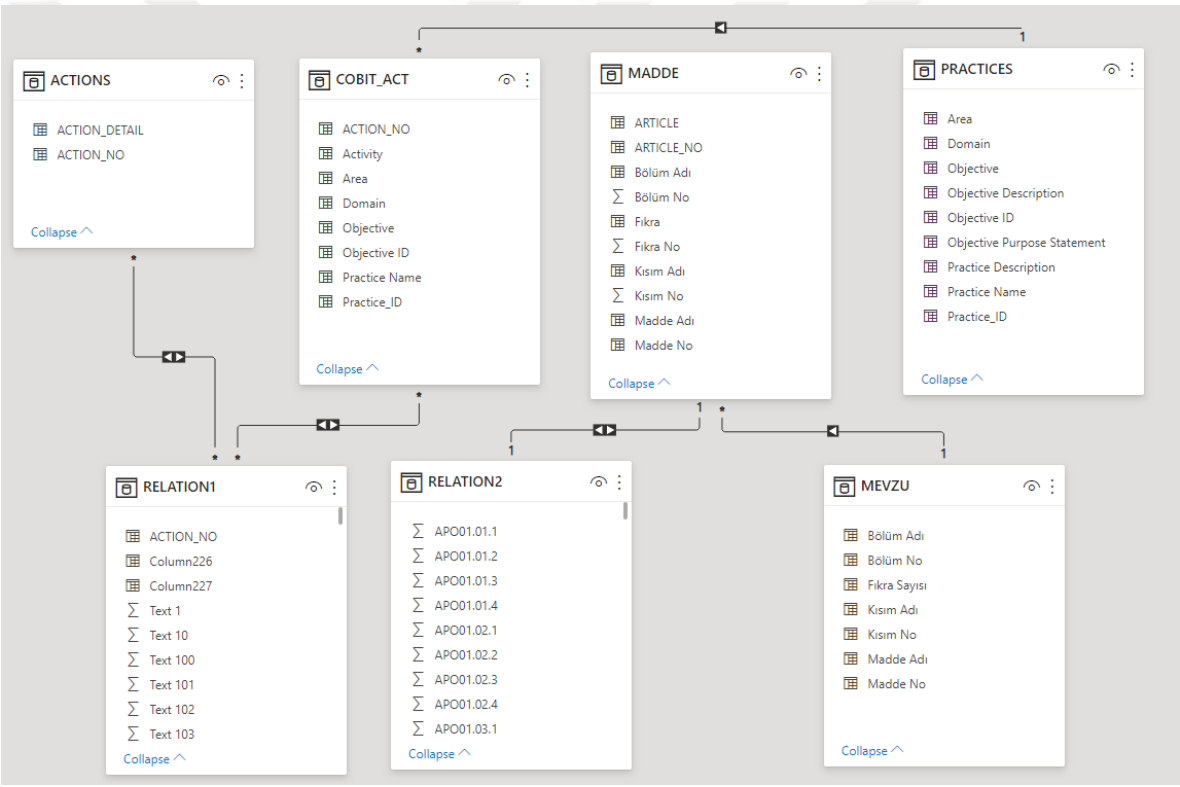


Figure 3.28. Power BI data model to create two dashboards

3.2.3.1. Cobit to Regulation Review

Firstly, for a sample review most important Cobit domain (defined by the survey by the sample bank) DSS 05 selected, it has 50 actions to relate to BRSA regulation articles. In this example, 50*224 matrices are filtered from the 1202*224 matrix first. To give a short example DSS 05's first 5 actions were assessed. The relatedness map is in Table 4.36. The defined relatedness criteria are relatedness ratio is over 80%. This ratio can be more or less to go deeper or higher to select only related regulation articles. (Table 3.34. DSS 05.01.3 action is related to 72 regulation articles so; the table is divided)

Table 3.34. DSS 05.01 processes actions' relatedness between regulation articles

ARTICLE_NO	DSS05.01.1
Text 52	0.86
Text 132	0.86
Text 34	0.86
Text 32	0.86
Text 217	0.85
Text 116	0.85
Text 82	0.84
Text 85	0.84
Text 109	0.83
Text 135	0.83
Text 65	0.83
Text 99	0.83
Text 185	0.83
Text 219	0.82
Text 75	0.82
Text 74	0.82
Text 123	0.82
Text 152	0.81
Text 138	0.81
Text 33	0.81
Text 183	0.81
Text 73	0.81
Text 214	0.81
Text 17	0.81
Text 151	0.80

ARTICLE_NO	DSS05.01.2
Text 55	0.84
Text 40	0.83
Text 31	0.82
Text 19	0.82
Text 39	0.81
Text 77	0.80
Text 94	0.80
Text 7	0.80

ARTICLE_NO	DSS05.01.3
Text 142	0.87
Text 104	0.85
Text 94	0.85
Text 95	0.85
Text 161	0.84
Text 158	0.84
Text 217	0.83
Text 33	0.83
Text 42	0.83
Text 38	0.83
Text 176	0.83
Text 146	0.83
Text 137	0.83
Text 86	0.83
Text 141	0.83
Text 88	0.83
Text 65	0.82
Text 138	0.82
Text 147	0.82
Text 117	0.82
Text 77	0.82
Text 164	0.82
Text 119	0.82
Text 125	0.82
Text 1	0.82
Text 22	0.82
Text 41	0.82
Text 26	0.82
Text 150	0.82
Text 140	0.82
Text 85	0.81
Text 152	0.81
Text 151	0.81
Text 78	0.81
Text 72	0.81
Text 57	0.81
Text 68	0.81
Text 131	0.81
Text 154	0.81
Text 43	0.81

DSS05.01.3 Continues

ARTICLE_NO	DSS05.01.3
Text 25	0.81
Text 51	0.81
Text 168	0.81
Text 189	0.81
Text 102	0.81
Text 31	0.81
Text 5	0.81
Text 169	0.81
Text 28	0.81
Text 132	0.80
Text 116	0.80
Text 82	0.80
Text 109	0.80
Text 135	0.80
Text 59	0.80
Text 206	0.80
Text 171	0.80
Text 35	0.80
Text 111	0.80
Text 101	0.80
Text 207	0.80
Text 136	0.80
Text 167	0.80
Text 92	0.80
Text 157	0.80
Text 190	0.80
Text 16	0.80
Text 160	0.80
Text 130	0.80
Text 19	0.80
Text 97	0.80
Text 165	0.80

ARTICLE_NO	DSS05.01.4
Text 119	0.84
Text 117	0.82
Text 120	0.81
Text 46	0.81
Text 88	0.80
Text 101	0.80
Text 6	0.80

ARTICLE_NO	DSS05.01.5
Text 155	0.84
Text 195	0.82
Text 194	0.82
Text 26	0.81
Text 213	0.80

“DSS 05.01.1” is; “Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).”

LSA results with this action are Text 52 and Text 132;

Text 52 is; “The Bank takes the necessary actions to ensure the integrity of transactions, records and data carried out through information systems, and ensures their accuracy, completeness and reliability. Measures to ensure integrity are established to cover all stages of data transmission, processing and storage. The same approach is used for transactions with external service providers.”

Text 132 is; “Bank, should ensure the availability of data which are obliged to give each backup scheme according to the accessibility requirements specified facilities. In order to restore backups taken from the system, operating system, application software and the operating system components that are included as data backup procedures. To make sure the backup works properly, the data on backup media by performing data restore operations are tested regularly. When moving the backup, protection by means of appropriate encryption techniques and physical security controls is provided.”

These two articles are about security protection on technology assets. Text 32 and 34 are again highly related with protect IS assets against malware.

Text 34; “In the transmission of sensitive data between environments with different security levels, it is essential to use end-to-end secure communication and to store these data in an encrypted form. The contents of desktop, laptop and mobile devices containing sensitive or secret data allocated to the bank's personnel are encrypted and server machines are scanned to determine whether sensitive data is available in clear text on the server devices connected to the network.”

To give an alternative delivery channel example. ATM endpoint security protection mentioned in Text 217, by 85%;

“ATM machines prevention on maliciously installed the or harmful programs and the necessary controls are taken to prevent unauthorized access, service and integrity of critical data for applications and application verified periodically. Automatically

or at regular intervals with the necessary updates and patches to address the vulnerability on installed ATMs. In this context, ATMs on the operating system that is set to run with the required minimum powers and privileges, stiffened by installing the necessary updates and patches, have a secure operating system based on the technology is stable and the day is provided. Banks, ATMs, take measures to prevent the supply and implementation of the study could not confirm the integrity of the code."

Other whole articles are related to a specific channel or a general security control about Cobit "DSS 05.01.1"'s related action. Text 116 again a security general control related to data protection, leakage prevention and malicious software attacks.

"DSS05.01.2" is; "Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails)."

Texts 55 and 40 are mainly about tracking security trails and unsolicited information unauthorized access, mentioned in Text 55 as "It is ensured that the track recording mechanism to be established is of a nature that allows the subsequent examination of information security incidents and obtaining reliable evidence about them." And other related Text 40; "With regarding the security of the identity authentication information of users on information systems, the Bank should keep authentication information in databases encrypted or mathematically impossible to be recycled, encrypted while being transferred for identity verification, protection against unauthorized access or uncontrolled changes in violation of the separation of duties principle, keeping sufficient track records regarding transactions performed on these databases, and It takes measures such as ensuring the security of these track records." In Text 31 regulation gives the responsibilities of Information security officer roles and again these roles contain DSS 05.01.2 In Text 19 IS risk analysis should contain this issue like protection against unsolicited information and filtering the network against malwares or phishing mails.

"DSS 05.01.3" is a common action to be taken in regulation about security awareness "Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and do not install shared or unapproved software." It is about security awareness and training this issue is widely mentioned in lots

of regulated articles, and because of this reason its relatedness map has higher text counts. 40 texts are related higher than 80%, most related is Text 142 with 87%.

Text 142 is about IS continuity plan test, its awareness like test period and training, Text 94 and 95 “A comprehensive information security awareness training program is created to increase the level of information security awareness across the bank. The training program includes information on information security policies and standards, as well as information on the individual responsibilities for information security and data protection, and the measures to be taken to protect information assets, and through these trainings, everyone who has access to the bank's IT resources and systems will be informed about the use of these resources. It is ensured that he/she has information about and directives.” And Text 95 “The information security awareness training program is approved by the Information Security Committee, and the content of the program is reviewed and updated at least once a year, taking into account new technologies and emerging risks. It is ensured that new and existing personnel who have access to the bank's IT resources and systems, and external service providers who have access to IT resources and systems in line with their areas of interest, undergo these trainings or document their training, and as the training program is updated, the relevant persons are provided with re-training on the updated parts.” It is directly highly related to this Cobit action.

DSS05.01.4 is “Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management.” Is about security alignment with change management. The most related regulation article is about the definition of change management and its implementation with security. Text 119; “Applications developed or outsourced at the bank, systematic or manual controls to carry out banking activities and business processes they are related to in accordance with the internal policies and legislative requirements and to ensure the accuracy, completeness and reliability of the data entered into these applications, modified, processed or produced by these applications. accommodates.

These controls are the identification of data that will constitute the input to the application; checking the type, format and size; verification of its source; ensuring the integrity and reliability of the data processed by the application; authorization of access to data in accordance with the separation of duties principle; establishing an entrant-validator structure where necessary; It performs functions such as ensuring the confidentiality, integrity,

consensus and distribution of the data that is the output of the application only to the necessary parties. The Bank pays attention to the fact that application controls are systemic as much as possible and that they are not carried out with manual procedures, and tests the controls they contain to ensure that they comply with the internal policies and legislative requirements before the application is set up, and records the test results." Text 117 and Text 120 are again defining change requests and management of changes in Banks. Text 117; "The Bank establishes an effective change management process that will minimize the number and impact of errors and problems that may occur due to changes that occur, ensure that changes are carried out effectively, quickly and in a controlled manner, and that the transactions made during changes can be audited after the change. Within the scope of this process, all kinds of changes to be made in the information systems elements such as network infrastructure, hardware, operating systems, software and the system, service, application configuration and parameters are initiated within the framework of a change request management process, the change request is based on a valid business need and the separation of duties principle. It is properly authorized, tested, realized, recorded and documented. It is essential that the changes are made by authorized users whose identity verification has been performed with appropriate techniques, that sufficient track records are kept for them and that the track records kept are reviewed regularly." In this article BRSA gave all security and other processes change management processes rules.

"DSS 05.01.5" is "Regularly review and evaluate information on new potential threats, reviewing vendors' products and services security advisories." Is about reviewing regularly vendor threads to a company. In the regulation Text 155 is more likely related with this action, BRSA creates rules about "Critical information systems .. manufacturer .. be located in Turkey and the utmost care for outsourcing is considered an important criterion. In addition, providers and manufacturers of these types of interventions are necessary for the team in Turkey. The Agency is authorized to determine additional requirements for security products and other IT elements can be used by banks." Again, relates with regulation.

3.2.3.2. Regulation to Cobit Review

These first 5 activities' relation is given as an example. On another side, users can reach relatedness by going from regulation to Cobit actions. For example, Text 32, 33 and 34 for data confidentiality controls in BRSA's regulation. Their relatedness map has higher percentages to related Cobit actions. To create a sample map, Text 32's most related actions

are filtered as a list in Table 3.35. This time if the selected cell scored higher than 80%, it would create too many results to evaluate. More than 124 actions for Text 32, 328 for Text 33 and 122 for Text 34. These 3 articles are all related to each other and can see Cobit actions relatedness again all 3 articles are related again same Cobit actions.

Table 3.35. Data confidentiality related articles relatedness map

ACTION_NO	Text 32	Text 33	Text 34
APO14.05.5	0.92	0.85	0.90
BAI07.02.6	0.91	0.88	0.89
DSS04.07.1	0.90	0.85	0.90
DSS06.02.3	0.89	0.88	0.90
APO14.07.3	0.89	0.87	0.90
DSS01.01.3	0.89	0.83	0.89
BAI07.02.7	0.89	0.86	0.88
BAI07.02.8	0.89	0.82	0.88
APO05.03.4	0.88	0.85	0.88
DSS04.07.4	0.88	0.84	0.88
APO14.04.2	0.88	0.83	0.87
DSS06.02.4	0.88	0.83	0.87
BAI10.05.5	0.88	0.81	0.86
APO14.02.4	0.87	0.87	0.87
APO01.07.2	0.87	0.84	0.87
DSS06.02.8	0.87	0.83	0.87
APO14.08.5	0.87	0.78	0.87
BAI04.02.3	0.87	0.86	0.85
BAI07.04.1	0.87	0.82	0.85
DSS04.03.6	0.87	0.79	0.85
APO03.02.6	0.86	0.85	0.87
APO06.05.5	0.86	0.84	0.87
EDM02.04.2	0.86	0.88	0.86
APO12.01.5	0.86	0.81	0.86
DSS05.01.1	0.86	0.81	0.86
APO14.06.3	0.86	0.77	0.86
APO12.01.4	0.86	0.82	0.85
APO14.05.6	0.86	0.80	0.85
APO11.03.5	0.86	0.81	0.84

The most relevant Cobit actions with data confidentiality articles are mentioned in Table 3.36.

Table 3.36. Most relevant Cobit actions with data confidentiality articles

ACTION_NO	Text 32
APO14.05.5	0.92
BAI07.02.6	0.91
DSS04.07.1	0.90
DSS06.02.3	0.89
APO14.07.3	0.89
BAI07.02.7	0.89
DSS01.01.3	0.89
BAI07.02.8	0.89
APO05.03.4	0.88
DSS04.07.4	0.88
APO14.04.2	0.88
DSS06.02.4	0.88
BAI10.05.5	0.88

ACTION_NO	Text 33
BAI02.01.1	0.91
BAI03.03.6	0.91
APO03.01.6	0.90
BAI07.08.1	0.90
DSS01.03.5	0.90
APO05.05.1	0.89
BAI02.04.2	0.89
BAI05.04.2	0.89
BAI09.02.8	0.89
BAI11.09.5	0.89
APO03.02.7	0.88
BAI01.05.4	0.88
BAI05.02.1	0.88
BAI07.02.6	0.88
DSS02.05.4	0.88
DSS03.04.	0.88
DSS06.02.3	0.88
EDM02.04.2	0.88
EDM05.01.3	0.88
MEA02.01.4	0.88
MEA04.07.4	0.88

ACTION_NO	Text 34
APO14.05.5	0.90
DSS04.07.1	0.90
DSS06.02.3	0.90
APO14.07.3	0.90
BAI07.02.6	0.89
DSS01.01.3	0.89
BAI07.02.7	0.88
BAI07.02.8	0.88
APO05.03.4	0.88
DSS04.07.4	0.88

Text 32 is about data confidentiality rules; “The Bank ensures the confidentiality of the data used in banking activities in the environments where it is transported, transmitted, processed, stored and kept as backup. Regardless of whether the environment where the data is kept is paper or electronic media, it is essential to keep data confidentiality and to establish additional controls where necessary. In the event that media or devices containing data are removed from use, it is ensured that the data they contain are destroyed safely in accordance with the degree of confidentiality.” “APO 14.05.5” is the most related Cobit action as “Ensure that results are centrally stored, systematically monitored and analyzed with respect to statistics and metrics. Provide the resulting insight to data quality improvements over time.” and BAI07.02.6 as “Coordinate and verify the timing and completeness of the conversion cutover so there is a smooth, continuous transition with no loss of transaction data. Where necessary, in the absence of any other alternative, freeze live operations.” “DSS 04.07.1” is “Backup systems, applications, data and documentation according to a defined schedule. Consider frequency (monthly, weekly, daily, etc.), mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention), type of backup (e.g., full vs. incremental), and type of media. Consider also automated online backups, data

types (e.g., voice, optical), creation of logs, critical end-user computing data (e.g., spreadsheets), physical and logical location of data sources, security and access rights, and encryption."

Text 33 from the regulation is a bit long but mainly about data encryption techniques "For the encryption techniques to be used to ensure data privacy, algorithms that have not lost their reliability as of the current situation and are in accordance with the current technology are used. The encryption keys to be used are selected for the relevant algorithms in such a way that the key will be valid and cannot be broken during the time it can be used, and the validity period of these keys is determined according to the criticality level of the relevant data or operation. The use of encryption keys that are found to have expired or become unreliable is immediately blocked. It is essential to ensure the security of encryption keys throughout their life cycle, to create them securely, to offer them to customers and personnel and to store them." Related Cobit action is "Ensure that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritized and recorded in a way that is understandable to all stakeholders, recognizing that the requirements may change and will become more detailed as they are implemented." And "Ensure that responsibilities for using high-security or restricted-access infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated." And "Verify that transactions are accurate, complete and valid. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness, duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmations. It must validate input data and edit where applicable, send back for correction as close to the point of origination as possible."

Text 34 is "In the transmission of sensitive data between environments with different security levels, it is essential to use end-to-end secure communication and to store these data in an encrypted form. The contents of desktop, laptop and mobile devices containing sensitive or secret data allocated to the bank's personnel are encrypted and server machines are scanned to determine whether sensitive data is available in clear text on the server devices connected to the network."

"APO 14.05.5" is; "Ensure that results are centrally stored, systematically monitored and analyzed with respect to statistics and metrics. Provide the resulting insight to data quality

improvements over time." "DSS 04.07.1" is again related in Text 32 and "DSS 06.02.3" again the most related Cobit action as mentioned on Text 33.

These three articles most related Cobit action can be found by mean of them. Text's relatedness percentage, after finding the mean average the highest score is "BAI 07.02.6" and it's the most relevant among these three articles. Regulation grouped all related items together so, if the governing body wants to see which actions are most likely related to regulation they can use mean values. In Table 3.37. data confidentiality related 3 articles mean values given.

Table 3.37. Data confidentiality articles related actions by calculating mean values

ACTION_NO	Text 32	Text 33	Text 34	Mean
BAI07.02.6	0.91	0.88	0.89	0.893
APO14.05.5	0.92	0.85	0.90	0.890
DSS06.02.3	0.89	0.88	0.90	0.890
APO14.07.3	0.89	0.87	0.90	0.887
DSS04.07.1	0.90	0.85	0.90	0.883
BAI07.02.7	0.89	0.86	0.88	0.877

This method can be used in Cobit for regulation review. To define which article is most related to Cobit's "DSS 05.01.1" to "DSS 05.01.5" calculate mean values and sort largest to smallest scores. "DSS 05.01" practice name is "Protect against malicious software." And practice description is "Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., malware, ransomware, viruses, worms, spyware, spam)." "DSS 05.01"'s 5 actions are given in Figure 3.29.

DSS05 Process Practices, Inputs/Outputs and Activities				
Management Practice	**Inputs**		**Outputs**	
DSS05.01 Protect against malware. Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	**From**	**Description**	**Description**	**To**
			Malicious software prevention policy	APO01.04
			Evaluations of potential threats	APO12.02 APO12.03
Activities				
1. Communicate malicious software awareness and enforce prevention procedures and responsibilities.				
2. Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).				
3. Distribute all protection software centrally (version and patch-level) using centralised configuration and change management.				
4. Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).				
5. Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).				
6. Conduct periodic training about malware in email and Internet usage. Train users to not install shared or unapproved software.				

Figure 3.29. Cobit DSS05.01 subprocesses practices and activities
(**Source:** ISACA Cobit 5, 2017)

The most relevant article to these subprocesses by mean is in Text 94 and Text 72;

Text 94;“ A comprehensive information security awareness training program is created to increase the level of information security awareness across the bank. The training program includes information on information security policies and standards, as well as information on the individual responsibilities for information security and data protection, and the measures to be taken to protect information assets, and through the training, everyone who has access to the bank's IT resources and systems will be informed about the use of these resources. It is ensured that he/she has information about and directives.”

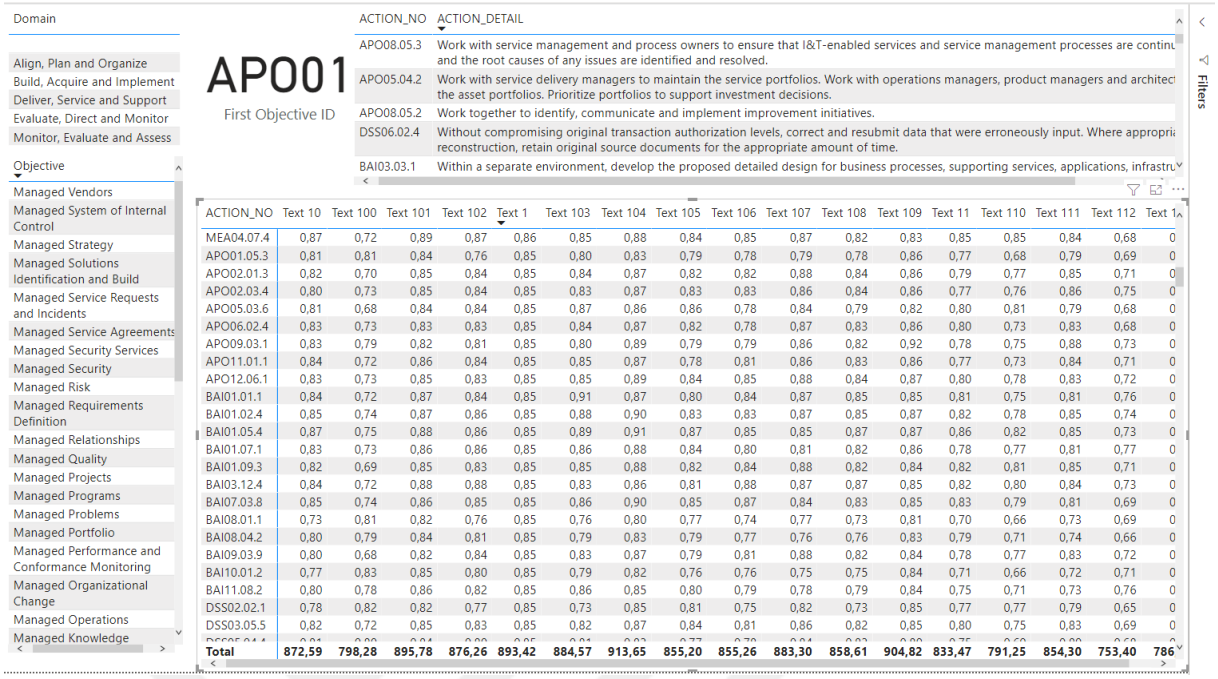
Text 72; “It creates tightened and tested secure standard configuration information for operating systems, databases and applications on banks, desktops, laptops, mobile devices and servers, and network devices such as firewalls, routers and switching devices. This standard configuration information, deviations from the standard configuration or updates in the standard configuration are recorded as part of the change management and subject to the approval mechanism. In this context, for any change request outside the secure standard configuration, information such as the business requirement that requires this change and the identity of the business responsible and the duration of the requirement are also recorded.”

Table 3.38. Protect against malware-related articles by calculating mean values

ARTICLE_NO	DSS05.01.1	DSS05.01.2	DSS05.01.3	DSS05.01.4	DSS05.01.5	Mean
Text 94	0.77	0.80	0.85	0.76	0.76	0.79
Text 72	0.79	0.79	0.81	0.78	0.76	0.79
Text 119	0.76	0.76	0.82	0.84	0.74	0.78
Text 137	0.74	0.78	0.83	0.79	0.78	0.78
Text 147	0.78	0.78	0.82	0.74	0.79	0.78

When the relevant items of Cobit and the regulation were evaluated together, it was seen that high similarity rates indicated related items in finding related Cobit items based on the regulation or in finding related regulatory items based on Cobit's related actions. In Table 3.38, when listed according to the regulation items with the highest similarity ratio, it is seen that Text 94 and Text 72 are related to the relevant "DSS 05.01" practices.

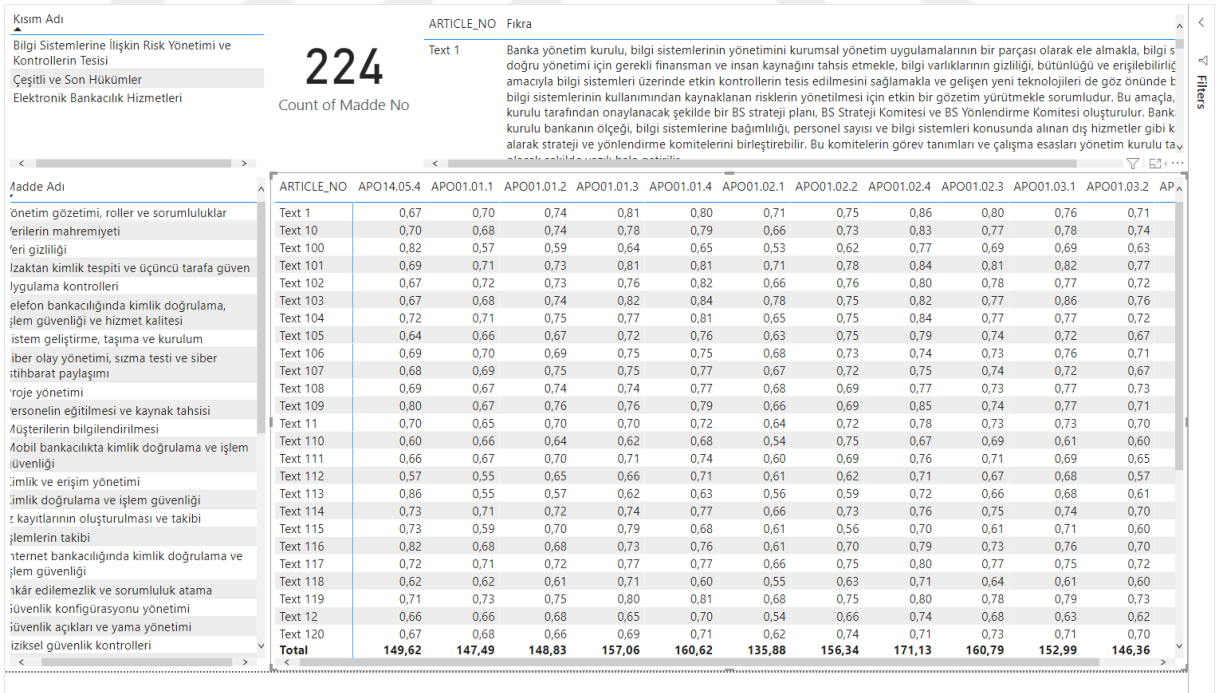
Created Power BI application has 2 dashboards to see the relation between selected Cobit and regulation items. In Figure 3.30 a user can select Cobit processes, practices and actions and Power BI gives related regulation actions automatically.



ACTION_NO	Text 10	Text 100	Text 101	Text 102	Text 1	Text 103	Text 104	Text 105	Text 106	Text 107	Text 108	Text 109	Text 11	Text 110	Text 111	Text 112	Text 1
MEA04.07.4	0,87	0,72	0,89	0,87	0,86	0,85	0,88	0,84	0,85	0,87	0,82	0,83	0,85	0,85	0,84	0,68	0
APO01.05.3	0,81	0,81	0,84	0,76	0,85	0,80	0,83	0,79	0,78	0,79	0,78	0,86	0,77	0,68	0,79	0,69	0
APO02.01.3	0,82	0,70	0,85	0,84	0,85	0,84	0,87	0,82	0,82	0,88	0,84	0,86	0,79	0,77	0,85	0,71	0
APO02.03.4	0,80	0,73	0,85	0,84	0,85	0,83	0,87	0,83	0,83	0,86	0,84	0,86	0,77	0,76	0,86	0,75	0
APO05.03.6	0,81	0,68	0,84	0,84	0,85	0,87	0,86	0,86	0,78	0,84	0,79	0,82	0,80	0,81	0,79	0,68	0
APO06.02.4	0,83	0,73	0,83	0,83	0,85	0,84	0,87	0,82	0,78	0,87	0,83	0,86	0,80	0,73	0,83	0,68	0
APO09.03.1	0,83	0,79	0,82	0,81	0,85	0,80	0,89	0,79	0,79	0,86	0,82	0,92	0,78	0,75	0,88	0,73	0
APO11.01.1	0,84	0,72	0,86	0,84	0,85	0,85	0,87	0,78	0,81	0,86	0,83	0,86	0,77	0,73	0,84	0,71	0
APO12.06.1	0,83	0,73	0,85	0,83	0,85	0,85	0,89	0,84	0,85	0,88	0,84	0,87	0,80	0,78	0,83	0,72	0
BAI01.01.1	0,84	0,72	0,87	0,84	0,85	0,91	0,87	0,80	0,84	0,87	0,85	0,85	0,81	0,75	0,81	0,76	0
BAI01.02.4	0,85	0,74	0,87	0,86	0,85	0,88	0,90	0,83	0,83	0,87	0,85	0,87	0,82	0,78	0,85	0,74	0
BAI01.05.4	0,87	0,75	0,88	0,86	0,85	0,89	0,91	0,87	0,85	0,85	0,87	0,87	0,86	0,82	0,85	0,73	0
BAI01.07.1	0,83	0,73	0,86	0,86	0,85	0,86	0,88	0,84	0,80	0,81	0,82	0,86	0,78	0,77	0,81	0,77	0
BAI01.09.3	0,82	0,69	0,85	0,83	0,85	0,85	0,88	0,82	0,84	0,88	0,82	0,84	0,82	0,81	0,85	0,71	0
BAI03.12.4	0,84	0,72	0,88	0,88	0,85	0,83	0,86	0,81	0,88	0,87	0,87	0,85	0,82	0,80	0,84	0,73	0
BAI07.03.8	0,85	0,74	0,86	0,85	0,85	0,86	0,90	0,85	0,87	0,84	0,83	0,85	0,83	0,79	0,81	0,69	0
BAI08.01.1	0,73	0,81	0,82	0,76	0,85	0,76	0,80	0,77	0,74	0,77	0,73	0,81	0,70	0,66	0,73	0,69	0
BAI08.04.2	0,80	0,79	0,84	0,81	0,85	0,79	0,83	0,79	0,77	0,76	0,76	0,83	0,79	0,71	0,74	0,66	0
BAI09.03.9	0,80	0,68	0,82	0,84	0,85	0,83	0,87	0,79	0,81	0,88	0,82	0,84	0,78	0,77	0,83	0,72	0
BAI10.01.2	0,77	0,83	0,85	0,80	0,85	0,79	0,82	0,76	0,76	0,75	0,75	0,84	0,71	0,66	0,72	0,71	0
BAI11.08.2	0,80	0,78	0,86	0,82	0,85	0,86	0,85	0,80	0,79	0,78	0,79	0,84	0,75	0,71	0,73	0,76	0
DSS02.02.1	0,78	0,82	0,82	0,77	0,85	0,73	0,85	0,81	0,75	0,82	0,73	0,85	0,77	0,77	0,79	0,65	0
DSS03.05.5	0,82	0,72	0,85	0,83	0,85	0,82	0,87	0,84	0,81	0,86	0,82	0,85	0,80	0,75	0,83	0,69	0
Total	**872,59**	**798,28**	**895,78**	**876,26**	**893,42**	**884,57**	**913,65**	**855,20**	**855,26**	**883,30**	**858,61**	**904,82**	**833,47**	**791,25**	**854,30**	**753,40**	**786**

Figure 3.30. Cobit processes, practices, and action selection and regulation relatedness dashboard

In Figure 3.31 users can select BRSA's regulation's processes, practices and actions and Power BI gives related regulation actions automatically.



ARTICLE_NO	APO14.05.4	APO01.01.1	APO01.01.2	APO01.01.3	APO01.01.4	APO01.02.1	APO01.02.2	APO01.02.4	APO01.02.3	APO01.03.1	APO01.03.2	AP
Text 1	0,67	0,70	0,74	0,81	0,80	0,71	0,75	0,86	0,80	0,76	0,71	
Text 10	0,70	0,68	0,74	0,78	0,79	0,66	0,73	0,83	0,77	0,78	0,74	
Text 100	0,82	0,57	0,59	0,64	0,65	0,53	0,62	0,77	0,69	0,69	0,63	
Text 101	0,69	0,71	0,73	0,81	0,81	0,71	0,78	0,84	0,81	0,82	0,77	
Text 102	0,67	0,72	0,73	0,76	0,82	0,66	0,76	0,80	0,78	0,77	0,72	
Text 103	0,67	0,68	0,74	0,82	0,84	0,78	0,75	0,82	0,77	0,86	0,76	
Text 104	0,72	0,71	0,75	0,77	0,81	0,65	0,75	0,84	0,77	0,77	0,72	
Text 105	0,64	0,66	0,67	0,72	0,76	0,63	0,75	0,79	0,74	0,72	0,67	
Text 106	0,69	0,70	0,69	0,75	0,75	0,68	0,73	0,74	0,73	0,76	0,71	
Text 107	0,68	0,69	0,75	0,75	0,77	0,67	0,72	0,75	0,74	0,72	0,67	
Text 108	0,69	0,67	0,74	0,74	0,77	0,68	0,69	0,77	0,73	0,77	0,73	
Text 109	0,80	0,67	0,76	0,76	0,79	0,66	0,69	0,85	0,74	0,77	0,71	
Text 11	0,70	0,65	0,70	0,70	0,72	0,64	0,72	0,78	0,73	0,73	0,70	
Text 110	0,60	0,66	0,64	0,62	0,68	0,54	0,75	0,67	0,69	0,61	0,60	
Text 111	0,66	0,67	0,70	0,71	0,74	0,60	0,69	0,76	0,71	0,69	0,65	
Text 112	0,57	0,55	0,65	0,66	0,71	0,61	0,62	0,71	0,67	0,68	0,57	
Text 113	0,86	0,55	0,57	0,62	0,63	0,56	0,59	0,72	0,66	0,68	0,61	
Text 114	0,73	0,71	0,72	0,74	0,77	0,66	0,73	0,76	0,75	0,74	0,70	
Text 115	0,73	0,59	0,70	0,79	0,68	0,61	0,56	0,70	0,61	0,71	0,60	
Text 116	0,82	0,68	0,68	0,73	0,76	0,61	0,70	0,79	0,73	0,76	0,70	
Text 117	0,72	0,71	0,72	0,77	0,77	0,66	0,75	0,80	0,77	0,75	0,72	
Text 118	0,62	0,62	0,61	0,71	0,60	0,55	0,63	0,71	0,64	0,61	0,60	
Text 119	0,71	0,73	0,75	0,80	0,81	0,68	0,75	0,80	0,78	0,79	0,73	
Text 12	0,66	0,66	0,68	0,65	0,70	0,54	0,66	0,74	0,68	0,63	0,62	
Text 120	0,67	0,68	0,66	0,69	0,71	0,62	0,74	0,71	0,73	0,71	0,70	
Total	**149,62**	**147,49**	**148,83**	**157,06**	**160,62**	**135,88**	**156,34**	**171,13**	**160,79**	**152,99**	**146,36**	

Figure 3.31. Regulation section, part and article selection, and Cobit relatedness dashboard

4. CONCLUSION

The use of technology by enterprises is becoming widespread in every sector. Businesses that use technology effectively and integrate innovations brought by information technologies into business processes can gain a competitive advantage. Enterprises that make technology investments sufficient and correctly, can automate their business processes, differentiate their products and services, and produce new innovative products and improved services. In addition to the positive aspects, businesses that cannot receive or use these technologies may not be successful despite the progress in technology. Technology alone is not a factor that makes a business sustainable or successful. It can be evaluated that the enterprise can achieve success as long as it enriches its expertise in the main business area with technology and develops its business with the possibilities of technology. Information technologies offer tools and techniques beyond a purpose, businesses that use these tools in the right way at the right time, and develop and integrate them with their core competence will be able to make a difference in their field and stay ahead in the competition race, no matter what sector they are in. The information technology governance risk and compliance model created within the scope of the thesis has been tried to convey what kind of contributions the companies that try to manage information technologies can make to their businesses by establishing the GRC model in these days where competition is increasing day by day in the business and technology world. All GRC frameworks and their related dimensions in the literature have been handled in detail as a whole. To manage information technologies with the GRC approach, IT GRC models, IT GRC frameworks within GRC models, IT governance frameworks, IT risk governance methodologies, and IT compliance and its importance are explained.

The financial sector is one of the areas that use information technologies intensively. With the digitalization of money, finance companies are transforming from the traditional financial model, where money is entrusted and loans are drawn, to technology companies that constantly develop new technologies and products related to the main field of technology management. With this transformation, customers can receive qualified banking services with 24/7 continuity. Customers, who access all services at any time of the day via their smart mobile devices, do not go to the branches except in obligatory cases. Banks are operating in a highly regulated area and their thread landscape is generally high. To govern banking information technologies, banks should create governance mechanisms to have effective oversight of the IT operations. IT creates values but without strategic alignment

between business and IT, this case results generally in high cost and inefficient source usage. IT processes or operations are not cheap so, this resource could not be used inefficiently. Also, IT investments are crucial for a bank. Banks cannot operate without IT systems and infrastructures to give stable services to customers. System resiliency is so important for a bank and its customers. Customer needs continuous services on all channels. Their needs are various and being online and reachable is highly important. Alternative delivery channels, ATMs, contact centers, and mobile or internet branch system continuity is crucial, these channels create new marketing places and competitive advantages. Moreover, in payment systems, it is more important. Customers do not need to carry alternative payment methods (cash or other payment methods) on them, they rely on banks' debit or credit cards to have goods or services. In a while, if the bank cannot complete the payment transaction, customer satisfaction easily decreases and customer losses may occur.

By allowing the use of remote customer acquisition in Turkey, by BRSA, banks were able to acquire customers by making use of remote video calling technologies and secure verification mechanisms of chip ID cards in almost all processes that require wet signatures in all banking services, starting with account opening to all other banking transactions. With the help of this technology, customers have lots of new service possibilities, like fast opening banking for any kind of account, increasing account or transfer limitations, or unlocking a sim block to use on a mobile channel. It is revolutionary in the banking sector; it disrupts branch channels and banks' customer service strategies. With this innovation, banks do not need thousands of branches to reach customers, customers can easily reach banks from anywhere on digital channels and prove their identity and approve the transaction. The need for face-to-face banking disrupts this permitted regulation. With this technological challenge, banks need more stable IT processes to have a competitive advantage and their importance level increases with these types of innovations. Customers are also preferring banks where they can get flexible, fast and quality service. All these positive developments continue to transform the banking sector, which is developing and changing with technology, into technological companies.

Banks that continue their technological development and even lead this trend, this way can provide a competitive advantage, and banks that create a difference with their customer experience can get ahead of their competitors. Because technological leadership can be closed in a short time by competitors, similar products and services can be seen in all banks

in a short time. Banks run on similar technological infrastructures and they need to carry out their business processes in harmony with IT processes. IT processes have become a prerequisite for banks to maintain their fundamental services. A bank whose information systems are not standing or sustaining will not be able to provide service continuity and will create negative results, even if it has billion-dollar capital, tens of millions of customers, and tens of thousands of branches. Banks, which use information technologies intensively, need to manage their information technology processes with the most accurate approaches, feed and harmoniously support each other and develop their IT and business unit capabilities to strategically align and move towards the same goal. This requirement is also valid for a bank that is growing and its processes are becoming more complex, as it is in every growing business. If the IT and business processes of a bank, which uses technology in almost all of its processes, are strategically incompatible, IT investments that would be incompatible with the objectives of the business can be made, and IT resources of the business may be spent on non-priority issues. To avoid this situation, where many more negative scenarios can be mentioned, IT GRC models have been proposed that allow the business and IT world to manage and execute the intertwined structure of each other in harmony. International good practices, large audit, and consultancy firms, and country regulatory and supervisory institutions suggest the establishment of mechanisms based on management in this regard.

Turkish banking sector is similar to the banking sectors of developed countries, using technology effectively and producing a large number of technology-based businesses that set an example for the world in creating new products and services. It can be claimed that it is ahead of banking processes. In some developed countries, banking services with long-term interruptions are possible, they are serving payments only limited options with prepaid cards. Account opening processes, which can take place within minutes with remote customer acquisition, can sometimes take days or even weeks/months in these countries. The technology in these processes has allowed digital-only banks to grow rapidly in the European and American banking sectors. These developments disrupt the traditional banking sector so, they started to be more agile to compete with these digital banks with the help of technology.

The main reasons for creating a GRC model for the Turkish banking sector in the thesis are that the banks of the country are subject to strict regulations and are frequently updated, and some banks use technology intensively. It has been considered that it will be an appropriate

sector choice since business and IT continuity are of high importance, the customer portfolio has no tolerance for interruptions, the use of card payment systems and pos is increasing day by day, and the basic condition of all these processes can be achieved with the correct information technology governance. As a sector in which all IT GRC dimensions are of high importance, the example of Turkey also has an advantage in compliance compared to other countries. With the first regulation published in the field of IT, BRSA introduced the Turkish banking sector to Cobit and made this compliance mandatory. This situation, which is not seen in other countries' legislation, has had a positive impact on IT governance in the Turkish banking sector. Banks based on this international good practice have been able to continuously increase the maturity of their IT processes. Because, in addition to the legislation created by both internal audit and external auditors every year, it has been audited within the scope of Cobit and has largely complied with the good practices recommended by the Cobit processes. All GRC frameworks obtained in the literature study, their IT relations, IT governance, and risk frameworks have been tried to be compiled, but a Cobit-like approach that mentions all IT processes of an end-to-end business has not been observed. Apart from Cobit being chosen out of legal obligation, the result from the literature study shows that Cobit is ahead of all other IT-related frameworks. Especially after the release of Cobit 4.1, it has proven to be a useful and comprehensive framework of good practice for IT-intensive businesses.

After the selection of the sector and the IT GRC model to be taken as a basis, all the main works of Cobit 2019 were scanned to establish a tailored GRC model with Cobit 2019, the latest version of Cobit. In particular, with the document called design guide, was desired to enable businesses to create a special framework for themselves. Cobit 2019 started with an important and useful model, but it also had weaknesses. The first of these, the proposed model was expected to be established with a top-down approach from the center with the participation of one or more IT governors. To strengthen this aspect, the methodology proposed by the design guide was transferred to a survey, and the method of Cobit Toolkit, which receives and processes a single opinion, is suggested to create a common model with the participation of all governing bodies stakeholders of the bank. At the same time, although it was specifically stated that the regulation dimension should provide input to the proposed model, a method on how to do this was not shared. To strengthen the regulation dimension, within the scope of this thesis, methods were researched to establish the relationship between

all banking IT-related regulation provisions and Cobit actions, and a method of creating an objective relationship matrix with LSA was proposed.

With this thesis, a tailored IT GRC model was created for a bank, this model uses Cobit 2019 design guide with a collaborative approach. The Cobit design guide is based on a unique assessment but in this thesis, a collaborative survey was created to gather the whole governing body's opinions. All the main mass was reached and assessed as a whole to create the GRC model. This model shows the importance level of Cobit's 40 governance and management processes importance level.

The sample bank's most important processes are;

- DSS 05 "Managed Security Services",
- DSS 04 "Managed Continuity"
- APO 12 Managed Risk"
- APO 13 "Managed Security"
- EDM 03 "Ensured Risk Optimization"
- MEA 03 "Managed Compliance with External Requirements"
- MEA 04 "Managed Assurance"

These results show that the bank's security management and continuity processes are the most important processes to improve, also these processes need to be more mature. After these two processes again, risk and security related to other domains (APO and EDM) processes to come. Finally, compliance management and banks' own assurance with all GRC-related controls' importance levels are higher than all other 33 Cobit processes.

Also, the mapping approach in this thesis is unique. In literature best practices mapping is generally made in high-level domains and subjective ways. There are some models to create a relation map, researchers use manual methods or UML diagrams. Some cases use language processing methods to analyze texts. Researches create relations with the main domain name or domain objective to relate two standards. The top-down approach creates complexity for subdomains or practices. Although the domain or process's name is the same their ingredients may be different. Creating a relatedness map only with a master domain or process name or definition is a top-down approach and can easily create incorrect results. But in the proposed bottom-up approach, Cobit's most detailed actions bound with the domains and processes to the regulation's every article. Latent semantic analysis' "one to many" approach helps to create relationship maps and assess two texts with predefined word-

by-word relevancy maps on a corpus. With the help of Colorado University's LSA web toolkit, the analysis made and create a static data set to use with the results of the IT GRC model. With this thesis, LSA is used as a regulation to best practice relation definition creator.

This model was created with the sufficiency of compliance dimension with the help of relatedness matrices of the model that were made with latent semantic analysis. This analysis creates effective results, a 1202*224 matrix created and its transpose to give a relatedness map between Cobit's actions and BRSA's IS and Electronic Banking regulation's articles. In the scope of this thesis, a Power BI application was created to prepare two dashboards. With these dashboards, users can analyze Cobit to regulation relatedness or regulation's Cobit relevance just by clicking filter criteria. The sample bank governing body can use this tool to evaluate their GRC models' actions or articles by the importance level. It saves time for users to assess 269.248 (1202*224) unique data.

The model gives the importance level of each process to evaluate, with the help of the created relatedness map, it can prioritize actions or articles to implement on the sample bank. The sample bank's defined most important domain evaluated as "DSS 05". Moreover, the LSA matrix gives important results such as which Cobit practices are not evaluated in regulation or which regulation article has not had a related action. Thus, users can make gap analyses in this method. While analyzing DSS 05 as an example, assessed another approach which is based on the mean values of related actions or regulation articles. By this method, a group of Cobit actions or a section's most related articles can be defined, and with the help of score sequencing overall related actions and articles can be defined easily.

Research Contributions;

- With the literature study, GRC and IT GRC have been compiled with all dimensions of the literature and the relevant sub-dimensions of governance frameworks have been compiled and the details have been presented together. GRC system and its relations with IT were associated with good practices and some standards, and the gap seen in the literature in the field of governance was tried to be eliminated. With the literature review, a systematic literature review was made by scanning the journals and academic databases that produced important academic papers in this field. The academic studies produced between 2010 and 2020 were compared with the results of the studies carried out between 2000 and 2010, and what kind of

developments in the field for 10-year periods were revealed. It has been demonstrated that the concepts of GRC and IT GRC continue to increase the interest of the academy and the industry.

- To find semantic similarities in texts, there are 5 main methods; string-based, character-based, corpus-based, knowledge-based, and hybrid similarity measurements methods. Corpus-based methods or mutual information-gathering methods could be used. This thesis suggests LSA can be used to map regulatory compliance requirements to a selected best practice. We use this semantic method to find meaning and define every regulation statement's relationship percentage of every Cobit activity to create a relatedness map.
- LSA can be used not only to establish relationship maps of good practices in relation to regulation and good practices but also to create all relationship maps between good practices. Relationships can also be established with existing relationship maps created by good practice publishers by subjective methods. For example, Cobit and ISO 27001 relationship maps have been published by ISACA. Within the scope of the thesis, the relationship map of the regulation, which has to be compatible with Cobit, has been created. Since one dimension of this map is Cobit, a relationship map can be created with all ready-to-use maps that have a common dimension. In this way, businesses that use good practices to mature their IT or business processes can spend less time and effort and have the opportunity to apply relevant good practice recommendations and practices.
- The relationship matrix created in the scope of this thesis is reported with 2 dashboards, created with Power BI. The need for maturation of IT processes was determined according to the order of importance set forth by the GRC model, and after the determination of the Cobit processes, the relevant actions were determined on created application screens where they could examine their equivalents in the regulation were designed to contribute to the governance of the bank.
- The created relationship matrix can be used not only in the bank studied as an example but also in all banks operating in the Turkish banking sector. It is planned that this matrix and application will create value for other banks and contribute to IT governance processes. Communicating with the relevant banking associations and regulatory authorities is planned to be shared with sector representatives.

- With this thesis, which contributes to the IT governance processes of the sample bank the importance and maturity levels of IT processes shared with senior managers and process owners, and reported the outputs they created with the application created and the relevant Cobit actions and regulation-related items were shared with the process owners.
- Within the scope of the thesis, the weaknesses of Cobit 2019 were also identified, and a collaborative IT GRC creation approach was proposed. With this method, a model has been proposed that will enable them to create an IT GRC model with the participation of all relevant stakeholders of a transaction based on Cobit 2019. Another important contribution is the problem that the regulation dimension cannot be taken as an input to Cobit despite its high recommendation. With the LSA-based relationship matrix, it was possible to integrate this dimension into the IT GRC model to be established. These suggested methods and the identified weaknesses are shared with ISACA to contribute to the current version that is planned to be published.

4.1. Recommendations

After creating our model and LSA-based relatedness map sample bank should create a project or a program that addresses the needs of increasing the maturity level of defined processes. This project may focus on every design factor's result and create techniques to assess these results with the related governing body. In this way, the sample bank's issues and risks can be addressed and can be solved in a collaborative environment. Because of the impact on too many business and IT processes, GRC projects need high-level sponsorship. Our advised projects' sponsor should be a chief executive or a strong partner to support results with high-level management or a board, at the same time other participants' involvement is so important to get a successful result in our GRC program.

This research covers the relatedness of two standards; Cobit and BRSA's IT-related regulation. Banks also want to implement other standards like ISO 27001 or NIST cybersecurity standards. In the future, researchers can use our LSA-based method to create a relatedness map with each standard. Also, we can implement ready use created relatedness map to bridge our created relatedness map. For example, Cobit and ISO standards are mapped by lots of parties' best practices. If a standard is mapped with Cobit we can easily implement our mapped matrices as another dimension. These increase complexity but, in the end, a bank (or a business) has a structured governance mechanism.

There are many regulations created by lots of legislative authorities. BRSA's IT-related other regulations are not valid today, and the most important regulation is our worked IS and Electronic Banking Regulation but in the telecom sector BTK (Bilgi Teknolojileri ve İletişim Kurulu; Information and Communication Technologies Authority) creates regulations that are related to lots of best practices. Some articles cover bank's operations or internet service providers affected articles effects banks indirectly. To have effective oversight and monitoring in compliance changes banks need to evaluate changes fastly, our relatedness map can be used for indirect legislations related to Cobit or other best practices, standards, or a security framework.

One of the difficulties encountered in the LSA process is the data cleaning process. Data quality can affect all data analysis processes. Data cleaning of the information to be analyzed and, in case of translation from a foreign language, must be done by experts in the subject. Developing applications that will automate data cleaning will facilitate the creation of relatedness maps by analyzing new legislation or good practices with LSA. Areas that can be automated in data cleaning, especially in the field of IT, can be developed to transfer the long versions of abbreviations, special abbreviations in the English language or the words that are divided due to reasons such as paragraph breaks can be developed.

4.2. Suggestions for Future Research

First of all, it is important that survey participants who contribute to the establishment of the IT GRC model needed to have more information about the GRC system. All these concepts were conveyed to all participants within the scope of the thesis, but due to the pandemic, the interviews and presentations were mostly conducted online. To increase the interaction, especially the meetings with the senior management were made face-to-face, if possible, and it was seen that the effect was higher. It is recommended that researchers who will work in this field in the future and who will need to inform the participants about the relevant issues, make the interviews face-to-face. In addition to GRC, in the thesis, the parties who have general knowledge about Cobit have been studied. Therefore, besides the introduction of the GRC system, it is important to provide basic information about Cobit.

In the case of using LSA in new studies to be conducted in the field, data cleaning should be done by experts in the field, and semantic distortions should be prevented after cleaning. It is possible to create a relatedness matrix of two or more good practices in LSA. By adding the 3rd dimension for researchers, cubes can be created in which the interaction of 3 different

good practices is increased. With this good practice cube, the business that chooses an area to develop can quickly obtain action-level recommendations within 3 best practices. Increasing the number of dimensions may be possible, but due to factors such as growing data and increased interpretation, each subsequent good practice should be well evaluated. With 2 or 3 separate relationship matrices, the business can perform faster evaluations.

5. REFERENCES

Abie, H., & Borking, J. J. (2012). Risk analysis methods and practices: privacy risk analysis methodology. NR-notat DART/05/2012. Norsk Regnesentral, Oslo, S, 37.

Advisera (2020, November 25). Cobit vs. ISO 27001: How much do they differ from 27001, from Advisera Academy website: https://advisera.com/27001academy/blog/2019/05/06/Cobit-vs-iso-27001-how-much-do-they-differ.

Agarwal, S., & Zhang, J. (2020). FinTech, lending and payment innovation: A review. Asia-Pacific Journal of Financial Studies, 49(3), 353-367.

Ailon, G. (2011). Mapping the cultural grammar of reflexivity: The case of the Enron scandal. Economy and Society, 40(1), 141-166.

Albu, C. N., Albu, N., & Alexander, D. (2014). When global accounting standards meet the local context—Insights from an emerging economy. Critical Perspectives on Accounting, 25(6), 489-510.

Altszyler, E., Sigman, M., Ribeiro, S., & Slezak, D. F. (2016). Comparative study of LSA vs Word2vec embeddings in small corpora: a case study in dreams database. arXiv preprint arXiv:1610.01520.

Ampazis, N., & Perantonis, S. J. (2004). LSISOM—A Latent Semantic Indexing Approach to Self-Organizing Maps of Document Collections. Neural Processing Letters, 19(2), 157-173.

Barth, J. R., Caprio, G., & Levine, R. (2013). Bank regulation and supervision in 180 countries from 1999 to 2011. Journal of Financial Economic Policy.

Behringer, G., & Hizli, M. (2021, March). Data Governance: State-of-the-Art. In International Conference on Wirtschaftsinformatik (pp. 687-699). Springer, Cham.

Beißel, S. (2017). Rahmenwerke für das IT-GRC-Management. In IT-GRC-Management–Governance, Risk und Compliance (pp. 65-81). Springer Vieweg, Wiesbaden.

Beißel, S., Ionita D, Hartel P, Pieters W, Wieringa RJ (2013) Current established risk assessment methodologies and tools. Technical Report TR-CTIT-14-04, Centre for Telematics and Information Technology, University of Twente, Enschede.

Bellegarda, J. R. (2007). Latent semantic mapping: Principles & applications. Synthesis Lectures on Speech and Audio Processing, 3(1), 1-101.

Bharadwaj, A., El Sawy, O., Pavlou, P., & Venkatraman, N. (2013). Digital business strategy:

Böhm, M. (2008). IT-Compliance als Triebkraft von Leistungssteigerung und Wertbeitrag der IT. HMD Praxis der Wirtschaftsinformatik, 45(5), 15-29.

Bradford, R. B. (2005, May). Efficient discovery of new information in large text databases. In International Conference on Intelligence and Security Informatics (pp. 374-380). Springer, Berlin, Heidelberg.

Bradford, R. B. (2006, May). Application of latent semantic indexing in generating graphs of terrorist networks. In International Conference on Intelligence and Security Informatics (pp. 674-675). Springer, Berlin, Heidelberg.

Brand, K., & Boonen, H. (2007). IT governance based on CobiT® 4.1-A management guide. Van Haren.

Brennan, N. (2006). Boards of directors and firm performance: is there an expectations gap?. Corporate Governance: An International Review, 14(6), 577-593.

Brooks, R. D., Faff, R. W., McKenzie, M. D., & Ho, Y. K. (2000). US banking sector risk in an era of regulatory change: a bivariate GARCH approach. Review of Quantitative Finance and Accounting, 14(1), 17-43.

Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. Communications of the Association for Information Systems, 15(1), 696–712.

BRSA (2020). Information Systems of Banks and Electronic Banking regulations About Services, from Resmigazete.gov.tr website: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm

BRSA. (2020, April 20), Banking Regulation Updates from Bddk.org.tr website: https://www.bddk.org.tr/Announcement/Turkey-s-banking-regulatory-and-supervisory-framework-is-fully-in-line-with-international-standards/580 (2020). Retrieved 11 April 2020, from https://www.bddk.org.tr/ContentBddk/dokuman/duyuru_0580_01.pdf

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic'in literature reviews. Formulating research methods for information systems, 48-78.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Campanella, F., Della Peruta, M. R., & Del Giudice, M. (2017). The effects of technological innovation on the banking sector. Journal of the Knowledge Economy, 8(1), 356-368.

Caron, J. (2000). Applying lsa to online customer support: A trial study. Retrieved March, 13, 2006.

Chergui, M., & Chakir, A. (2020). IT GRC smart adviser: Process driven architecture applying an integrated framework. Advances in Science, Technology and Engineering Systems, 5(6), 247-255.

Chew, E. K., & Gottschalk, P. (Eds.). (2009). Information Technology Strategy and Management: Best Practices: Best Practices. IGI Global.

Choi, J. J., Park, S. W., & Yoo, S. S. (2007). The value of outside directors: Evidence from corporate governance reform in Korea. Journal of financial and Quantitative Analysis, 42(4), 941-962.

Ciffolilli, A., & Muscio, A. (2018). Industry 4.0: national and regional comparative advantages in key enabling technologies. European Planning Studies, 26(12), 2323-2343.

Cortada, J. W. (1998). Best practices in information technology: How corporations get the most value from exploiting their digital investments. Prentice-Hall, Inc.

Da Silva, H. C. C., Araújo, M. A. V., & Dornelas, J. S. (2018). Determinantes da não utilização de frameworks de gestão e/ou governança de TI. Revista Gestão & Tecnologia, 18(2), 274-299.

Daily, C. M., Dalton, D. R., & Cannella Jr, A. A. (2003). Corporate governance: Decades of dialogue and data. Academy of management review, 28(3), 371-382.

Davis, J., Frankforter, S., Vollrath, D., & Hill, V. (2007). An empirical test of stewardship theory. Journal of Business & Leadership: Research, Practice, and Teaching (2005-2012), 3(1), 40-50.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. In Enterprise governance of information technology (pp. 125-162). Springer, Cham.

De Smet, D., & Mayer, N. (2016, October). Integration of it governance and security risk management: A systematic literature review. In 2016 International Conference on Information Society (i-Society) (pp. 143-148). IEEE.

Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., & Harshman, R. (1990). Indexing by latent semantic analysis. Journal of the American society for information science, 41(6), 391-407.

Denhière, G., & Lemaire, B. (2004). A computational model of children's semantic memory. In Proceedings of the Annual Meeting of the Cognitive Science Society (Vol. 26, No. 26).

Denis, D. K. (2001). Twenty-five years of corporate governance research… and counting. Review of financial economics, 10(3), 191-212.

Denis, D. K., & McConnell, J. J. (2003). International corporate governance. Journal of financial and quantitative analysis, 38(1), 1-36.

Denis, D. K., & McConnell, J. J. (2003). International corporate governance. Journal of financial and quantitative analysis, 38(1), 1-36.

Dumais, S. (1994). Latent semantic indexing (LSI) and TREC-2. Nist Special Publication Sp, 105-105.

Dumais, S. T. (1995). Latent semantic indexing (LSI): TREC-3 report. Nist Special Publication SP, 219-219.

Dumais, S. T., Furnas, G. W., Landauer, T. K., Deerwester, S., & Harshman, R. (1988, May). Using latent semantic analysis to improve access to textual information. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 281-285).

Edwards, J., & Wolfe, S. (2004). The compliance function in banks. Journal of financial regulation and compliance.

Falk, M. (2012). IT-Compliance in der Corporate Governance: Anforderungen und Umsetzung. Springer-Verlag.

Fama, E. F. (1980). Agency Problems and the Theory of the Firm, 88 J. Pol. Econ, 288(10.2307), 1837292288.

Fettke, P. (2006). State-of-the-Art des State-of-the-Art. Wirtschaftsinformatik, 48(4), 257-266.

Fettke, P., & Loos, P. (Eds.). (2006). Reference modeling for business systems analysis. Igi Global.

Foltz, P. W., & Dumais, S. T. (1992). Personalized information delivery: An analysis of information filtering methods. Communications of the ACM, 35(12), 51-60.

Foltz, P. W., Laham, D., & Landauer, T. K. (1999). Automated essay scoring: Applications to educational technology. In Edmedia+ innovate learning (pp. 939-944). Association for the Advancement of Computing in Education (AACE).

Forbes, D. P., & Milliken, F. J. (1999). Cognition and corporate governance: Understanding boards of directors as strategic decision-making groups. Academy of management review, 24(3), 489-505.

Gálvez, R. H., & Gravano, A. (2017). Assessing the usefulness of online message board mining in automatic stock prediction systems. Journal of Computational Science, 19, 43-56.

Garrity, J. T. (1963). Top management and computer profits. Harvard Business Review, 41(4), 6-12.

Gartner. (2019, November 20). Gartner says global IT spending to reach $3.8 Trillion in 2019. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2019-01-28-gartner-says-global-itspending- to-reach–3-8-trillio.

Gartner. (2021, March 12), Gartner Says Global IT Spending to Reach $3.9 Trillion in 2020January 2021, from https://www.gartner.com/en/newsroom/press-releases/2020-01-15-gartner-says-global-it-spending-to-reach-3point9-trillion-in-2020

Gartner. (2022, March 12), IT Spending Forecast: Technology Trends Accelerated by COVID. from https://www.gartner.com/en/webinars/3989289/it-spending-forecast-3q20-technology-trends-accelerated-by-covid

Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: Empirical evidence from the literature. Risk Management and Insurance Review, 18(1), 29-53.

Gee, K. R. (2003, March). Using latent semantic indexing to filter spam. In Proceedings of the 2003 ACM symposium on Applied computing (pp. 460-464).

Gericke, A., Fill, H. G., Karagiannis, D., & Winter, R. (2009, May). Situational method engineering for governance, risk and compliance information systems. In Proceedings of the 4th international conference on design science research in information systems and technology (pp. 1-12).

Gill, A. Q., Loumish, A., Riyat, I., & Han, S. (2018). DevOps for information management systems. VINE Journal of Information and Knowledge Management Systems.

Gill, S., & Purushottam, U. (2008). Integrated GRC-is your organization ready to move. Governance, Risk and Compliance, 37-46.

Gillan, S. L. (2006). Recent developments in corporate governance: An overview. Journal of corporate finance, 12(3), 381-402.

Gillan, S., & Starks, L. T. (1998). A survey of shareholder activism: Motivation and empirical evidence. Available at SSRN 663523.

Gomaa, W. H., & Fahmy, A. A. (2013). A survey of text similarity approaches. International journal of Computer Applications, 68(13), 13-18.

Gong, Y., & Liu, X. (2001, September). Generic text summarization using relevance measure and latent semantic analysis. In Proceedings of the 24th annual international ACM SIGIR conference on Research and development in information retrieval (pp. 19-25).

Gordon, M. D., & Dumais, S. (1998). Using latent semantic indexing for literature based discovery. Journal of the American Society for Information Science, 49(8), 674-685.

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT consumerization and the transformation of IT governance. Mis Quarterly, 42(4), 1225-1253.

Greuning, H. V., & Brajovic-Bratanovic, S. (2022). Analyzing banking risk: a framework for assessing corporate governance and risk management.

Hellwig, M. F. (2009). Systemic risk in the financial sector: An analysis of the subprime-mortgage financial crisis. De economist, 157(2), 129-207.

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. IBM systems journal, 38(2.3), 472-484.

Hirschheim, R., & Sabherwal, R. (2001). Detours in the path toward strategic information systems alignment. California Management Review, 44 (1), 87-108.

How CIOs should think about business value. (2020, March 20), from McKinsey & Company website: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-cios-should-think-about-business-value

Huff, S. L., Maher, P. M., & Munro, M. C. (2004). What boards don't do-but must do-about information technology. Ivey Business Journal Online, 69(1), 1-4.

Huff, S. L., Maher, P. M., & Munro, M. C. (2006). Information technology and the board of directors: Is there an IT attention deficit?. MIS Quarterly Executive, 5(2).

Huygh, T., & De Haes, S. (2016). Exploring the research domain of IT governance in the SME context. International Journal of IT/Business Alignment and Governance (IJITBAG), 7(1), 20-35.

Huyut, M. M., Kocaoğlu, B., & Meram, U. (2022). Regulation Relatedness Map Creation Method with Latent Semantic Analysis. Computers, Materials, and Continua.

Impressions from Delivering Cobit 2019 Foundation Training for Auditors. (2019, March 20), from Isaca.org website: https://www.isaca.org/resources/news-and-trends/newsletters/Cobit-focus/2019/impressions-from-delivering-Cobit-2019-foundation-training-for-auditors

Institute of Directors in Southern Africa. (2019, August 20). King III code of corporate governance for South Africa. Retrieved from https://jutalaw.co.za/uploads/King_III_Report/.

Ionita, D. (2013). Current established risk assessment methodologies and tools (Master's thesis, University of Twente).

ISACA (2012), "COBIT-5 A business framework for the governance and management of enterprise IT", ISBN 978-1-60420-237-3, USA.

ISACA (2012), "COBIT-5 Enabling processes", ISBN 978-1-60420-239-7, USA.

ISACA (2012), "COBIT-5 Implementation", ISBN 978-1-60420-238-0, USA.

ISACA. (2009). The Risk IT Framework. ISACA.

ISACA. (2018), COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution.

ISACA. (2018), COBIT 2019 Framework: Governance and Management Objectives.

ISACA. (2018), COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution.

ISACA. (2018), Implementing the NIST Cybersecurity Framework Using COBIT 2019.

ISACA. (2018). Cobit 2019 Framework: Introduction & methodology & Enabling & Design Guides and Toolkit.

Islam, M. M., & Hoque, A. L. (2010, December). Automated essay scoring using generalized latent semantic analysis. In 2010 13th International Conference on Computer and Information Technology (ICCIT) (pp. 358-363). IEEE.

IT Spending Forecast, 3Q20: Technology Trends Accelerated by COVID. (2020). Retrieved June 29, 2021, from Gartner website: https://www.gartner.com/en/webinars/3989289/it-spending-forecast-3q20-technology-trends-accelerated-by-covid

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. In Computer applications for security, control and system engineering (pp. 144-152). Springer, Berlin, Heidelberg.

Johannsen, A., & Kant, D. (2022). IT-Governance-, Risiko-und Compliance-Management (IT-GRC)–Ein kompetenzorientierter Ansatz für KMU. In Faktor Mensch (pp. 275-294). Springer Vieweg, Wiesbaden.

Joseph, M., McClure, C., & Joseph, B. (1999). Service quality in the banking sector: the impact of technology on service delivery. International journal of bank marketing.

Kane, G. C., & Alavi, M. (2007). Information technology and organizational learning: An investigation of exploration and exploitation processes. Organization Science, 18(5), 796-812.

Kaplan, R., & Norton, D. (1993). Putting the Balanced Scorecard to Work. Harvard Business Review, 71(5), 134- 147.

Karlin, D. IT-gestütztes Compliance Management für Geschäftsprozesse (Doctoral dissertation, Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2015).

Keller N. (2018, April 12). Informative References: What are they, and how are they used, from NIST website: https://www.nist.gov/cyberframework/online-learning/informative-references

Kiel, G. C., & Nicholson, G. J. (2002). Real world governance: Driving business success through effective corporate governance. Mt Eliza Business Review, 5(1), 17-28.

Kiel, G. C., & Nicholson, G. J. (2006). Multiple directorships and corporate performance in Australian listed companies. Corporate Governance: An International Review, 14(6), 530-546.

Kiff, M. J., Alwazir, J., Davidovic, S., Farias, A., Khan, M. A., Khiaonarong, M. T., ... & Zhou, P. (2020). A survey of research on retail central bank digital currency.

Kintsch, W., McNamara, D. S., Dennis, S., & Landauer, T. K. (2007). LSA and meaning: In theory and application. In Handbook of latent semantic analysis (pp. 479-492). Psychology Press.

Kitsios, F., Kyriakopoulou, M., & Kamariotou, M. (2022). Exploring Business Strategy Modelling with ArchiMate: A Case Study Approach. Information, 13(1), 31.

Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. Risk Management and Insurance Review, 6(1), 53-73.

Klotz, M. (2009). IT-Compliance. Ein Überblick. Dpunkt, Heidelberg.

Knoll, M., & Strahringer, S. (2017). IT-GRC-Management im Zeitalter der Digitalisierung. In IT-GRC-Management–Governance, Risk und Compliance (pp. 1-24). Springer Vieweg, Wiesbaden.

Kolesova, I. V., & Girzheva, Y. S. (2018). Impact of financial technologies on the banking sector. KnE Social Sciences, 215-220.

Kontostathis, A., & Pottenger, W. M. (2002, December). Detecting patterns in the LSI term-term matrix. In Workshop on the Foundation of Data Mining and Discovery, IEEE International Conference on Data Mining.

KPMG (2020, May 29). Integrated GRC Target Operating Model, from KPMG website: https://home.kpmg/be/en/home/insights/2020/05/rc-integrated-grc-target-operating-model.html

Kroll, M., Walters, B. A., & Wright, P. (2008). Board vigilance, director experience, and corporate outcomes. Strategic Management Journal, 29(4), 363-382.

Kukharuk, A. (2021). Competition 4.0: the new age of business transformation (Doctoral dissertation, National Aviation University).

Kurniawan, M. A., & Surendro, K. (2018, September). Similarity measurement algorithms of writing and image for plagiarism on Facebook's social media. In IOP Conference Series: Materials Science and Engineering (Vol. 403, No. 1, p. 012074). IOP Publishing.

La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (1999). Corporate ownership around the world. The journal of finance, 54(2), 471-517.

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. (2000). Investor protection and corporate governance. Journal of financial economics, 58(1-2), 3-27.

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1997). Legal determinants of external finance. The journal of finance, 52(3), 1131-1150.

Landauer, T. K. (2007). LSA as a theory of meaning. In Handbook of latent semantic analysis (pp. 15-46). Psychology Press.

Landauer, T. K., Foltz, P. W., & Laham, D. (1998). An introduction to latent semantic analysis. Discourse processes, 25(2-3), 259-284.

Landauer, T. K., Laham, D., & Derr, M. (2004). From paragraph to graph: Latent semantic analysis for information visualization. Proceedings of the National Academy of Sciences, 101(suppl 1), 5214-5219.

Laudon, K. C., & Laudon, J. P. (2018). Management information systems (15 ed., global edition). New York: Pearson Education.

Lawrence, P. R., & Lorsch, J. W. (1967). Organization and environment. Boston, MA: Harvard Business School, Division of Research.

Leavitt, S. D., & Dubner, S. J. (2005). Freakonomics. A Rogue Economist Explores the Hidden Side of Everything. William Morrow.

Lemaire, B., & Denhière, G. (2004). Incremental construction of an associative network from a corpus. In Proceedings of the Annual Meeting of the Cognitive Science Society (Vol. 26, No. 26).

Lemaire, B., & Denhière, G. (2004). Incremental construction of an associative network from a corpus. In Proceedings of the Annual Meeting of the Cognitive Science Society (Vol. 26, No. 26).

Lenhard, W., Baier, H., Hoffmann, J., & Schneider, W. (2007). Automatische Bewertung offener Antworten mittels Latenter Semantischer Analyse. Diagnostica, 53(3), 155-165.

Loh, L., & Venkatraman, N. (1992). Diffusion of information technology outsourcing: influence sources and the Kodak effect. Information systems research, 3(4), 334-358.

Long, G. (2017). The Importance of GRC in the Enterprise. Available at SSRN 2951123.

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. International Journal of Accounting Information Systems, 15(1), 66-81.

Macarthy, R. W., & Bass, J. M. (2021, May). The Role of Skillset in the Determination of DevOps implementation Strategy. In 2021 IEEE/ACM Joint 15th International Conference on Software and System Processes (ICSSP) and 16th ACM/IEEE International Conference on Global Software Engineering (ICGSE) (pp. 50-60). IEEE.

Magerman, T., Van Looy, B., Baesens, B., & Debackere, K. (2011). Assessment of Latent Semantic Analysis (LSA) text mining algorithms for large scale mapping of patent and scientific publication documents. FBE Research Report MSI_1114.

Maletic, J. I., & Marcus, A. (2000, November). Using latent semantic analysis to identify similarities in source code to support program understanding. In Proceedings 12th IEEE internationals conference on tools with artificial intelligence. ICTAI 2000 (pp. 46-53). IEEE.

Marchant, G. E., & Wallach, W. (2015). Coordinating technology governance. Issues in Science and Technology, 31(4), 43.

Martin, D. I., & Berry, M. W. (2007). Mathematical foundations behind latent semantic analysis. Handbook of latent semantic analysis, 35-56.

Mayer, N., Barafort, B., Picard, M., & Cortina, S. (2015, September). An ISO compliant and integrated model for IT GRC (governance, risk management, and compliance). In European Conference on Software Process Improvement (pp. 87-99). Springer, Cham

Meckling, W. H., & Jensen, M. C. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of financial economics, 3(4), 305-360.

Mitchell, S. (2017). GRC Capability Model (Red Book) in Paperback. Lulu. com.

Mitchell, S. L. (2007). GRC360: A framework to help organizations drive principled performance. International Journal of Disclosure and Governance, 4(4), 279-296.

Monay, F., & Gatica-Perez, D. (2003, November). On image auto-annotation with latent space models. In Proceedings of the eleventh ACM international conference on Multimedia (pp. 275-278).

Mueller, D. C. (2006). Corporate governance and economic performance. International Review of Applied Economics, 20(5), 623-643.

Müller, G., & Terzidis, O. (2008). IT-Compliance und IT Governance. Wirtschaftsinformatik, 50(5), 341-343.

Nakov, P., Popova, A., & Mateev, P. (2001). Weight functions impact on LSA performance. Euro Conference RANLP, 2001.

NIST (2010, March 20) FISMA Implementation Project | CSRC. Retrieved March 8, 2020, from Nist.gov website: https://csrc.nist.gov/projects/risk-management/risk- management-framework-(RMF)-Overview

Blank, R., & Gallagher, P. (2012). Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1, Joint Task Force Transformation Initiative. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

NIST (2018, April 20), Guide for applying the risk management framework to federal information systems a security life cycle approach, NIST Special Publication, Revision 1. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Noonan, C., & Watson, S. (2007). The foundations of corporate governance in New Zealand: A post-contractualist view of the role of company directors. New Zealand Universities Law Review, 22, 649-681.

NormShield (2019, November 11), Using the FAIR Model to Quantify Third-Party Cyber Risk from NormShield Cyber Risk Scorecard website: https://www.normshield.com/using-the-fair-model-to-quantify-third-party-cyber-risk/

OCEG. (2021, April 21). GRC Capability Model- Red Book version 3.0. from OCEG website: https://go.oceg.org/grc-capability-model-red-book/

OCEG. (2021, April 21). OCEG – GRC Standarts (GRC). From OCEG website: https://www.oceg.org/standards/

OCEG. (2021, April 21). OCEG- The ultimate Resource for Governance, Risk and Compliance (GRC)., from OCEG website: https://www.oceg.org/

Oparaugo, C. (2014). ISO/IEC-27001 Process Mapping to COBIT 4.1 to Derive a Balanced Scorecard for IT Governance., ISACA.

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. Information Systems Frontiers, 18(6), 1251-1263.

Parent, M., & Reich, B. H. (2007). Building Better Boards: Governing IT Risk.

Parent, M., & Reich, B. H. (2009). Governing information technology risk. California Management Review, 51(3), 134-152.

Peltier, TR. (2014). Risk management: the facilitated risk analysis and assessment process. Information security fundamentals, 2. Aufl. CRC Press, Boca Raton, S 59–108.

Pérez-Castillo, R., Delgado, A., Ruiz, F., Bacigalupe, V., & Piattini, M. (2022). A method for transforming knowledge discovery metamodel to ArchiMate models. Software And Systems Modeling, 21(1), 311-336.

Peterson, R. R. (2004). Integration strategies and tactics for information technology governance. In Strategies for information technology governance (pp. 37-80). Igi Global.

Pforsich, H. D., Kramer, B. K. P., & Just, G. R. (2006). Establishing an effective internal audit department: it's a critical part of corporate governance and a good way to advance your business. Strategic Finance, 22-29.

Porta, R. L., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. Journal of political economy, 106(6), 1113-1155.

PricewaterhouseCoopers. (2019, March 28). GRC (Governance, Risk and Compliance), from PwC website: https://www.pwc.com.tr/governance-risk-and-compliance-services

Quesado, P. R., Aibar Guzmán, B., & Lima Rodrigues, L. (2018). Advantages and contributions in the balanced scorecard implementation. Intangible capital, 14(1), 186-201.

Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (GRC) status quo and software use: results from a survey among large enterprises.

Racz, N., Weippl, E., & Bonazzi, R. (2011, July). IT governance, risk & compliance (GRC) status quo and integration: An explorative industry case study. In 2011 IEEE World Congress on Services (pp. 429-436). IEEE.

Racz, N., Weippl, E., & Seufert, A. (2010, July). A process model for integrated IT governance, risk, and compliance management. In Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010) (pp. 155-170).

Racz, N., Weippl, E., & Seufert, A. (2010, May). A frame of reference for research of integrated governance, risk and compliance (GRC). In IFIP International Conference on Communications and Multimedia Security (pp. 106-117). Springer, Berlin, Heidelberg.

Racz, N., Weippl, E., & Seufert, A. (2011). Integrating IT governance, risk, and compliance management processes. In Databases and Information Systems VI (pp. 325-338). IOS Press.

Racz, N., Weippl, E., & Seufert, A. (2011, January). Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives. In 2011 44th Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

Rath, M., & Sponholz, R. (2009). IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen. Erich Schmidt Verlag GmbH & Co KG.

Raja, J., & Kumar, A. S. (2007). SME entrepreneurship, firm performance, and corporate governance practices in Indian service firms. Journal of Services Research, 7(2), 99.

Ramesh, N. (2021). Outsourcing Your Information Technology Support? Some Key Lessons in How to Make It Work for Your Organization. IEEE Engineering Management Review, 49(2), 16-17.

Riivari, J. (2005). Mobile banking: a powerful new marketing and CRM tool for financial services companies all over Europe. Journal of Financial Services Marketing, 10(1), 11-20.

RIMS (2006, August 19), RIMS Risk Maturity Model (RMM) for enterprise risk management. http://rims.logicmanager.com/LogicERM/documents/rims_rmm_full_version.pdf

Rieger, L. (2021). The semantic analysis of philosophical texts. In The Prague School (pp. 83-102). University of Texas Press.

Ritchie, L. D. (2008). Book Review: Landauer, TK, McNamara, DS, Dennis, S., & Kintsch, W.(Eds.).(2007). Handbook of Latent Semantic Analysis. Mahwah, NJ: Lawrence Erlbaum. Journal of Language and Social Psychology, 27(3), 300-306.

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. MIT Sloan Management Review, 59(2), 12-15.

Rozanova, N. M. (2021). Contemporary Competition: Process or Result?. Mirovaia ekonomika mezhdunarodnye otnosheniia, 65(8), 5-13.

Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. Computer standards & interfaces, 63, 67-82.

Sambamurthy, V., & Zmud, R. (1999). Arrangements for information technology governance: A theory of multiple contingencies. Management Information Systems Quarterly, 23(2), 261–290.

Sambamurthy, V., & Zmud, R. W. (2000). Research commentary: The organizing logic for an enterprise's IT activities in the digital era A prognosis of practice and a call for research. Information Systems Research, 11(2), 105–114.

Sarkar, A., Marjit, U., & Biswas, U. (2014, January). A conceptual model to develop an advanced plagiarism checking tool based on semantic matching. In 2014 2nd International Conference on Business and Information Management (ICBIM) (pp. 104-108). IEEE.

Sarno, R., Sanjoyo, B.A., Mukhlash, I., Astuti, H.M. 2013. Petri Net model of ERP business process variation for Small and Medium Enterprises. Journal of Theoretical and Applied Information Technology

Sen, A. (2021). DevOps, DevSecOps, AIOPS-paradigms to IT operations. In Evolving technologies for computing, communication and smart world (pp. 211-221). Springer, Singapore.

Sharma, S., & Sharma, S. K. (2020). Probing the links between team resilience, competitive advantage, and organizational effectiveness: Evidence from information technology industry. Business Perspectives and Research, 8(2), 289-307.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. The journal of finance, 52(2), 737-783.

Simonsson, M. (2008). Predicting it governance performance: A method for model-based decision making (Doctoral dissertation, KTH).

Soboroff, I. M., Nicholas, C. K., Kukla, J. M., & Ebert, D. S. (1997, November). Visualizing document authorship using n-grams and latent semantic indexing. In Proceedings of the 1997 workshop on New paradigms in information visualization and manipulation (pp. 43-48).

Sowa, A. (2011). Metriken–der Schlüssel zum erfolgreichen Security und Compliance Monitoring. Wiesbaden: Vieweg+ Teubner Verlag.

Strasser, A., & Wittek, M. (2012). IT-Compliance. Informatik-Spektrum, 35(1), 39-44.

Successful Governance, Risk and Compliance within reach - Compact. (2018, December 6), from Compact website: https://www.compact.nl/articles/successful-governance-risk-and-compliance-within-reach/

Surah Ash-Sharh - 1-8 - Quran.com. (2022). Retrieved July 8, 2022, from Quran.com website: https://quran.com/ash-sharh

Svatá, V., & Fleischmann, M. (2011). IS/IT risk management in banking industry. Acta oeconomica pragensia, 19(3), 42-60.

TAC A.S. (2021, January 10). TAC CONIG from Conig.org website: http://www.conig.org/document

Teubner, A., & Feller, T. (2008). Informationstechnologie, Governance und Compliance. Wirtschaftsinformatik, 50(5), 400-407.

Tiwana, A., & Kim, S. K. (2015). Discriminating IT governance. Information Systems Research, 26(4), 656–674.

Topçu, S., & Metin, B. (2011, November). Organizing COBIT control objectives for effective information technology compliance. In 2011 IEEE 12th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 461-464). IEEE.

Toward a next generation of insights. MIS Quarterly, 37(2), 471–482.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British journal of management, 14(3), 207-222.

Trim, P., & Lee, Y. I. (2016). Cyber security management: a governance, risk and compliance framework. Routledge.

Tvrdíková, M. (2016). Increasing the business potential of companies by ensuring continuity of the development of their information systems by current information technologies. Journal of Business Economics and Management, 17(3), 475-489.

Valentine, E., & Stewart, G. (2015). Enterprise business technology governance: Three competencies to build board digital leadership capability. In HICSS 2015 Proceedings.

Van Grembergen, W., & De Haes, S. (Eds.). (2007). Implementing information technology governance: models, practices and cases: models, practices and cases. IGI Global.

Vicente, P., & da Silva, M. M. (2011, July). A business viewpoint for integrated IT governance, risk and compliance. In 2011 IEEE World Congress on Services (pp. 422-428). IEEE.

Vicente, P., & Mira da Silva, M. (2011, June). A conceptual model for integrated governance, risk and compliance. In International Conference on Advanced Information Systems Engineering (pp. 199-213). Springer, Berlin, Heidelberg.

Wade-Stein, D., & Kintsch, E. (2004). Summary Street: Interactive computer support for writing. Cognition and instruction, 22(3), 333-362.

Weill, P., & Ross, J. (2004). IT Governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Weiss, J. & Thorogood, A. (2011). Information Technology (IT)/Business Alignment as a Strategic Weapon: A Diagnostic Tool. Engineering Management Journal, 23(2), 30-41.

Wiesche, M., Schermann, M., & Krcmar, H. (2011, September). Understanding the role of information technology for organizational control design: Risk control as new control mechanism. In IFIP International Working Conference on Governance and Sustainability in Information Systems-Managing the Transfer and Diffusion of IT (pp. 135-152). Springer, Berlin, Heidelberg.

Wikipedia Contributors. (2021, January 31). Latent semantic analysis. Retrieved April 4, 2021, from Wikipedia website: https://en.wikipedia.org/wiki/Latent_semantic_analysis#cite_note-Altszyler2017-7

Wild, F., Stahl, C., Stermsek, G., & Neumann, G. (2005). Parameters driving effectiveness of automated essay scoring with LSA.

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. Journal of Information Systems, 24(2), 107–146.

Wolfe, M. B., Schreiner, M. E., Rehder, B., Laham, D., Foltz, P. W., Kintsch, W., & Landauer, T. K. (1998). Learning from text: Matching readers and texts by latent semantic analysis. Discourse processes, 25(2-3), 309-336.

Yarowsky, D., & Florian, R. (1999). Taking the load off the conference chairs-towards a digital paper-routing assistant. In 1999 Joint SIGDAT Conference on Empirical Methods in Natural Language Processing and very Large Corpora.

Zaring, D. (2006). Best practices. NYUL Rev., 81, 294.

6. CURRICULUM VITAE

Name Surname: Mehmet Murat Huyut

P,hD: Istanbul University, Management and Organization 2011-2019, on thesis statement transferred to Piri Reis University, Business Administration 2019-2022

B, SC: Yıldız Technical University, Computer Engineering Department

M, SC: Yıldız Technical University, Master of Business Administration

Assc. D: Anadolu University, Justice

Professional Experience:

Kuveyt Turk-Head of IT Systems and Infrastructure, 2019- Continues

-IT Audit Manager, 2011-2019

Garanti Teknoloji- Software Developer, 2009-2011

Deloitte Technology Services- Software Developer, 2008-2009

Academic Experiences:

Piri Reis University- Guest Lecturer, 2018- Continues

Yıldız Technical University- Guest Lecturer, 2020-2021

Certifications:

CISA, PMP, CISM, and ISO 27001 LA, ISO 22301 LA, Cobit 5 Foundation, ISO15838, ISO 10002, and Microsoft Azure Foundation, AZ-900, SC-900.

7. PUBLICATIONS/PRESENTATIONS ON THE THESIS

M. M. Huyut, B. Kocaoğlu, Ü. Meram, "Regulation relatedness map creation method with latent semantic analysis," Computers, Materials & Continua, vol. 72, no.1, pp. 2093–2107, 2022.

M. M. Huyut, B. Kocaoğlu, Ü. Meram, "A Collaborative Approach to Create IT GRC Modal with COBIT 2019," V-International European Conference on Interdisciplinary Scientific Research, January 28-29, 2022, Valencia, Spain.

M. M. Huyut, B. Kocaoğlu, Ü. Meram, "GRC Models & IT Relation: A Literature Review," V-International European Conference on Interdisciplinary Scientific Research, January 28-29, 2022, Valencia, Spain.

APPENDIX A

Questionnaire (Prepared in Turkish)

Piri Reis Üniversitesi Doktora Tez Çalışması
IT GRC (Governance, Risk & Compliance; Yönetişim, Risk ve Uyum) Model Önerisi ve Uygulaması Tez çalışması Prof. Dr. Batuhan Kocaoğlu danışmalığı ile Mehmet Murat Huyut tarafından yapılmaktadır. Anketi doldurmak yaklaşık 20 dakika sürmektedir. Katkı sağladığınız için çok teşekkürler. Tez Başlığı; "A Model and an Application for Information Technology Governance, Risk and Compliance and Implementation in a Bank"

1.Lütfen Bankadaki görevinizi (unvan) belirtiniz;

_____

2.Toplam tecrübenizi yıl olarak belirtiniz;

_____

3.Kurumsal Strateji Modelinin Önemi, Aşağıda belirtilen 4 farklı stratejinin önemini 1 en önemsiz, 5 en önemli olacak şekilde belirtiniz. Stratejilerin tanımlarını görselde görebilirsiniz. (DF 1)

Strateji Modeli	Açıklama
Büyüme/Şirket Edinim	Kuruluş, büyümeye odaklanmıştır (gelirler)[2]
İnovasyon/Farklılaşma	Kuruluş müşterilerine farklı ve/veya yenilikçi ürünler ve hizmetler sunmaya odaklanmıştır.[3]
Maliyet Liderliği	Kuruluş, kısa vadede maliyet azaltmaya odaklanmıştır.[4]
Müşteri Hizmeti/İstikrar	Kuruluş istikrarlı ve müşteri-odaklı hizmet vermeye odaklanmıştır.[5]

	Önem Seviyesi 1	Önem Seviyesi 2	Önem Seviyesi 3	Önem Seviyesi 4	Önem Seviyesi 5
Büyüme/Edinim					
İnovasyon/Farklılaşma					
Maliyet Liderliği					
Müşteri Hizmetleri/İstikrar					

4. Kurumsal Amacın Önemi, Aşağıda belirtilen 13 farklı stratejinin önemini 1 en önemsiz, 5 en önemli olacak şekilde belirtiniz. Amaçların tanımlarını görselde görebilirsiniz. (DF 2)

BSC Boyutu	Kurumsal Amaç	Önem Seviyesi 1	Önem Seviyesi 2	Önem Seviyesi 3	Önem Seviyesi 4	Önem Seviyesi 5
Finansal	EG01—Rekabetçi ürün ve hizmetler portföyü					
	EG02—Yönetilen iş riski					
	EG03—Dış yasa ve düzenlemelerle uyumluluk					
	EG04—Finansal bilgi kalitesi					
Müşteri	EG05—Müşteri odaklı hizmet kültürü					
	EG06—İş hizmetleri sürekliliği ve erişilebilirliği					
Kurum İçi	EG07—Yönetim bilgisi kalitesi					
	EG08—Kurum içi iş süreçlerinin optimizasyonu					
	EG09—İş süreç maliyetlerinin optimizasyonu					

BSC Boyutu	Kurumsal Amaç	Önem Seviyesi 1	Önem Seviyesi 2	Önem Seviyesi 3	Önem Seviyesi 4	Önem Seviyesi 5
	EG10 Personel becerileri, motivasyonu ve üretkenliği					
Gelişim	EG11—İç politikalarla uyumluluk					
	EG12—Yönetilen dijital dönüşüm programları					
	EG13—Ürün ve iş inovasyonu					

5. BT Risk Kategorisinin Önemi, Aşağıda belirtilen 19 farklı risk kategorisini düşük riskten- çok yüksek riske göre belirtiniz. Örnek risk senaryoları için aşağıdaki linke bakabilirsiniz. (Appendix D) (DF 3)
https://docs.google.com/document/d/10tzil07sm8oqxJ8gsYDjg2RJNaIa6ejZGcitjYSCXI/edit?usp=sharing

	Düşük Risk	Normal Risk	Yüksek Risk	Çok Yüksek Risk
1. BT yatırımı karar verme, portföy tanımı & bakımı				
2. Program & projelerin yaşam döngüsü yönetimi				
3. BT maliyeti & gözetimi				
4. BT uzmanlığı, becerileri & davranışı				
5. Kurumsal/BT mimarisi				
6. BT Operasyonel alt yapı olayları				
7. Yetkisiz faaliyetler				
8. Yazılım uyarlama/kullanım problemleri				
9. Donanım olayları				
10. Yazılım arızaları				
11. Mantıksal ataklar (bilgisayar korsanlığı, kötücül yazılım vs)				
12. Üçüncü taraf/tedarikçi olayları				
13. Mevzuat Uyumsuzlukları				
14. Jeopolitik sorunlar (Terör, Müdahale vb.)				
15. Grev				
16. Doğa olayları (Deprem, Sel vb.)				
17. Teknoloji-tabanlı köklü değişim				
18. Çevresel durumlar (Çevre Kirliliği vb.)				
19. Veri & bilgi yönetimi				

6. BT-İlişkili Sorunlar ve Önem Seviyeleri, Aşağıda belirtilen 20 farklı sorunun yaşanma durumlarını 3 farklı kategoride belirtiniz. (DF 4)

		Sorun Yok	Sorun Var	Önemli Seviyede Sorun Var
A	İş değerine düşük katkısı olduğu algısı nedeniyle, kuruluş genelinde farklı BT birimleri arasındaki hayal kırıklığı			
B	Başarısız girişimler ya da işletme değerine düşük katkısı algısı nedeniyle iş birimleri (yani, BT müşterisi) ile BT departmanı arasındaki hayal kırıklığı			
C	BT kaynaklı veri kaybı, güvenlik ihlalleri, proje başarısızlığı ve uygulama hataları gibi önemli BT ile ilgili olaylar			
D	BT dış kaynaklarının hizmet sunumu sorunları			
E	BT ile ilgili düzenleyici veya sözleşmeden doğan gereklilikleri yerine getirememe			
F	Düşük BT performansı ile ilgili düzenli denetim bulguları veya diğer değerlendirme raporları veya raporlanan BT kalitesi veya hizmet sorunları			
G	BT yönetiminden habersiz BT harcamaları, normal BT yatırım karar mekanizmalarının ve kontrolü dışında İş Birimleri tarafından yapılan BT yatırımları			
H	Çeşitli girişimler veya diğer boşa harcanan kaynak türleri arasında yinelenmeler veya çakışmalar			
I	Yetersiz BT kaynakları, yetersiz vasıflı personel veya personel tükenmişliği / memnuniyetsizliği			
J	BT-etkin değişikliklerin ve projelerin sık sık iş ihtiyaçlarını karşılamaması ve bunların geç veya bütçe aşan teslimatları			
K	Yönetim kurulu üyeleri, yürütme veya üst düzey yöneticiler tarafından BT ile ilişki kurma konusundaki isteksizliği veya BT için kararlı bir iş sponsorluğu eksikliği			
L	BT-ilişkin kararlar için karmaşık BT işletim modeli ve/veya net olmayan karar mekanizmaları			
M	Oldukça yüksek maliyetli BT			
N	Mevcut BT mimarisi ve sistemlerinin neden olduğu yeni girişimlerin veya yeniliklerin engellenmesi veya başarısız şekilde uygulanması			
O	İş kullanıcıları ve bilgi ve/veya teknoloji uzmanlarının farklı dilleri konuşmasının yol açtığı iş ve teknik bilgi arasındaki fark			
P	Veri kalitesi ve verilerin çeşitli kaynaklara entegrasyonu ile ilgili düzenli sorunlar			
Q	Yüksek düzeyde son kullanıcı bilişim kullanımı, (diğer sorunların yanı sıra) geliştirilmekte ve kullanılmakta olan uygulamalar üzerinde denetim ve kalite kontrol eksikliği oluşturması			
R	İş birimlerinin kurumsal BT departmanının katılımı olmadan ya da çok az katkı verdiği kendi bilişim çözümlerini uygulamaları			
S	Veri mahremiyeti kurallarına uymama ve/veya habersiz olma			
T	BT kullanarak yeni teknolojilerden faydalanamama veya yenilik yapamama			

7. Tehdit Görünümü (Aşağıdaki görselde tanımlanmış olan iki kategoriyi toplamları %100 olacak şekilde dağıtınız; Örnek: Normal; %25- Yüksek; %75 gibi.) Cevap alanına manuel yazabilirsiniz. (DF 5)

Tehdit Görünümü	Açıklama
Normal	İşletme, normal tehdit seviyesi olarak kabul edilenlerin altında faaliyet göstermektedir.
Yüksek	Jeopolitik durumu, sanayi sektörü veya belirli profiller nedeniyle işletme yüksek tehdit içeren bir ortamda faaliyet göstermektedir.

Yanıtınız;

_____

8. Uyumluluk Gereksinimi Önemi (Aşağıdaki görselde tanımlanmış olan 3 kategoriyi toplamları %100 olacak şekilde dağıtınız; Örnek: Yüksek; %50; Normal;%25; Düşük; %25 gibi.) Cevap alanına manuel yazabilirsiniz.
(DF 6)

Düzenleyici Ortam	Açıklama
Düşük uyumluluk gereksinimleri	İşletme, ortalamanın altında minimum bir dizi düzenli uyumluluk gereksinimlerine tabidir.
Normal uyumluluk gereksinimleri	İşletme, farklı endüstrilerde yaygın olan bir dizi düzenli uyumluluk gereksinimlerine tabidir.
Yüksek uyumluluk gereksinimleri	İşletme, çoğunlukla sanayi sektörü veya jeopolitik koşullarla ilgili olarak, ortalamanın üzerinde bir uyumluluk gereksinimlerine tabidir.

Yanıtınız;

_____

9. BT Rolünün Önemi (Aşağıdaki görselde tanımlanmış olan 4 kategoriye göre 1 önemsiz, 5 en önemli olacak şekilde değerlendiriniz.) (DF 7)

BT'nin Rolü [9]	Açıklama
Destek	BT, iş sürecinin ve hizmetlerin yürütülmesi ve sürekliliği için ve bunların yenilikçi yönü için çok önemli değildir.
Fabrika	BT başarısız olursa, iş süreçlerinin ve hizmetlerinin yürütülmesi ve sürekliliği üzerinde anında bir etki oluşur. Ancak BT, iş süreçlerini ve hizmetlerini yenilemek için bir itici güç olarak görülmemektedir.
Dönüşüm	BT, iş süreçlerini ve hizmetlerini yenilemek için bir itici güç olarak görülmektedir. Ancak şu anda, iş süreçlerinin ve hizmetlerinin mevcut çalışması ve sürekliliği için BT'ye kritik bir bağımlılık yoktur.
Stratejik	BT, kuruluşun iş süreçlerini ve hizmetlerini yürütmek ve yenilemek için çok önemlidir.

	Önem Seviyesi 1	Önem Seviyesi 2	Önem Seviyesi 3	Önem Seviyesi 4	Önem Seviyesi 5
Destek					
Fabrika					
Dönüşüm					
Stratejik					

10. BT Uygulama Yöntemlerinin Önemi (Aşağıdaki görselde tanımlanmış olan 3 kategoriyi toplamları %100 olacak şekilde dağıtınız; (Örnek: Çevik; %10; DevOps; %20; Geleneksel; %50; Karma %20) Cevap alanına manuel yazabilirsiniz. (DF 8)

BT Uygulama Yöntemi	Açıklama
Çevik	İşletme yazılım geliştirmesi için çevik geliştirme çalışma yöntemlerini kullanır.
DevOps	İşletme yazılım oluşturma, uygulama ve operasyonları için DevOps çalışma yöntemlerini kullanır.
Geleneksel	İşletme yazılım geliştirmede şelale gibi daha klasik bir yaklaşım kullanır ve yazılım geliştirmeyi operasyonlardan ayırır.
Karma	İşletme genellikle "çift modlu BT" olarak adlandırılan geleneksel ve modern BT uygulama yöntemlerinin bir karışımını kullanır.

Yanıtınız;

_____

11. Teknoloji Benimseme Stratejisinin Önemi (Aşağıdaki görselde tanımlanmış olan 3 kategoriyi toplamları %100 olacak şekilde dağıtınız; Örnek: İlk Benimseyen; %70- Takip; %20- Yavaş Benimseyen; %10 gibi.) Cevap alanına manuel yazabilirsiniz. (DF 9)

Teknoloji Benimseme Stratejisi	Açıklama
İlk Benimseyen	İşletme genellikle yeni teknolojileri mümkün olan en erken zamanda benimsemekte ve ilk avantajı elde etmeye çalışmaktadır.
Takipçi	İşletme normal olarak yeni teknolojileri benimsemeden önce bunların yaygınlaşmasını ve kanıtlanmasını bekler.
Yavaş Benimseyen	İşletme yeni teknolojileri çok geç benimser.

Yanıtınız;

_____

APPENDIX B

"DF 1 Mapping Table; Enterprise Strategies to Governance and Management Objectives"

B2 to E41 DF1 Map Matrix;

	A	B	C	D	E
1	DF1	Growth / Acquisition	Innovation / Differentiation	Cost Leadership	Client Service / Stability
2	EDM01	1.0	1.0	1.5	1.5
3	EDM02	1.5	1.0	2.0	3.5
4	EDM03	1.0	1.0	1.0	2.0
5	EDM04	1.5	1.0	4.0	1.0
6	EDM05	1.5	1.5	1.0	2.0
7	APO01	1.0	1.0	1.0	1.0
8	APO02	3.5	3.5	1.5	1.0
9	APO03	4.0	2.0	1.0	1.0
10	APO04	1.0	4.0	1.0	1.0
11	APO05	3.5	4.0	2.5	1.0
12	APO06	1.5	1.0	4.0	1.0
13	APO07	2.0	1.0	1.0	1.0
14	APO08	1.0	1.5	1.0	3.5
15	APO09	1.0	1.0	1.5	4.0
16	APO10	1.0	1.0	3.5	1.5
17	APO11	1.0	1.0	1.0	4.0
18	APO12	1.0	1.5	1.0	2.5
19	APO13	1.0	1.0	1.0	2.5
20	APO14	1.0	1.0	1.0	1.0
21	BAI01	4.0	2.0	1.5	1.5
22	BAI02	1.0	1.0	1.5	1.0
23	BAI03	1.0	1.0	1.5	1.0
24	BAI04	1.0	1.0	1.0	3.0
25	BAI05	4.0	2.0	1.0	1.5
26	BAI06	2.0	2.0	1.0	1.5
27	BAI07	1.5	2.0	1.0	1.5
28	BAI08	1.0	3.5	1.0	1.0
29	BAI09	1.0	1.0	1.0	1.0
30	BAI10	1.0	1.0	1.0	1.0
31	BAI11	3.5	3.0	1.5	1.0
32	DSS01	1.0	1.0	1.0	1.5
33	DSS02	1.0	1.0	1.0	4.0
34	DSS03	1.0	1.0	1.0	3.0
35	DSS04	1.0	1.0	1.0	4.0
36	DSS05	1.0	1.0	1.0	2.5
37	DSS06	1.0	1.0	1.0	1.5
38	MEA01	1.0	1.0	1.0	1.0
39	MEA02	1.0	1.0	1.0	1.0
40	MEA03	1.0	1.0	1.0	1.0
41	MEA04	1.0	1.0	1.0	1.0

D7 to E10 DF1 Matrix;

	A	D	E
1	Value	Importance (1-5)	Baseline
7	Growth/Acquisition		3.00
8	Innovation/Differentiation		3.00
9	Cost Leadership		3.00
10	Client Service/Stability		3.00

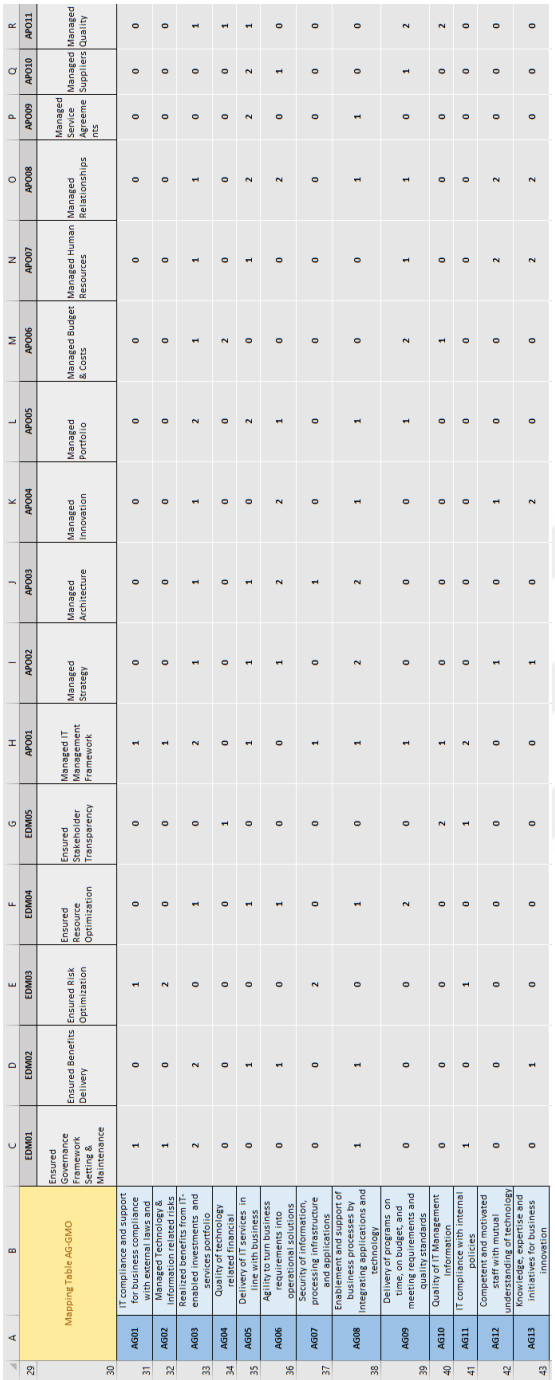
APPENDIX C

"DF 2 Mapping Table-Enterprise Goals to Alignment Goals Metrics and Individual Matrices"*

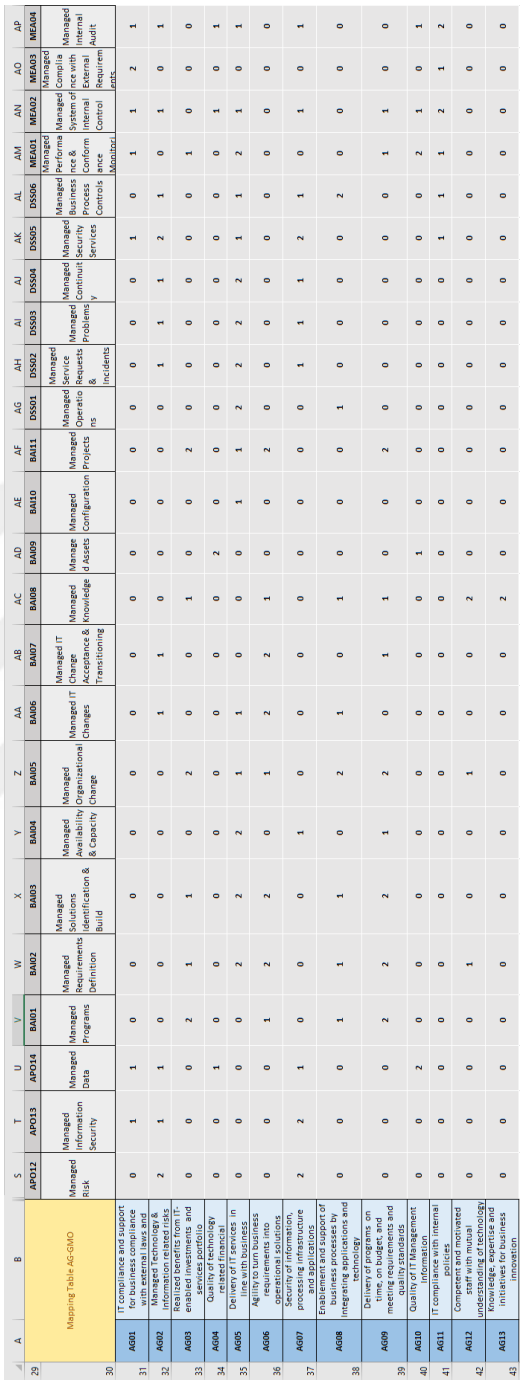
C9 to O21, DF2 Map Matrix;

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
7			AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
8		Mapping table EG-GA	IT compliance and support for business compliance with external laws and regulations	Managed Technology & information related risks	Realized benefits from IT-enabled investments and services portfolio	Quality of technology related financial information	delivery of IT services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastucture and applications	Enablement and support of business processes by integrating applications and technology	Delivery of programs on time, on budget, and meeting requirements and quality standards	Quality of IT Management information	IT compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business.	Knowledge, expertise and initiatives for business innovation
9	EG01	Portfolio of agile and competitive products and services	0	0	1	0	2	2	0	2	2	0	0	0	2
10	EG02	Managed business risks	1	2	0	0	0	0	1	0	0	0	1	0	0
11	EG03	Compliance with external laws and regulations	2	0	0	0	0	0	0	0	0	0	2	0	0
12	EG04	Transparency and accuracy of financial information	0	0	0	2	0	0	0	0	0	2	0	0	0
13	EG05	Customer-oriented service culture	0	0	1	0	1	1	0	2	1	0	0	1	0
14	EG06	Business service continuity and availability	0	1	0	0	1	0	2	0	0	0	0	0	0
15	EG07	Quality of management information	0	0	0	2	0	0	0	0	0	2	0	0	0
16	EG08	Optimisation of business process functionality	0	0	1	0	1	1	0	1	1	0	0	0	0
17	EG09	Optimization of business process costs	0	0	1	2	0	0	0	0	1	1	0	0	0
18	EG10	Staff skills, motivation and productivity	0	0	0	0	0	0	0	1	0	0	0	2	0
19	EG11	Compliance with internal policies	1	0	0	0	0	0	0	0	0	0	2	0	0
20	EG12	Managed business transformation programs	0	0	2	0	1	1	0	2	2	0	0	0	1
21	EG13	Product and business innovation	0	0	0	0	0	1	0	1	1	0	0	0	2

C31 to R43, DF2 Map;



S31 to AP43, DF2 Map;



“Mapping Table-Alignment Goals to Cobit Domains (EDM 01 to APO 11)”*

“Mapping Table-Alignment Goals to Cobit Domains (APO 12 to MEA 04)”*

*0 means no relation, 1 means primary, and 2 means secondary relation defined by ISACA.

APPENDIX D

"Risk Profile Design Factor (IT Risk Categories)"

Reference	Risk Category	Example Risk Scenarios
1	IT-investment decision making, portfolio definition and maintenance	A. Programs selected for implementation misaligned with corporate strategy and priorities B. Failure of IT-related Investments to support digital strategy of the enterprise C. Selection of wrong software (in terms of cost, performance, features, compatibility, redundancy, etc.) for acquisition and implementation D. Selection of wrong infrastructure (in terms of cost, performance, features, compatibility, etc.) for implementation E. Duplication or important overlaps between different investment initiatives F. Long-term incompatibility between new investment programs and enterprise architecture G. Misallocation, inefficient management and/or competition for resources without alignment to business priorities
2	Program and projects lifecycle management	A. Failure of senior management to terminate failing projects (due to cost explosion, excessive delays, scope creep, changed business priorities) B. Budget overruns for I&T projects C. Lack of quality of I&T projects D. Late delivery of I&T projects E. Failure of third-party outsourcers to deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery)
3	IT cost and oversight	A. Extensive dependency on, and use of, user-created, user-defined, user-maintained applications and *ad hoc* solutions B. Excess cost and/or ineffectiveness of I&T-related purchases outside of the I&T procurement process C. Inadequate requirements leading to ineffective Service Level Agreements (SLAs) D. Lack of funds for I&T related investments
4	IT expertise, skills and behavior	A. Lack or mismatch of IT-related skills within IT (e.g., due to new technologies or working methods) B. Lack of business understanding by IT staff that affects service delivery/project quality C. Inability to recruit and retain IT staff D. Recruitment of unsuitable profiles because of lack of due diligence in the recruitment process E. Lack of I&T training F. Overreliance for I&T services on key staff
		D. Undocumented EA leading to inefficiencies and duplications E. Excessive number of exceptions on enterprise architecture standards
6	IT operational infrastructure incidents	A. Accidental damaging of IT equipment B. Errors by IT staff (during backup, during upgrades of systems, during maintenance of systems, etc.) C. Incorrect information input by IT staff or system users D. Destruction of data center (sabotage, etc.) by staff E. Theft of device with sensitive data F. Theft of a key infrastructure component G. Erroneous configuration of hardware components H. Intentional tampering with hardware (security devices, etc.) I. Abuse of access rights from prior roles to access IT infrastructure J. Loss of backup media or backups not checked for effectiveness K. Loss of data by cloud provider L. Operational-service interruption by cloud providers
7	Unauthorized actions	A. Tampering with software B. Intentional modification or manipulation of software leading to incorrect data C. Intentional modification or manipulation of software leading to fraudulent actions D. Unintentional modification of software leading to inaccurate results E. Unintentional configuration and change-management errors
8	Software adoption/ usage problems	A. Nonadoption of new application software by users B. Inefficient use of new software by users
9	Hardware incidents	A. System instability in wake of installing new infrastructure, leading to operational incidents (e.g., BYOD program) B. Inability of systems to handle transaction volumes when user volumes increase C. Inability of systems to handle load when new applications or initiatives are deployed D. Utilities failure (telecom, electricity) E. Hardware failure due to overheating and/or other environmental conditions like humidity F. Damaging of hardware components leading to destruction of data by internal staff G. Loss/disclosure of portable media containing sensitive data (CD, USB-drives, portable disks, etc.) H. Extended resolution time or support delays in case of hardware incidents
10	Software failures	A. Inability to use the software to realize desired outcomes (e.g., failure to make required business model or organizational changes) B. Implementation of immature software (early adopters, bugs, etc.) C. Operational glitches when new software is made operational D. Regular software malfunctioning of critical application software E. Obsolete application software (outdated, poorly documented, expensive to maintain, difficult to extend, not integrated in current architecture, etc.) F. Inability to revert back to former versions in case of operational issues with a new version G. Software-induced corrupted data(base) leading to inaccessible data

“Risk Profile Design Factor (IT Risk Categories)” (continues);

Reference	Risk Category	Example Risk Scenarios
11	Logical attacks (hacking, malware, etc.)	A. Unauthorized (internal) users trying to break into systems B. Service interruption due to denial-of-service (DoS) attack C. Website defacement D. Malware attack E. Industrial espionage F. Hacktivism G. Disgruntled employee implements a time bomb which leads to data loss H. Company data stolen through unauthorized access gained by a phishing attack I. Foreign government attacks on critical systems
12	Third-party/supplier incidents	A. Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement (e.g., through lack of supplier due diligence regarding financial viability, delivery capability and sustainability of supplier’s service) B. Accepting unreasonable terms of business from IT suppliers C. Inadequate support and services delivered by vendors, not in line with SLA D. Noncompliance with software license agreements (use and/or distribution of unlicensed software) E. Inability to transfer to alternative suppliers due to overreliance or overdependence on current supplier F. Purchase of IT services (especially cloud services) by the business without consultation /involvement of IT, resulting in inability to integrate the service with in-house services. G. Inadequate or unenforced SLA to obtain agreed services and penalties in case of noncompliance
13	Noncompliance	A. Noncompliance with national or international regulations (e.g., privacy, accounting, manufacturing, environmental, etc.) B. Lack of awareness of potential regulatory changes that may have a business impact C. Operational obstacles caused by regulations D. Failure to comply with internal procedures
14	Geopolitical issues	A. Lack of access due to disruptive incident in other premises B. Government interference and national policies impacting the business C. Targeted action from government-sponsored groups or agencies
15	Industrial action	A. Facilities and building inaccessible because of labor union strike B. Third-party providers unable to provide services because of strike C. Key staff unavailable through industrial action (e.g., transportation or utilities strike)
16	Acts of nature	A. Earthquake destroying or damaging important IT infrastructure B. Tsunami destroying critical premises C. Major storms and tropical cyclone or tornado damaging critical infrastructure D. Major wildfire E. Flooding F. Rising water table leaving critical location unusable G. Rising temperature rendering critical locations uneconomical to operate
17	Technology-based innovation	A. Failure to identify new and important technology trends B. Failure to appreciate the value and potential of new technologies C. Failure to adopt and exploit new technologies in a timely manner (functionality, process optimization, etc.) D. Failure to provide technology support new business models
18	Environmental	A. Environmentally unfriendly equipment (e.g., power consumption, packaging)
19	Data and information management	A. Discovery of sensitive information by unauthorized persons due to inefficient retaining/archiving/disposing of information B. Intentional illicit or malicious modification of data C. Unauthorized disclosure of sensitive information through email or social media D. Loss of IP and/or leakage of competitive information

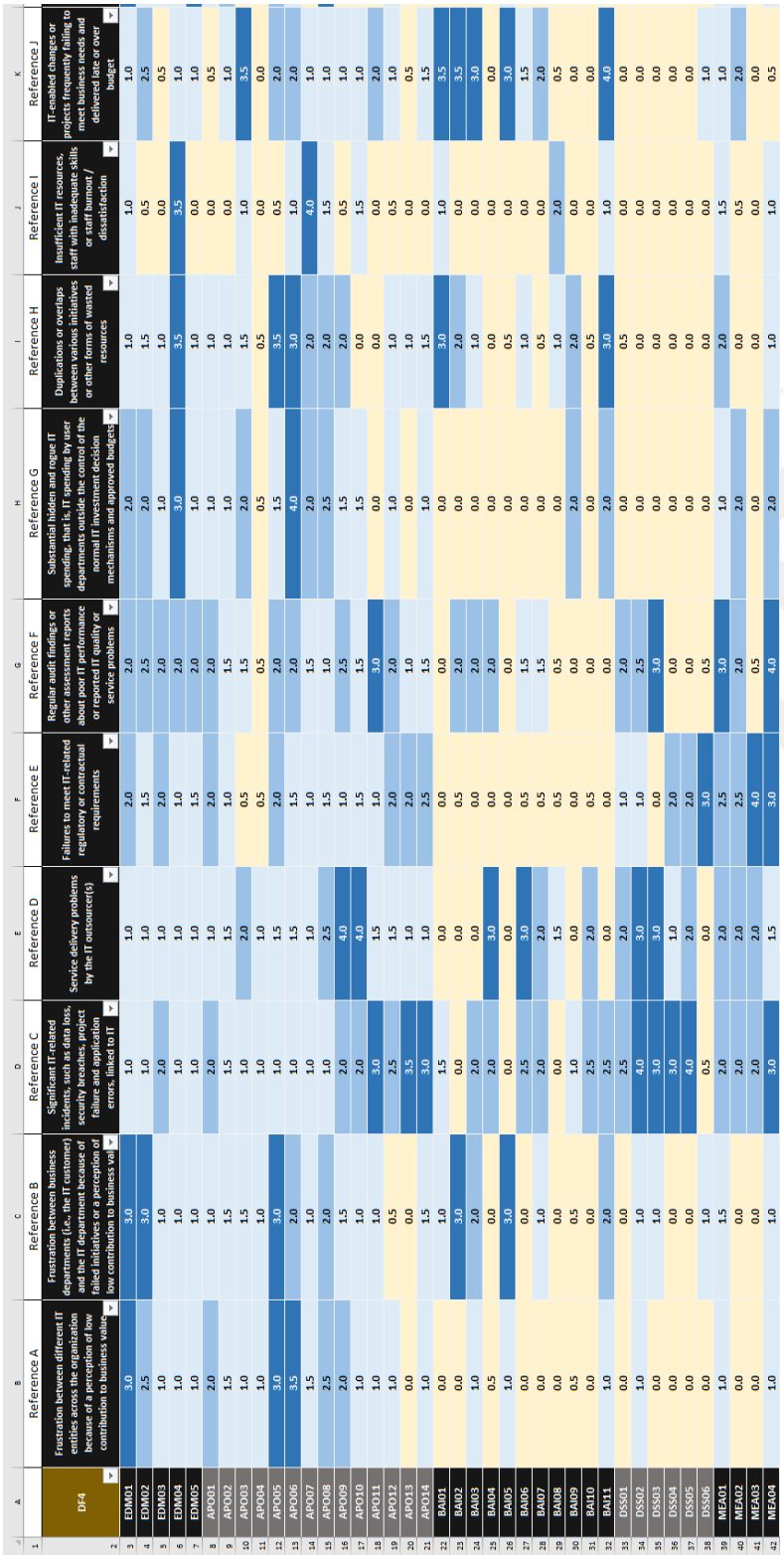
APPENDIX E

"DF3; Mapping IT Risk to Governance and Management Obj."; B3 to T42, DF 3 Map Matrix;

DF3	RISKCAT01 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCAT02 Program & Projects Life Cycle Management	RISKCAT03 IT Cost & Oversight	RISKCAT04 IT Expertise, Skills & Behavior	RISKCAT05 Enterprise/ IT Architecture	RISKCAT06 IT Operational Infrastructure Incidents	RISKCAT07 Unauthorized Actions	RISKCAT08 Software Adoption / Usage Problems	RISKCAT09 Hardware Incidents	RISKCAT10 Software Failures	RISKCAT11 Logical Attacks (Hacking, Malware, etc.)	RISKCAT12 Third-Party/ Supplier Incidents	RISKCAT13 Noncompliance	RISKCAT14 Geopolitical Issues	RISKCAT15 Industrial Action	RISKCAT16 Acts of Nature	RISKCAT17 Technology-Based Innovation	RISKCAT18 Environmental	RISKCAT19 Data & Information Management
EDM01	3.0	2.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	3.0	2.0	0.0	0.0	2.0	2.0	2.0
EDM02	3.0	2.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	3.0	1.0	3.0
EDM03	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	2.0	0.0	3.0	3.0	0.0	0.0	0.0	2.0	3.0
EDM04	3.0	0.0	4.0	3.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	1.0	0.0	2.0	0.0	0.0	2.0	3.0
EDM05	3.0	1.0	3.0	0.0	0.0	0.0	2.0	0.0	0.0	1.0	0.0	1.0	3.0	3.0	0.0	0.0	0.0	2.0	2.0
APO01	2.0	3.0	2.0	0.0	2.0	2.0	4.0	2.0	0.0	2.0	3.0	3.0	3.0	0.0	0.0	0.0	3.0	2.0	3.0
APO02	2.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	1.0	0.0	1.0	2.0	0.0	0.0	0.0	0.0	2.0	2.0	1.0
APO03	2.0	0.0	0.0	0.0	4.0	0.0	0.0	2.0	0.0	2.0	2.0	2.0	0.0	0.0	0.0	0.0	2.0	0.0	3.0
APO04	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.0	0.0	0.0
APO05	4.0	2.0	2.0	0.0	2.0	0.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0
APO06	2.0	3.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	2.0	0.0	0.0	2.0	2.0	0.0
APO07	0.0	0.0	0.0	4.0	0.0	2.0	3.0	3.0	0.0	0.0	2.0	0.0	0.0	2.0	4.0	0.0	2.0	2.0	0.0
APO08	0.0	0.0	0.0	2.0	2.0	0.0	0.0	4.0	0.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	3.0	0.0	2.0
APO09	0.0	0.0	2.0	0.0	0.0	0.0	2.0	3.0	0.0	1.0	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
APO10	0.0	2.0	3.0	0.0	0.0	0.0	2.0	2.0	3.0	2.0	2.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
APO11	0.0	3.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0
APO12	0.0	0.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	3.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0
APO13	0.0	0.0	0.0	0.0	0.0	0.0	4.0	0.0	0.0	0.0	4.0	0.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0
APO14	0.0	0.0	0.0	0.0	0.0	0.0	3.0	2.0	0.0	0.0	2.0	0.0	3.0	0.0	2.0	4.0	2.0	0.0	4.0
BAI01	0.0	4.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI02	2.0	2.0	0.0	0.0	2.0	0.0	0.0	3.0	0.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI03	0.0	3.0	0.0	0.0	2.0	0.0	0.0	2.0	0.0	3.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI04	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI05	0.0	2.0	0.0	2.0	0.0	0.0	0.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI06	0.0	0.0	0.0	0.0	0.0	3.0	4.0	0.0	0.0	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	3.0
BAI07	0.0	0.0	0.0	0.0	0.0	2.0	3.0	2.0	0.0	4.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI08	0.0	0.0	0.0	2.0	0.0	3.0	0.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	2.0
BAI09	0.0	0.0	0.0	0.0	0.0	1.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI10	0.0	0.0	0.0	0.0	0.0	2.0	4.0	0.0	0.0	2.0	3.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
BAI11	0.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS01	0.0	0.0	0.0	0.0	0.0	4.0	3.0	0.0	4.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0
DSS02	0.0	0.0	0.0	0.0	0.0	3.0	2.0	3.0	2.0	2.0	4.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS03	0.0	0.0	0.0	0.0	0.0	3.0	1.0	4.0	0.0	3.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
DSS04	0.0	0.0	0.0	0.0	0.0	3.0	3.0	0.0	3.0	0.0	4.0	0.0	2.0	0.0	3.0	4.0	0.0	0.0	2.0
DSS05	0.0	0.0	0.0	0.0	0.0	3.0	4.0	0.0	2.0	0.0	4.0	0.0	3.0	0.0	3.0	2.0	0.0	0.0	3.0
DSS06	0.0	0.0	0.0	0.0	0.0	3.0	4.0	2.0	0.0	0.0	2.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	3.0
MEA01	1.0	2.0	2.0	0.0	0.0	2.0	2.0	0.0	0.0	2.0	3.0	2.0	2.0	2.0	0.0	2.0	0.0	0.0	2.0
MEA02	1.0	2.0	2.0	0.0	0.0	3.0	3.0	0.0	0.0	2.0	3.0	2.0	2.0	3.0	0.0	2.0	0.0	0.0	2.0
MEA03	0.0	1.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0	0.0	3.0	2.0	4.0	2.0	0.0	0.0	0.0	0.0	2.0
MEA04	1.0	2.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	2.0	3.0	2.0	2.0	4.0	0.0	2.0	2.0	0.0	2.0

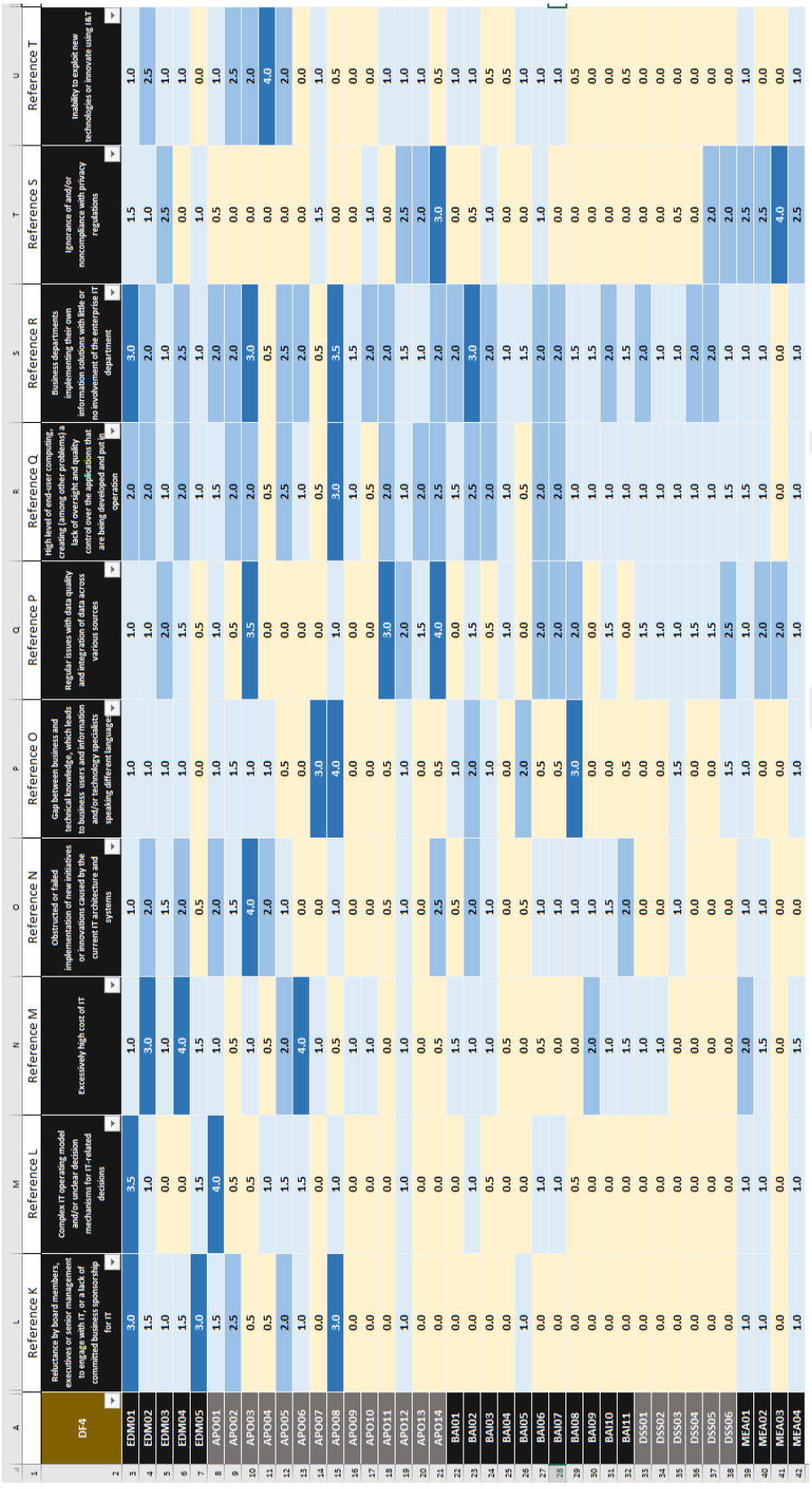
APPENDIX F

"DF4; I&T-Related Issues to Governance and Management Objectives Mapping Table"; B2 to K42, DF 4 Map Matrix;



DF4	Reference A: Frustration between different IT entities across the organization because of a perception of low contribution to business value	Reference B: Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business val	Reference C: Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	Reference D: Service delivery problems by the IT outsourcer(s)	Reference E: Failures to meet IT-related regulatory or contractual requirements	Reference F: Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	Reference G: Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	Reference H: Duplications or overlaps between various initiatives or other forms of wasted resources	Reference I: Insufficient IT resources, staff with inadequate skills or staff burnout / dissatisfaction	Reference J: IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
EDM01	3.0	3.0	1.0	1.0	2.0	2.0	2.0	1.0	1.0	1.0
EDM02	2.5	3.0	1.0	1.0	1.5	2.5	2.0	1.5	0.5	2.5
EDM03	1.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
EDM04	1.0	1.0	1.0	1.0	1.0	2.0	3.0	3.5	3.5	1.0
EDM05	1.0	1.0	1.0	1.0	1.5	2.0	1.0	1.0	0.0	1.0
APO01	2.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
APO02	1.5	1.5	1.5	1.5	1.0	1.5	1.0	1.0	0.0	1.0
APO03	1.0	1.5	1.0	2.0	0.5	1.5	2.0	1.5	1.0	3.5
APO04	1.0	1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.0	0.0
APO05	3.0	3.0	1.0	1.5	2.0	2.0	1.5	3.5	0.5	2.0
APO06	3.5	2.0	1.0	1.5	1.5	2.0	4.0	3.0	1.0	2.0
APO07	1.5	1.0	1.0	1.0	1.0	1.5	2.0	2.0	4.0	1.0
APO08	2.5	2.0	1.0	2.5	1.5	1.0	2.5	2.0	1.5	1.0
APO09	2.0	1.5	2.0	4.0	1.0	2.5	1.5	2.0	0.5	1.0
APO10	1.0	1.0	2.0	4.0	1.5	1.5	1.5	0.0	1.5	1.0
APO11	1.0	1.0	3.0	1.5	1.0	3.0	0.0	0.0	0.0	2.0
APO12	1.0	0.5	2.5	1.5	2.0	2.0	1.0	1.0	0.5	1.0
APO13	0.0	0.0	3.5	1.0	2.0	1.0	0.0	1.0	0.0	0.5
APO14	1.0	1.5	3.0	1.0	2.5	1.5	1.0	1.5	0.0	1.5
BAI01	0.0	1.0	1.5	0.0	0.0	0.0	0.0	3.0	1.0	3.5
BAI02	0.0	3.0	0.0	0.0	0.5	2.0	0.0	2.0	0.0	3.5
BAI03	1.0	2.0	2.0	0.0	0.0	2.0	0.0	1.0	0.0	3.0
BAI04	0.5	0.0	2.0	3.0	0.0	2.0	0.0	0.0	0.0	0.0
BAI05	1.0	3.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	3.0
BAI06	0.0	0.0	2.5	3.0	0.5	1.5	0.0	1.0	0.0	1.5
BAI07	0.0	1.0	2.0	2.0	0.5	1.5	0.0	0.5	0.0	2.0
BAI08	0.0	0.0	0.0	1.5	0.5	0.5	0.0	1.0	2.0	0.5
BAI09	0.5	0.5	1.0	0.0	0.0	0.0	2.0	2.0	0.0	0.0
BAI10	0.0	0.0	2.5	2.0	0.5	0.0	0.0	0.5	0.0	0.0
BAI11	1.0	2.0	2.5	0.0	0.0	0.0	2.0	3.0	1.0	4.0
DSS01	0.0	0.0	2.5	2.0	1.0	2.0	0.0	0.5	0.0	0.0
DSS02	1.0	1.0	4.0	3.0	1.0	2.5	0.0	0.0	0.0	0.0
DSS03	0.0	1.0	3.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0
DSS04	0.0	0.0	3.0	1.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS05	0.0	0.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS06	0.0	1.0	0.5	0.0	3.0	0.5	0.0	0.0	0.0	1.0
MEA01	1.0	1.5	2.0	2.0	2.5	3.0	1.0	2.0	1.5	1.0
MEA02	0.0	0.0	2.0	2.0	2.5	2.0	2.0	0.0	0.5	2.0
MEA03	0.0	0.0	2.0	2.0	4.0	0.5	0.0	0.0	0.0	0.0
MEA04	1.0	1.0	3.0	1.5	3.0	4.0	2.0	1.0	1.0	0.5

DF 4 Reference K to T issues; L3 to U42 Matrix (Final B3 to U42 DF4 Map)



DF4	Reference K: Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	Reference L: Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	Reference M: Excessively high cost of IT	Reference N: Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	Reference O: Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	Reference P: Regular issues with data quality and integration of data across various sources	Reference Q: High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	Reference R: Business departments implementing their own information solutions with little or no involvement of the enterprise IT department	Reference S: Ignorance of and/or noncompliance with privacy regulations	Reference T: Inability to exploit new technologies or innovate using I&T
EDM01	3.0	3.5	1.0	1.0	1.0	1.0	2.0	3.0	1.5	1.0
EDM02	1.5	1.0	3.0	2.0	1.0	1.0	2.0	2.0	1.0	2.5
EDM03	1.0	0.0	1.0	1.5	1.0	2.0	1.0	1.0	2.5	1.0
EDM04	1.5	0.0	4.0	2.0	1.0	1.5	2.0	2.5	0.0	1.0
EDM05	3.0	1.5	1.5	0.5	0.0	0.5	1.0	1.0	1.0	0.0
AP001	1.5	4.0	1.0	2.0	1.0	1.0	1.5	2.0	0.5	1.0
AP002	2.5	0.5	0.5	1.5	1.5	0.5	2.0	2.0	0.0	2.5
AP003	0.5	0.5	1.0	4.0	1.0	3.5	2.0	3.0	0.0	2.0
AP004	0.5	1.0	0.5	2.0	1.0	0.0	0.5	0.5	0.0	4.0
AP005	2.0	1.5	2.0	1.0	0.5	0.0	2.5	2.5	0.0	2.0
AP006	1.0	1.5	4.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0
AP007	0.0	0.0	1.0	0.0	3.0	0.0	0.5	0.5	1.5	1.0
AP008	3.0	1.0	0.5	1.0	4.0	1.0	3.0	3.5	0.0	0.5
AP009	0.0	0.0	1.0	0.0	0.0	0.0	1.0	1.5	0.0	0.0
AP010	0.0	0.0	1.0	0.0	0.0	0.0	0.5	2.0	1.0	0.0
AP011	0.0	0.0	0.0	0.5	0.5	3.0	2.0	2.0	0.0	1.0
AP012	1.0	1.0	1.0	1.0	1.0	2.0	1.0	1.5	2.5	1.0
AP013	0.0	0.0	0.0	0.0	0.0	1.5	2.0	1.0	2.0	1.0
AP014	0.0	0.0	0.5	2.5	0.5	4.0	2.5	2.0	3.0	0.5
BAI01	0.0	0.0	1.5	0.5	1.0	0.0	1.5	2.0	0.0	1.0
BAI02	0.0	1.0	1.0	2.0	2.0	1.5	2.5	3.0	0.5	1.0
BAI03	0.0	0.5	1.0	1.0	1.0	0.5	2.0	2.0	1.0	0.5
BAI04	0.0	0.0	0.5	0.0	0.0	1.0	1.0	1.0	0.0	0.5
BAI05	1.0	0.0	0.0	0.5	2.0	0.0	0.5	1.5	0.0	1.0
BAI06	0.0	1.0	0.5	1.0	0.5	2.0	2.0	2.0	1.0	1.0
BAI07	0.0	1.0	0.0	1.0	0.5	2.0	2.0	2.0	0.0	1.0
BAI08	0.0	0.5	0.0	1.0	3.0	2.0	1.0	1.5	0.0	0.5
BAI09	0.0	0.0	2.0	1.0	0.0	0.0	1.0	1.5	0.0	0.0
BAI10	0.0	0.0	1.0	1.5	0.0	1.5	1.0	2.0	0.0	0.0
BAI11	0.0	0.0	1.5	2.0	0.5	0.0	1.0	1.5	0.0	0.5
DSS01	0.0	0.0	1.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS02	0.0	0.0	1.0	0.0	0.0	1.0	1.0	1.0	0.0	0.0
DSS03	0.0	0.0	0.0	1.0	1.5	1.0	1.0	1.0	0.5	0.0
DSS04	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS05	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	2.0	0.0
DSS06	0.0	0.0	0.0	0.0	1.5	2.5	1.5	1.0	2.0	0.0
MEA01	1.0	1.0	2.0	1.0	1.0	1.0	1.5	1.0	2.5	1.0
MEA02	1.0	1.0	1.5	1.0	0.0	2.0	1.0	1.0	2.5	0.0
MEA03	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	4.0	0.0
MEA04	1.0	1.0	1.5	0.0	1.0	1.0	1.0	1.0	2.5	1.0

APPENDIX G

"Threat Landscape to Governance and Management Objectives Mapping Table"
B2 to C41 DF 5 Map Matrix;

	A	B	C
1	DF5	High	Normal
2	EDM01	3.0	1.0
3	EDM02	1.0	1.0
4	EDM03	4.0	1.0
5	EDM04	1.0	1.0
6	EDM05	2.0	1.0
7	APO01	3.0	1.0
8	APO02	1.0	1.0
9	APO03	3.0	1.0
10	APO04	1.0	1.0
11	APO05	1.0	1.0
12	APO06	1.0	1.0
13	APO07	2.0	1.0
14	APO08	1.0	1.0
15	APO09	2.0	1.0
16	APO10	3.0	1.0
17	APO11	2.0	1.0
18	APO12	4.0	1.0
19	APO13	4.0	1.0
20	APO14	3.0	1.0
21	BAI01	1.0	1.0
22	BAI02	1.0	1.0
23	BAI03	1.0	1.0
24	BAI04	2.0	1.0
25	BAI05	1.0	1.0
26	BAI06	3.0	1.0
27	BAI07	1.0	1.0
28	BAI08	1.0	1.0
29	BAI09	1.0	1.0
30	BAI10	3.0	1.0
31	BAI11	1.0	1.0
32	DSS01	1.0	1.0
33	DSS02	3.0	1.0
34	DSS03	2.0	1.0
35	DSS04	4.0	1.0
36	DSS05	3.0	1.0
37	DSS06	3.0	1.0
38	MEA01	3.0	1.0
39	MEA02	2.0	1.0
40	MEA03	3.0	1.0
41	MEA04	3.0	1.0

APPENDIX H

"Mapping Compliance Requirements to Governance and Management Objectives"

B2 to D41 DF 6 Map Matrix;

	A	B	C	D
1	DF6	High	Normal	Low
2	EDM01	3.0	2.0	1.0
3	EDM02	1.0	1.0	1.0
4	EDM03	4.0	2.0	1.0
5	EDM04	1.0	1.0	1.0
6	EDM05	1.5	1.0	1.0
7	APO01	2.0	1.5	1.0
8	APO02	1.0	1.0	1.0
9	APO03	1.0	1.0	1.0
10	APO04	1.0	1.0	1.0
11	APO05	1.0	1.0	1.0
12	APO06	1.0	1.0	1.0
13	APO07	1.0	1.0	1.0
14	APO08	1.0	1.0	1.0
15	APO09	1.0	1.0	1.0
16	APO10	1.5	1.0	1.0
17	APO11	1.0	1.0	1.0
18	APO12	4.0	2.0	1.0
19	APO13	1.5	1.0	1.0
20	APO14	2.0	1.5	1.0
21	BAI01	1.0	1.0	1.0
22	BAI02	1.0	1.0	1.0
23	BAI03	1.0	1.0	1.0
24	BAI04	1.0	1.0	1.0
25	BAI05	1.0	1.0	1.0
26	BAI06	1.0	1.0	1.0
27	BAI07	1.0	1.0	1.0
28	BAI08	1.0	1.0	1.0
29	BAI09	1.0	1.0	1.0
30	BAI10	1.0	1.0	1.0
31	BAI11	1.0	1.0	1.0
32	DSS01	1.0	1.0	1.0
33	DSS02	1.0	1.0	1.0
34	DSS03	1.0	1.0	1.0
35	DSS04	1.5	1.0	1.0
36	DSS05	2.0	1.0	1.0
37	DSS06	1.0	1.0	1.0
38	MEA01	1.0	1.0	1.0
39	MEA02	1.0	1.0	1.0
40	MEA03	4.0	2.0	1.0
41	MEA04	3.5	2.0	1.0

APPENDIX I

"Mapping Role of IT to Governance and Management Objectives"
B2 to E41, DF 7 Matrix;

	A	B	C	D	E
1	DF7	Support	Factory	Turnaround	Strategic
2	EDM01	1.0	2.0	1.5	4.0
3	EDM02	1.0	1.0	2.5	3.0
4	EDM03	1.0	3.0	1.0	3.0
5	EDM04	1.0	1.0	1.0	2.0
6	EDM05	1.0	1.0	1.0	2.0
7	APO01	1.0	1.5	1.5	2.5
8	APO02	1.0	1.0	3.0	3.0
9	APO03	1.0	1.0	2.0	2.0
10	APO04	0.5	1.0	3.5	4.0
11	APO05	1.0	1.0	2.5	3.0
12	APO06	1.0	1.0	1.0	2.0
13	APO07	1.0	1.0	1.0	1.5
14	APO08	1.0	1.0	2.0	2.5
15	APO09	1.0	2.0	1.5	2.0
16	APO10	1.0	2.5	1.5	2.0
17	APO11	1.0	1.5	1.5	2.0
18	APO12	1.0	2.5	1.0	3.0
19	APO13	1.0	2.0	1.5	3.0
20	APO14	1.0	1.5	1.5	2.5
21	BAI01	1.0	1.0	2.0	2.5
22	BAI02	1.0	1.0	3.0	3.0
23	BAI03	1.0	1.0	3.0	3.0
24	BAI04	1.0	2.5	1.5	2.0
25	BAI05	1.0	1.0	1.0	2.0
26	BAI06	1.0	2.5	1.0	2.0
27	BAI07	1.0	1.0	2.0	2.0
28	BAI08	1.0	1.0	1.0	2.0
29	BAI09	1.0	1.0	1.0	2.0
30	BAI10	1.0	1.5	1.0	2.0
31	BAI11	1.0	1.0	2.0	2.0
32	DSS01	1.0	3.5	1.0	3.0
33	DSS02	1.0	3.0	1.5	3.0
34	DSS03	1.0	3.0	1.5	3.5
35	DSS04	1.0	3.0	1.5	3.5
36	DSS05	1.5	2.5	1.5	3.5
37	DSS06	1.0	1.0	1.0	2.5
38	MEA01	1.0	1.0	1.0	2.0
39	MEA02	1.0	1.0	1.0	2.0
40	MEA03	1.0	1.0	1.0	1.5
41	MEA04	1.0	1.0	1.0	2.0

APPENDIX J

"Sourcing Model for IT to Governance and Management Objectives"
B2 to D41, DF8 Matrix;

	A	B	C	D
1	DF8	Outsourcing	Cloud	Insourcing
2	EDM01	1.0	1.0	1.0
3	EDM02	1.0	1.0	1.0
4	EDM03	1.0	2.0	1.0
5	EDM04	1.0	1.0	1.0
6	EDM05	1.0	1.0	1.0
7	APO01	1.0	1.0	1.0
8	APO02	1.0	1.0	1.0
9	APO03	1.0	1.0	1.0
10	APO04	1.0	1.0	1.0
11	APO05	1.0	1.0	1.0
12	APO06	1.0	1.0	1.0
13	APO07	1.0	1.0	1.0
14	APO08	1.0	1.0	1.0
15	APO09	4.0	4.0	1.0
16	APO10	4.0	4.0	1.0
17	APO11	1.0	1.0	1.0
18	APO12	2.0	2.0	1.0
19	APO13	1.0	1.0	1.0
20	APO14	1.0	1.0	1.0
21	BAI01	1.0	1.0	1.0
22	BAI02	1.0	1.0	1.0
23	BAI03	1.0	1.0	1.0
24	BAI04	1.0	1.0	1.0
25	BAI05	1.0	1.0	1.0
26	BAI06	1.0	1.0	1.0
27	BAI07	1.0	1.0	1.0
28	BAI08	1.0	1.0	1.0
29	BAI09	1.0	1.0	1.0
30	BAI10	1.0	1.0	1.0
31	BAI11	1.0	1.0	1.0
32	DSS01	1.0	1.0	1.0
33	DSS02	1.0	1.0	1.0
34	DSS03	1.0	1.0	1.0
35	DSS04	1.0	1.0	1.0
36	DSS05	1.0	1.0	1.0
37	DSS06	1.0	1.0	1.0
38	MEA01	3.0	3.0	1.0
39	MEA02	1.0	1.0	1.0
40	MEA03	1.0	1.0	1.0
41	MEA04	1.0	1.0	1.0

APPENDIX K

"Mapping IT Implementation Methods to Governance and Management Objectives" B2 to D41, DF9 Map Matrix;

	A	B	C	D
1	DF9	Agile	DevOps	Traditional
2	EDM01	1.0	1.0	1.0
3	EDM02	1.0	1.0	1.0
4	EDM03	1.0	1.0	1.0
5	EDM04	1.0	1.0	1.0
6	EDM05	1.0	1.0	1.0
7	APO01	1.0	1.0	1.0
8	APO02	1.0	1.0	1.0
9	APO03	1.0	2.0	1.0
10	APO04	1.0	1.0	1.0
11	APO05	1.0	1.0	1.0
12	APO06	1.0	1.0	1.0
13	APO07	1.0	1.5	1.0
14	APO08	1.0	1.0	1.0
15	APO09	1.0	1.0	1.0
16	APO10	1.0	1.0	1.0
17	APO11	1.0	1.0	1.0
18	APO12	1.0	1.5	1.0
19	APO13	1.0	1.0	1.0
20	APO14	1.0	1.0	1.0
21	BAI01	2.0	1.5	1.0
22	BAI02	3.5	2.0	1.0
23	BAI03	4.0	3.0	1.0
24	BAI04	1.0	1.0	1.0
25	BAI05	2.5	1.5	1.0
26	BAI06	3.5	2.0	1.0
27	BAI07	2.5	2.5	1.0
28	BAI08	1.0	1.0	1.0
29	BAI09	1.0	1.0	1.0
30	BAI10	1.5	2.0	1.0
31	BAI11	2.5	1.0	1.0
32	DSS01	1.0	2.5	1.0
33	DSS02	1.0	1.5	1.0
34	DSS03	1.0	1.5	1.0
35	DSS04	1.0	1.0	1.0
36	DSS05	1.0	1.0	1.0
37	DSS06	1.0	1.0	1.0
38	MEA01	1.5	1.5	1.0
39	MEA02	1.0	1.0	1.0
40	MEA03	1.0	1.0	1.0
41	MEA04	1.0	1.0	1.0

APPENDIX L

"Technology Adoption Strategies to Governance and Management Objectives" B2 to D41, DF 10 Map Matrix;

	A	B	C	D
1	DF10	First Mover	Follower	Slow Adopter
2	EDM01	3.5	2.5	1.5
3	EDM02	4.0	2.5	1.5
4	EDM03	1.5	1.0	1.0
5	EDM04	2.5	2.0	1.5
6	EDM05	1.5	1.0	1.0
7	APO01	2.5	1.5	1.0
8	APO02	4.0	3.0	1.5
9	APO03	2.0	1.0	1.0
10	APO04	4.0	3.0	1.0
11	APO05	4.0	2.5	1.0
12	APO06	1.0	1.5	1.0
13	APO07	2.5	1.0	1.0
14	APO08	3.0	1.5	1.0
15	APO09	1.5	1.5	1.0
16	APO10	2.5	1.5	1.0
17	APO11	1.5	1.5	1.0
18	APO12	2.0	1.5	1.0
19	APO13	1.0	1.0	1.0
20	APO14	2.5	2.0	1.0
21	BAI01	4.0	3.0	1.5
22	BAI02	3.5	2.5	1.0
23	BAI03	4.0	2.5	1.0
24	BAI04	1.5	1.5	1.0
25	BAI05	3.0	2.0	1.0
26	BAI06	2.5	2.0	1.0
27	BAI07	3.5	2.5	1.0
28	BAI08	1.5	1.0	1.0
29	BAI09	1.0	1.0	1.0
30	BAI10	1.5	1.0	1.0
31	BAI11	3.5	2.5	1.0
32	DSS01	1.0	1.0	1.0
33	DSS02	1.0	1.0	1.0
34	DSS03	1.5	1.0	1.0
35	DSS04	1.5	1.0	1.0
36	DSS05	1.5	1.0	1.0
37	DSS06	1.0	1.0	1.0
38	MEA01	3.0	2.0	1.0
39	MEA02	1.0	1.0	1.0
40	MEA03	1.0	1.0	1.0
41	MEA04	1.0	1.0	1.0

APPENDIX M

Area	Domain	Objective ID	Objective	Objective Description
Governance	Evaluate, Direct and Monitor	EDM01	Ensured Governance Framework Setting and Maintenance	"Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives."
Governance	Evaluate, Direct and Monitor	EDM02	Ensured Benefits Delivery	"Optimize the value to the business from investments in business processes, I&T services and I&T assets."
Governance	Evaluate, Direct and Monitor	EDM03	Ensured Risk Optimization	"Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed."
Governance	Evaluate, Direct and Monitor	EDM04	Ensured Resource Optimization	"Ensure that adequate and sufficient business and I&T-related resources (people, process and technology) are available to support enterprise objectives effectively and, at optimal cost."
Governance	Evaluate, Direct and Monitor	EDM05	Ensured Stakeholder Engagement	"Ensure that stakeholders are identified and engaged in the I&T governance system and that enterprise I&T performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and necessary remedial actions."
Management	Align, Plan and Organize	APO01	Managed I&T Management Framework	"Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system."

Area	Domain	Objective ID	Objective	Objective Description
Management	Align, Plan and Organize	APO02	Managed Strategy	“Provide a holistic view of the current business and I&T environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the I&T strategy. Assess the organization’s current digital maturity and develop a road map to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the organization's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives.”
Management	Align, Plan and Organize	APO03	Managed Enterprise Architecture	“Establish a common architecture consisting of business process, information, data, application and technology architecture layers. Create key models and practices that describe the baseline and target architectures, in line with the enterprise and I&T strategy. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.”
Management	Align, Plan and Organize	APO04	Managed Innovation	“Maintain an awareness of I&T and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined I&T strategy. Analyze what opportunities for business innovation or improvement can be created by emerging technologies, services or I&T-enabled business innovation; through existing established technologies; and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.”

Area	Domain	Objective ID	Objective	Objective Description
Management	Align, Plan and Organize	APO05	Managed Portfolio	"Execute the strategic direction set for investments in line with the enterprise architecture vision and I&T road map. Consider the different categories of investments and the resources and funding constraints. Evaluate, prioritize and balance programs and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programs into the active products or services portfolio for execution. Monitor the performance of the overall portfolio of products and services and programs, proposing adjustments as necessary in response to program, product or service performance or changing enterprise priorities."
Management	Align, Plan and Organize	APO06	Managed Budget and Costs	"Manage the I&T-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the I&T strategic and tactical plans. Initiate corrective action where needed."
Management	Align, Plan and Organize	APO07	Managed Human Resources	"Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation and development of human resources (both internal and external)."
Management	Align, Plan and Organize	APO08	Managed Relationships	"Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives."
Management	Align, Plan and Organize	APO09	Managed Service Agreements	"Align I&T-enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of I&T products and services, service levels and performance indicators."

Area	Domain	Objective ID	Objective	Objective Description
Management	Align, Plan and Organize	APO10	Managed Vendors	“Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.”
Management	Align, Plan and Organize	APO11	Managed Quality	“Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.”
Management	Align, Plan and Organize	APO12	Managed Risk	“Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.”
Management	Align, Plan and Organize	APO13	Managed Security	“Define, operate and monitor a system for information security and privacy management.”
Management	Align, Plan and Organize	APO14	Managed Data	“Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.”
Management	Build, Acquire and Implement	BAI01	Managed Programs	“Manage all programs from the investment portfolio in alignment with enterprise strategy and in a coordinated way, based on a standard program management approach. Initiate, plan, control, and execute programs, and monitor expected value from the program.”
Management	Build, Acquire and Implement	BAI02	Managed Requirements Definition	“Identify solutions and analyze requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.”
Management	Build, Acquire and Implement	BAI03	Managed Solutions Identification and Build	“Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.”

Area	Domain	Objective ID	Objective	Objective Description
Management	Build, Acquire and Implement	BAI04	Managed Availability and Capacity	Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.
Management	Build, Acquire and Implement	BAI05	Managed Organizational Change	"Maximize the likelihood of successfully implementing sustainable enterprise wide organizational change quickly and with reduced risk. Cover the complete life cycle of the change and all affected stakeholders in the business and IT."
Management	Build, Acquire and Implement	BAI06	Managed IT Changes	"Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation."
Management	Build, Acquire and Implement	BAI07	Managed IT Change Acceptance and Transitioning	"Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review."
Management	Build, Acquire and Implement	BAI08	Managed Knowledge	"Maintain the availability of relevant, current, validated and reliable knowledge and management information to support all process activities and to facilitate decision making related to the governance and management of enterprise I&T. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge."
Management	Build, Acquire and Implement	BAI09	Managed Assets	"Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements."

Area	Domain	Objective ID	Objective	Objective Description
Management	Build, Acquire and Implement	BAI10	Managed Configuration	"Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository."
Management	Build, Acquire and Implement	BAI11	Managed Projects	"Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review."
Management	Deliver, Service and Support	DSS01	Managed Operations	"Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities."
Management	Deliver, Service and Support	DSS02	Managed Service Requests and Incidents	"Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents."
Management	Deliver, Service and Support	DSS03	Managed Problems	"Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements."
Management	Deliver, Service and Support	DSS04	Managed Continuity	"Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise."
Management	Deliver, Service and Support	DSS05	Managed Security Services	"Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security and privacy policy. Establish and maintain information security and privacy roles and access privileges. Perform security monitoring."

Area	Domain	Objective ID	Objective	Objective Description
Management	Deliver, Service and Support	DSS06	Managed Business Process Controls	"Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements."
Management	Monitor, Evaluate and Assess	MEA01	Managed Performance and Conformance Monitoring	"Collect, validate and evaluate enterprise and alignment goals and metrics. Monitor that processes and practices are performing against agreed performance and conformance goals and metrics. Provide reporting that is systematic and timely."
Management	Monitor, Evaluate and Assess	MEA02	Managed System of Internal Control	"Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness."
Management	Monitor, Evaluate and Assess	MEA03	Managed Compliance with External Requirements	"Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance."
Management	Monitor, Evaluate and Assess	MEA04	Managed Assurance	"Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities."

APPENDIX N

Action No	Action Detail
DSS05.01.1	“Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).”
DSS05.01.2	“Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).”
DSS05.01.3	“Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software.”
DSS05.01.4	“Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management.”
DSS05.01.5	“Regularly review and evaluate information on new potential threats (e.g., reviewing vendors’ products and services security advisories).”
DSS05.02.1	“Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.”
DSS05.02.2	“Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.”
DSS05.02.3	“Apply approved security protocols to network connectivity.”
DSS05.02.4	“Configure network equipment in a secure manner.”
DSS05.02.5	“Encrypt information in transit according to its classification.”
DSS05.02.6	“Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.”
DSS05.02.7	“Establish trusted mechanisms to support the secure transmission and receipt of information.”
DSS05.02.8	“Carry out periodic penetration testing to determine adequacy of network protection.”
DSS05.02.9	“Carry out periodic testing of system security to determine adequacy of system protection.”
DSS05.03.1	“Configure operating systems in a secure manner.”
DSS05.03.2	“Implement device lockdown mechanisms.”
DSS05.03.3	“Manage remote access and control (e.g., mobile devices, teleworking).”
DSS05.03.4	“Manage network configuration in a secure manner.”
DSS05.03.5	“Implement network traffic filtering on endpoint devices.”
DSS05.03.6	“Protect system integrity.”
DSS05.03.7	“Provide physical protection of endpoint devices.”
DSS05.03.8	“Dispose of endpoint devices securely.”
DSS05.03.9	“Manage malicious access through email and web browsers. For example, block certain websites and deactivate click-through on links for smartphones.”

Action No	Action Detail
DSS05.03.1	“Encrypt information in storage according to its classification.”
DSS05.04.1	“Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.”
DSS05.04.2	“Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.”
DSS05.04.3	“Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts.”
DSS05.04.4	“Uniquely identify all information processing activities by functional roles. Coordinate with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.”
DSS05.04.5	“Authenticate all access to information assets based on the individual's role or business rules. Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.”
DSS05.04.6	“Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT infrastructure, system operations, development and maintenance) are uniquely identifiable.”
DSS05.04.7	“Maintain an audit trail of access to information dependent upon its sensitivity and regulatory requirements.”
DSS05.04.8	“Perform regular management review of all accounts and related privileges.”
DSS05.05.1	“Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.”
DSS05.05.2	“Ensure all personnel display properly approved identification at all times.”
DSS05.05.3	“Require visitors to be escorted at all times while on-site.”
DSS05.05.4	“Restrict and monitor access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors.”
DSS05.05.5	“Manage requests to allow appropriately authorized access to the computing facilities.”
DSS05.05.6	“Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.”
DSS05.05.7	“Conduct regular physical information security awareness training.”
DSS05.06.1	“Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise.”
DSS05.06.2	“Ensure cryptographic controls are in place to protect sensitive electronically stored information.”
DSS05.06.3	“Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.”
DSS05.06.4	“Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.”
DSS05.06.5	“Establish appropriate physical safeguards over sensitive documents.”

Action No	Action Detail
DSS05.06.6	“Put cryptographic controls in place to ensure the protection of sensitive information (confidentiality, authenticity, integrity).”
DSS05.07.1	“Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.”
DSS05.07.2	“Define and communicate risk scenarios so they can be easily recognized and the likelihood and impacts understood.”
DSS05.07.3	“Regularly review the event logs for potential incidents.”
DSS05.07.4	“Ensure that security-related incident tickets are created in a timely manner when monitoring identifies potential incidents.”
DSS05.07.5	“Log security-related events and retain records for appropriate period.”