

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
MUHASEBE VE DENETİM YÜKSEK LİSANS PROGRAMI

RİSK ODAKLI İÇ DENETİM VE BİR UYGULAMA

Mevlûde SOYSAL
116758003

Prof. Dr. Burcu ADİLOĞLU

İSTANBUL
2022

İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
MUHASEBE VE DENETİM YÜKSEK LİSANS PROGRAMI

RİSK ODAKLI İÇ DENETİM VE BİR UYGULAMA

Mevlûde SOYSAL
116758003

Prof. Dr. Burcu ADİLOĞLU

İSTANBUL
2022

Risk Odaklı İç Denetim ve Bir Uygulama

Risk-Based Internal Audit and an Application

Mevlûde Soysal

116758003

Tez Danışmanı: Prof. Dr. Burcu ADİLOĞLU
İstanbul Üniversitesi

Jüri Üyesi: Prof. Dr. Cenktan ÖZYILDIRIM
İstanbul Bilgi Üniversitesi

Jüri Üyesi: Dr. Öğr. Üyesi Derya ÜÇOĞLU
İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih:

Toplam Sayfa Sayısı:

Anahtar Kelimeler (Türkçe)

Anahtar Kelimeler (İngilizce)

1) İç Denetim

1) Internal Audit

2) Risk Yönetimi

2) Risk Management

3) Risk Odaklı İç Denetim

3) Risk-Based Internal Audit

ÖNSÖZ

Bu çalışmada işletmelerin risk odaklı iç denetim yaklaşımları denetçiler ile görüşülerek tespit edilmeye çalışılmıştır.

Öncelikle tezimin her aşamasında emeğini, desteğini ve hoşgörüsünü esirgemeyen, gerek iş hayatı ve gerekse akademik hayatı boyunca edinmiş olduğu bilgi ve tecrübeleri aktararak birlikte çalışmaktan zevk aldığım saygıdeğer hocam ve tez danışmanım Prof. Dr. Burcu Adilođlu'na, lisans hayatım boyunca kendisinden aldığım muhasebe dersleri sayesinde yolumu aydınlatarak Muhasebe ve Denetim Yüksek Lisans Programı'na başvurmamda yol gösterici olan Bilgi Üniversitesi Muhasebe ve Denetim Yüksek Lisans Program Direktörü ve aynı zamanda İşletme Fakültesi Dekan Yardımcısı saygıdeğer Dr. Öğretim Üyesi Derya Üçođlu hocama, uygulama bölümünde mülakat yaptığım iç denetçiler başta olmak üzere, sevgi ve desteklerini hiçbir zaman esirgemeyerek beni bu günlere getiren anneme, babama, ablama ve enişteme sonsuz teşekkürlerimi sunarım. Bu çalışmayı sevgili anne ve babama ithaf ediyorum.

Mevlüde SOYSAL

İstanbul, 2022

İÇİNDEKİLER

ÖNSÖZ.....	iii
İÇİNDEKİLER	iv
KISALTMALAR	ix
ŞEKİLLER LİSTESİ.....	xi
TABLolar LİSTESİ.....	xii
ÖZET.....	xiii
ABSTRACT.....	xiv
GİRİŞ.....	1
BİRİNCİ BÖLÜM.....	3
1.İÇ DENETİM	3
1.1. İç Denetimin Tanımı ve Tarihsel Gelişimi.....	3
1.2. İç Denetimin Türleri	5
1.2.1. Mali Denetim.....	6
1.2.2. Uygunluk Denetimi.....	7
1.2.3. Performans Denetimi.....	7
1.2.4. Bilgi Teknolojileri Denetimi.....	8
1.2.5. Sistem Denetimi	8
1.3. İç Denetim ile İlgili Bazı Kuruluşlar	9
1.3.1. Uluslararası İç Denetçiler Enstitüsü (IIA – The Institute on Internal Auditors).....	9
1.3.2. Avrupa İç Denetim Enstitüleri Konfederasyonu (ECIIA – The European Conferadation of Institutes of Internal Auditing).....	10
1.3.3. Türkiye İç Denetim Enstitüsü (TİDE)	10

1.3.4. Kamu İç Denetçileri Derneği (KİDDER)	11
1.4. İç Denetçinin Özellikleri.....	11
1.4.1. Etik İlkeler.....	12
1.4.2. Etik Davranış Kuralları	13
1.5. İç Denetim ve Bağımsız Denetim İlişkisi.....	14
1.6. İç Denetim ve Kurumsal Risk Yönetimi (KRY) İlişkisi	15
1.6.1. COSO Kurumsal Risk Yönetimi Çerçevesi.....	18
1.6.1.1. Yönetişim ve Kültür	19
1.6.1.2. Strateji ve Hedef Belirleme	22
1.6.1.3. Performans.....	23
1.6.1.4. Gözden Geçirme ve Düzeltme	26
1.6.1.5. Bilgi, İletişim ve Raporlama.....	28
1.7. Kurumsal Risk Yönetiminin Faydaları	29
1.8. İç Denetim ve İç Kontrol İlişkisi.....	30
1.8.1. Yönetimsel Kontroller	33
1.8.2. Muhasebesel Kontroller	34
1.8.3. COSO İç Kontrol Çerçevesi.....	34
1.8.3.1. Kontrol Ortamı (Control Environment).....	37
1.8.3.2. Risk Değerlendirmesi (Risk Assessment)	38
1.8.3.3. Kontrol Faaliyetleri (Control Activities).....	39
1.8.3.4. Bilgi ve İletişim (Information and Communication)	40
1.8.3.5. İzleme (Monitoring)	41
1.9. İç Denetimin Sağladığı Faydalar	42
İKİNCİ BÖLÜM	44
2. RİSK ODAKLI İÇ DENETİM SÜRECİ	44
2.1. Risk ve Risk Çeşitleri.....	44
2.1.1. İçsel Riskler	45
2.1.2. Dışsal Riskler.....	47
2.2. Risk Yönetimi ve Risk Yönetim Süreçleri	48

2.2.1. Risk Yönetim Stratejileri.....	51
2.2.1.1. Riskten Kaçınma	51
2.2.1.2. Riski Transfer Etme.....	51
2.2.1.3. Riski Azaltma	52
2.2.1.4. Riski Kabul Etme	52
2.3. Risk Odaklı İç Denetim	53
2.4. Geleneksel İç Denetim ile Risk Odaklı İç Denetimin Karşılaştırılması ..	54
2.5. Risk Odaklı İç Denetim Süreci	56
2.5.1. Riskin Tanımlanması	57
2.5.1.1. Yüksek Risk Düzeyi	58
2.5.1.2. Orta Risk Düzeyi	58
2.5.1.3. Düşük Risk Düzeyi	58
2.5.2. Riskin Değerlendirilmesi	58
2.5.2.1. Risk Matrisinin Oluşturulması	64
2.5.3. Denetim Kaynaklarının Ayrılması	68
2.5.4. Denetim Plan ve Programının Hazırlanması.....	68
2.5.5. Denetimin Yapılması.....	74
2.5.5.1. Uygulama Hazırlığı	74
2.5.5.2. Kontrol Testlerinin Uygulanması	76
2.5.5.3. Test Sonuçlarının Yorumlanması.....	79
2.5.5.4. Bulguların Tespit Edilmesi ve Öneri Sunulması	80
2.5.5.5. Kapanış Toplantısı	81
2.5.6. Raporlama	82
2.5.7. İzleme	87
2.6. Risk Odaklı İç Denetimin Sağladığı Faydalar.....	88
ÜÇÜNCÜ BÖLÜM	90
3.RİSK ODAKLI İÇ DENETİM VE TÜRKİYE’DEKİ İŞLETMELER	
ÜZERİNDE BİR UYGULAMA	90
3.1. Literatür Taraması	90
3.2. Araştırmanın Amacı	95

3.3. Araştırmanın Kapsamı ve Kısıtları	96
3.4. Araştırmanın Yöntemi.....	96
3.5. Elde Edilen Bulgular	97
3.5.1. Demografik Özellikler	97
3.5.2. İç Denetimin Genel Yapısına İlişkin Bulgular	99
3.5.3. İç Denetimin Hazırlık Aşamasına İlişkin Bulgular.....	104
3.5.4. Risklerin Önlenmesi ve Yönetilmesine İlişkin Bulgular.....	110
3.5.5. Denetim Sonunda Elde Edilen Bulgulara Yaklaşım İlişkin Bulgular.....	111
3.5.6. İç Denetimin Performansına İlişkin Bulgular	112
3.5.7. İç Denetimin Faydasına İlişkin Bulgular	113
3.6. Araştırmanın Sonuçları.....	115
SONUÇ VE ÖNERİLER.....	118
KAYNAKÇA	121
EKLER.....	131
Ek 1: A Katılımcısı Mülakatı	131
Ek 2: B Katılımcısı Mülakatı	138
Ek 3: C Katılımcısı Mülakatı	147
Ek 4: D Katılımcısı Mülakatı	156
Ek 5: E Katılımcısı Mülakatı	164
Ek 6: F Katılımcısı Mülakatı.....	172
Ek 7: G Katılımcısı Mülakatı.....	176
Ek 8: H Katılımcısı Mülakatı.....	185
Ek 9: I Katılımcısı Mülakatı	196
Ek 10: J Katılımcısı Mülakatı	211
Ek 11: K Katılımcısı Mülakatı.....	223

Ek 12: L Katılımcısı Mülakatı	231
Ek 13: M Katılımcısı Mülakatı	241
Ek 14. İç Denetim Standartları	248
Nitelik Standartları	248
Performans Standartları	249



KISALTMALAR

AAA	: American Association of Accountants - Amerikan Muhasebeciler Birliđi
ABD	: Amerika Birleşik Devletleri
AICPA	: American Institute of Certified Public Accountants – Amerikan Serbest Muhasebeciler Enstitüsü
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
CCSA	: Certified Control Self Assessment – Kontrol Öz Deđerlendirme
CFE	: Certified Fraud Examiner – Suistimal İnceleme Uzmanı
CFSA	: Certified Financial Services Auditor – Uluslararası Mali Hizmetler Denetçisi
CIA	: Certified Internal Auditor - Sertifikalı İç Denetçi
CICA	: Certified Internal Control Auditor – Sertifikalı İç Kontrol Denetçisi
COSO	: Commission Committee of Sponsoring Organizations of the Treadway
CRMA	: Certification in Risk Management Assurance – Risk Yönetimi Denetçisi
ECIIA	: The European Conferadation of Institutes of Internal Auditing- Avrupa İç Denetim Enstitüleri Konfederasyonu
ESG	: Environment, Social and Governance (Çevre, Sosyal ve Yönetişim)
FEI	: Uluslararası Finans Yöneticileri Güvencesi Sertifikası
IIA	: Uluslararası İç Denetçiler Enstitüsü

İMA	: Yönetim Muhasebecileri Enstitüsü
İSMMM	: İstanbul Serbest Muhasebeci Mali Müşavirler Odası
KİDDER	: Kamu İç Denetçileri Derneği
KPI	: Key Performance Indicator - Temel Performans Göstergesi
KRY	: Kurumsal Risk Yönetimi
KVKK	: Kişisel Verileri Koruma Kanunu
MASAK	: Mali Suçları Araştırma Kurulu
SAP	: Systems Analysis and Program Development
SMMM	: Serbest Muhasebeci Mali Müşavir
SPK	: Sermaye Piyasası Kurulu
TDK	: Türk Dil Kurumu
TİDE	: Türkiye İç Denetim Enstitüsü
TL	: Türk Lirası
QR	: Quality Representative

ŞEKİLLER LİSTESİ

Şekil 1.1. Kurumsal Risk Yönetimi ve İç Denetim İlişkisi.....	18
Şekil 1.2. Risk Profili ve Performans.....	26
Şekil 1.3. COSO İç Kontrol Bütünleşik Çerçevesi.....	36



TABLULAR LİSTESİ

Tablo 1.1 Dışsal Risklerin Dayandığı Sebepler.....	48
Tablo 2.1. Risk Odaklı İç Denetim ile Geleneksel İç Denetimin Karşılaştırılması.....	56
Tablo 2.2. Risk Etki ve Olasılık Derecesi.....	64
Tablo 2.3. Risk Etki ve Sonuçlarının Ölçülmesi.....	65
Tablo 2.4. Örnek Risk Matrisi.....	66
Tablo 2.5. Denetim Çalışma Programı Örneği.....	76
Tablo 2.6. Bulgu Takip Planı.....	88
Tablo 3.1. Katılımcıların ve İşletmelerin Demografik Özellikleri.....	98

ÖZET

Değişen işletme çevresi ve ihtiyaçları doğrultusunda iç denetim geçmişten günümüze gelişmiş ve şekillenmiştir. İşletme koşulları ve ihtiyaçları nedeniyle iç denetim yaklaşımlarının yetersiz gelmesi işletmede iç denetim sürecinin katma değerini artıracak yeni yaklaşımlara yönelmelere yol açmıştır. Böylece klasik iç denetim yaklaşımından ziyade risk odaklı iç denetim anlayışı benimsenmiştir. Risk, işletmenin amaçlarına ulaşmasını engelleyen her türlü unsur olarak tanımlanabilir. İşletmelerin meydana gelebilecek söz konusu riskleri yok etmek, kabul etmemek, riski transfer etmek ve minimize etmek gibi yollarla kontrol mekanizmalarını geliştirmeleri gerekmektedir. Bu nedenle, işletmeler riski tanımalı, değerlendirmeli, nasıl yönetileceğini bilmeli ve alınması gereken önleyici veya düzeltici kontrolleri belirlemelidir. Risk odaklı iç denetim anlayışı geçmişe değil geleceğe odaklanır. Böylece bu anlayış ile işletmenin hedeflerine ulaşabilmesi için maruz kalacağı riskleri önceden tespit ederek riskleri fırsata dönüştürme ve işletme faaliyetlerini geliştirme imkanı sağlamaktadır.

Bu çalışmada iç denetimin gelişimi, denetim türleri, Türkiye'deki iç denetim kuruluşları, iç denetimin kurumsal yönetim ve iç kontrol ilişkisi, risk odaklı iç denetim süreci anlatılarak uygulama bölümünde Türkiye'de faaliyet gösteren işletmelerin risk odaklı iç denetim yaklaşımları tespit edilmeye çalışılmıştır.

Anahtar sözcükler: İç Denetim, Risk Yönetimi, Risk Odaklı İç Denetim

ABSTRACT

Internal audit has developed and shaped from the past to the present in line with the changing business environment and needs. Inadequate internal audit approaches due to business conditions and needs, there has been a tendency towards new approaches that will increase the added value of the internal audit process. Thus, a risk based internal audit approach has been adopted rather than the classical internal audit approach. Risk can be defined as all kinds of factors that prevent the business from achieving its goals. Businesses need to develop control mechanisms in ways such as eliminating, not accepting, transferring and minimizing these risks that may occur. Therefore, businesses must recognize and evaluate risk, know how to manage it, and determine the preventive or corrective controls that should be taken. Risk-based internal audit approach focuses on the future, not the past. Thus, with this understanding, it is possible to identify the risks that the enterprise will be exposed to in order to reach its goals and to transform the risks into opportunities and to improve the business activities.

In this study, the development of internal auditing, types of audits, internal audit organizations in Turkey, the relationship of internal auditing with corporate risk management and internal control, the risk-based internal audit process were explained and the risk-based internal audit approaches of the companies operating in Turkey were tried to be determined in the application chapter.

Keywords: Internal Audit, Risk Management, Risk-Based Internal Audit

GİRİŞ

Küreselleşme ile birlikte gelişen teknolojik değişimler nedeniyle yaşanan finansal krizler ve skandallar denetimin gerekliliğini ve önemini göz önüne sermiştir. İşletmeler varlıklarını sürdürebilmek için faaliyetlerini etkin ve verimli bir biçimde yürütmek ve yönetmekle sorumludur. İstanbul Serbest Muhasebeci Mali Müşavirler Odası (İSMMMO)'nın iç denetim tanımı ise kuruma değer katmak amacıyla objektif bir güvence ve danışmanlık hizmeti sağlayarak kurum faaliyetlerini geliştirmek şeklindedir. Enron skandalı ile başlayan iç denetim sürecinin finansal tabloların hazırlanması, iç kontrollerin güçlendirilmesiyle risk yönetimine duyulan ihtiyaç geleneksel iç denetim yerini risk odaklı iç denetim sürecine bırakmıştır. Risk odaklı iç denetim süreci risklerin tanımlanması ile başlayarak denetim kaynaklarının ve araçlarının risk esaslı olarak kullanılmasıyla risk yönetimine dayanmaktadır. Risk yönetiminin başlangıç noktası işletmelerin içinde bulunduğu belirsizliklerdir. Bu nedenle risk odaklı denetim işletmelerin içinde bulunduğu belirsizliklerin etkili bir biçimde yönetilmesini sağlayarak yönetime değer katmayı hedeflerken makul güvence hizmeti veren ve danışmanlık görevi üstlenen bir yönetim aracıdır.

İşletmeler çeşitli nedenlerden dolayı risklerle karşı karşıya kalabilir. Dolayısıyla risk değerlendirme sürecinde, işletmenin risk haritasının belirlenmesi oldukça önemlidir. Risk haritaları; risklerin kaynağını ve önem derecelerini göstererek, işletmenin karşı karşıya kalabileceği riskleri tanımlayıp, risklerin değerlendirilmesi ve riske karşı önlem alınmasına yardımcı olan özet grafik ve çizelgelerdir. (Usul ve Mizrahi, 2016, s.29) Risk odaklı iç denetimin odak noktası mevzuatlar değil risklerdir. Riskler geçmişe değil geleceğe dönük, işletmenin hedeflerine ulaşmasını engelleyebilecek olayların sonuçlarıdır. Örneğin, işletmede geçmişte yapılmış hata, hile ve suistimaller riskten kaynaklı oluşan sonuçlardır. Risk odaklı iç denetim çalışanların ve yöneticilerin hatalarını ortaya çıkarmak için değil işletmedeki eksikleri kapatmaya yardımcıdır. Bu yönüyle risk odaklı denetim

iřletmenin ynetim aracıdır. Bu nedenle iřletmeler i denetim faaliyetlerine gvenmeli ve i denetimi desteklemelidir.

Literatrde Trkiye’de risk odaklı i denetim ve uygulamalarına ynelik ve birok rnek mevcuttur. Bu alıřmada ise risk odaklı i denetim ile ilgili kavramlar aıklanarak iřletmelerin risk odaklı i denetim yaklařımlarını tespit etmek amalanmıřtır.

alıřmanın birinci blmnde i denetimin tanımı ve tarihsel geliřimi, denetim trleri, Trkiye’deki kuruluřlara deęinilerek i denetinin sahip olması gereken zellikler ve i denetim srecinin iliřkisi bulunan alanlar incelenerek i denetimin saęladığı faydalara yer verilmiřtir.

alıřmanın ikinci blmnde risk odaklı i denetim srecinin ařamalarına detaylı olarak yer verilmiřtir.

alıřmanın nc blmnde ise iřletmelerdeki risk odaklı i denetim yaklařımlarını tespit etmek amacıyla 13 i deneti ile mlakat grřmesi yapılarak elde edilen bulgular deęerlendirilmiřtir.

BİRİNCİ BÖLÜM

1. İÇ DENETİM

1.1. İç Denetimin Tanımı ve Tarihsel Gelişimi

Latince'den dilimize yerleşen denetim kelimesi, Latince “*audits*”, İngilizce “*audit*” ve Fransızca “*audire*” kelimelerinin karşılığı olarak “*duymak, işitmek*” anlamına gelmektedir. Denetim kelimesi Fransızca “*controle*” kelimesinin yerine de kullanılmaktadır fakat amaç ve nitelik olarak birbirinden farklıdır. Günümüzde kontrol, denetim ve teftiş kelimeleri eş anlamlı kelimeler olarak kullanılsalar da birbirinden farklı ancak birbirleriyle iç içe geçmiş bağlantılı kelimelerdir. Denetim, eylem gerçekleştiikten sonra geçmişe yönelik olaylar üzerinde inceleme yapılır. Kontrol ise eylem gerçekleşmeden ya da gerçekleştiğinde eş zamanlı anında müdahale gerektirir. Denetim bağımsız olarak bir defa yapılırken kontrol devamlı olarak yürütülen bir faaliyettir. Denetimde bağımsızlık şartı aranırken, kontrolde bağımsızlık şartı aranmaz. İç denetim kavramı, kurumun mali ve mali nitelikte olmayan iç kontrol sistemlerinin etkili bir şekilde yürütülüp yürütülmediğini inceleyen ve sonuçlarını yönetime raporlayan birimdir. (Adiloğlu, 2011, s.3-5)

Uluslararası İç Denetçiler Enstitüsü (IIA)'nın tanımına göre iç denetim işletmeye değer katmak ve işletme faaliyetlerini geliştirmek amacını benimseyen bağımsız ve objektif bir güvence ve danışmanlık hizmetidir. İç denetim faaliyeti, kontrol, risk yönetimi ve yönetim süreçlerinin etkin olup olmadığını değerlendirerek işletme süreçlerini geliştirmek, işletmenin amaçlarına ulaşması yönünde sistemli ve disiplinli bir yaklaşım getirmektedir. (<https://global.theiia.org/translations/Pages/Turkish-Translations.aspx>, 2019)

Güvence hizmeti, işletmenin yönetim, kontrol ve risk yönetimi süreçlerinde objektif bir inceleme ve değerlendirme sağlamaktır. Finansal yapı, performans, bilgi sistemleri güvenliği, mevzuata uygunluk ile ilgili görevleri kapsar. Karar alıcılar ve yatırımcılar için mali nitelikteki bilgiler ve işletme başarısının ölçülmesine yönelik verilen hizmettir. Danışmanlık hizmeti ise, sorumluluk üstlenmeden işletme faaliyetlerine değer katmak ve geliştirmek amacıyla yol göstermek, eğitim vermek tavsiyelerde bulunmak ile ilgili görevleri kapsar. Amacı sadece hata ve hileleri ortaya çıkartmak değil, işletme ihtiyaçları doğrultusunda danışmanlık hizmeti vermektir. (İSMMM, İç Denetime Genel Bir Bakış, 2015, s.7)

İç denetimin amacı kurumun belirlenmiş politikalar çerçevesinde hedeflere ulaşmasını, işletme faaliyetlerinde geliştirilmesi gereken değişiklikleri önermeyi, kurumun çalışma alanlarını geliştirmeyi, işletme kaynaklarının etkili, verimli ve ekonomik olarak kullanılmasını, hesap verilebilir ve mali konularda şeffaflığı sağlamaktır. Bu amaçlara ulaşabilmek için kurumun iç kontrol sisteminin etkili bir şekilde oluşturulması kaçınılmazdır. Çünkü iç kontrol sistemi işletmenin hedeflerine ulaşmasına yardımcı olmaktadır. (Çevikbaş, 2011, s.51-52)

İç denetimin tarihine bakıldığında ilk olarak 12. yüzyılda Venedik ve Milano gibi büyük ölçekli İtalyan Ticaret Merkezleri'nde muhasebe kayıtlarını kontrol etmek amacıyla ortaya çıktığı görülmektedir. Amerika'da ise ilk olarak iç denetim demir yolu şirketlerinde işletme faaliyetlerinin kontrol edilmesi ihtiyacına yönelik ortaya çıkmıştır. Endüstri Devrimi ile birlikte denetim alanında değişimler yaşanırken, 2. Dünya Savaşı'ndan sonra da Amerika'da iç denetim anlayışında değişiklikler meydana gelmiştir. Zamanla işletme faaliyetlerinin değişmesi ve gelişmesi sonucunda 1941 yılında ABD'de Uluslararası İç Denetim Enstitüsü kurularak, iç denetim mesleğinin etkin uygulanabilmesi için etik kurallar ve standartlar belirlenmiştir. (Adıoğlu, 2011, s.16-18)

İç denetimin uygulanma alanı öncelikle muhasebe ve mali konular ile sınırlıyken risk odaklı iç denetim ile birlikte iç denetimin uygulanma alanı işletme faaliyetlerinin ve iç kontrollerin denetimini kapsayacak şekilde genişletilmiştir. Türedi, risk odaklı iç denetimin gelişim süreci aşağıdaki gibi ifade etmiştir: (Türedi, Zor ve Filiz, 2015, s.4)

- 1960'lı yıllarda iç denetim işletme bilgilerinin güvenilirliğinin sağlanması,
- 1970'li yıllarda uygunluk denetimi,
- 1980'li yıllarda işletme etkinliğinin denetlenmesi,
- 1990'lı yıllarda işletme amaçlarına ulaşılmasının denetlenmesi,
- 2000'li yıllarda ise risk odaklı denetimlerin gerçekleştirilmesi.

İşletme faaliyetlerinin olduğu yerde risk de vardır. İşletmelerin oluşan hataları tespit etmek ve oluşabilecek hataların ortaya çıkmasına sebep olan riskleri göz önünde bulundurarak risk odaklı denetim anlayışına ve uygulamalarına ihtiyaç duyduğu yadsınamaz bir gerçektir. Bu risklerin nasıl yönetildiği geleceğe dönük hedeflere ulaşmada işletmenin ana odak noktasıdır. Dolayısıyla iç denetimin en önemli fonksiyonun risk ve kontroller olduğu görülmektedir. (Çevikbaş, 2011, s.51)

İç denetim proaktif olmalıdır. İşletmenin riske maruz kalacak olayların yaşanmadan önce önlemler olarak yönetim kurulu tarafından belirlenmiş hedeflere ulaşmasına katkı sağlamalıdır. (İSMMMO, İç Denetime Gel Bir Bakış, 2015, s.7)

1.2. İç Denetimin Türleri

İç denetim türleri mali denetim, performans denetimi, uygunluk denetimi, bilgi teknolojileri denetimi ve sistem denetimi olarak beş kategoride incelenebilir.

1.2.1. Mali Denetim

Bir işletmenin finansal tablolarının belirlenmiş ölçütlere göre gerçeğe uygunluğunu ve güvenilirliğinin tespit edilmesini sağlayan denetim türüdür. (Adiloğlu, 2011, s.19) Mali denetimde amaç, işletmenin finansal tablolarındaki yansımaların genel kabul görmüş muhasebe ilkelerine ve yasal mevzuatlara uygun olup olmadığının araştırılmasıdır. (İSMMMO, 2 Denetim Türleri, 2019, s.39)

Mali denetimin odak noktası mali tablolardır. Mizan ile hesaplar arasındaki ilişkinin iyi bir şekilde kavranılarak mali tablolarda yer alan kalemler ile bu kalemlerin zaman içerisinde göstermiş oldukları eğilimler olasılık (senaryo) analizi, oran analizi, regresyon analizi, trend analizi ve çok değişkenli analizler ile incelenebilir. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.23)

Olasılık analizi, tek bir değişkenin değil bütün değişkenlerin değerlerinin iyimser, kötümser ve ikisinin ortalaması olarak tahmin edilmesi tekniğidir.

Oran analizi, mali tablolarda yer alan kalemlerin arasındaki oransal ilişkilerin analiz tekniğidir.

Regresyon analizi, iki ya da daha fazla değişkenin birbirleriyle olan ilişkisini açıklamak ve eğer aralarında güçlü bir bağ var ise sonuçlarını tahmin etmek için kullanılan analiz tekniğidir.

Trend analizi, işletmenin farklı tarihlerdeki iki veya daha fazla mali tablosunun karşılaştırılması, hesaplarda ya da hesap gruplarında meydana gelen değişiklikler ve bu değişikliklerin trendlerinin belirlenmesi ve yorumlanması tekniğidir.

Çok değişkenli analizler, birçok değişken arasındaki ilişkiyi incelemek için kullanılan küme analizi, ana bileşenler analizi, ayırıcı analiz ve faktör analizi olarak bir dizi istatistiksel analizleri içeren model oluşturma tekniğidir.

1.2.2. Uygunluk Denetimi

Bir işletmede mali ve mali olmayan faaliyetlerin belirlenmiş olan kural ve yöntemlere uygun olup olmadığının denetlenmesidir. (Adilođlu, 2011, s.19) Uygunluk denetiminde amaç, işletme faaliyetlerinin işletme içerisindeki ve işletme dışındaki yetkili otoriteler tarafından belirlenen ölçütlere uygunluk derecesinin araştırılmasıdır. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.19)

1.2.3. Performans Denetimi

Bir işletmenin bütün bölümlerinde gerçekleştirilen satın alma, üretim ve pazarlama politikaları vb. gibi faaliyetlerin uygulama alanlarının ve kontrol aşamalarının etkinliğinin ve verimliliğinin denetlenmesidir. (Adilođlu, 2011, s.19)

Performans denetiminde amaç, işletmenin performansını incelemek, belirlenen hedeflerin ne ölçüde gerçekleştiğini tespit etmek ve işletme içerisinde verimli çalışılıp çalışılmadığını incelemektir. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.39)

Performans denetimi işletmedeki yönetim ve organizasyon süreçlerinin geliştirilmesi, kaynakların kullanımında tasarruf sağlanması, işletme amaçlarına etkin yöntemlerle ulaşılması ve işletme faaliyetleri ve hizmetlerinin daha iyi sunulması için ihtiyaç duyulan iyileştirmeler konusunda yol göstericidir. İç denetçi performans denetimi sayesinde işletmede hesap verme sorumluluğunun güçlendirilmesine, planlama ve kontrol faaliyetlerinin geliştirilmesine, işletmenin amaçlarına ulaşmasında ve işletme kaynaklarının kullanılmasında verimlilik, etkinlik ve ekonomikliğin sağlanmasına katkıda bulunur. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.27-28)

Verimlilik, etkinlik ve ekonomiklik performans denetiminin üç ana unsurudur. Performans denetiminin ana unsurlarından biri olan verimlilik, işletme faaliyetlerinde kullanılan girdilerin sabit kalması koşuluyla belirli bir kalitedeki en fazla mal veya hizmetin sunulmasıdır. Performans denetiminin diğer bir unsuru olan etkinlik, işletme amaçları ve çıktıları ile elde edilen sonuçlar arasındaki ilişkiyi göstermektedir. İşletme hedeflerine ulaşıp ulaşılmadığını ve hedeflere ulaşmak için izlenen politikaların başarısını sorgular. Performans denetiminin son unsuru olan ekonomiklik ise, belirli bir kalitedeki işletme kaynaklarının maliyetinin en aza indirilmesidir. Başka bir deyişle en uygun girdinin en iyi fiyata elde edilmesidir. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.27-28)

1.2.4. Bilgi Teknolojileri Denetimi

Bir işletmenin bilgi sistemlerinin sürekliliğini ve güvenilir olup olmadığını denetlenmesidir. (Adiloğlu, 2011, s.21) Elektronik bilgi sistemlerinin güvenliği, veri tabanında depolanmış bilgilerin yanlış kullanılmasına, zarara uğratılmasına ya da yok edilmesine karşı alınan önlem derecesi olarak da tanımlanabilir. (İSMMMO, İç Denetime Genel Bir Bakış, 2015, s.22) Bilgi teknolojileri denetimi, işletmenin amaçlarına ve kontrol hedeflerine ulaşmasını sağlayan bilgi sistemleri ve bu sistemlere ilişkin kontrollerin yeterli olup olmadığı konusunda nesnel bir güvence sağlayarak bilgi teknolojisi sistemlerinin incelenmesi, kanıtların toplanması, değerlendirilmesi ve sonuçların raporlanması sürecidir. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.32)

1.2.5. Sistem Denetimi

Bir işletmenin mali usul ve esaslarındaki eksiklerini tespit etme ve giderme konusunda etkili olup olmadığının denetimidir. (İSMMMO, İç Denetime Genel Bir

Bakış, 2015, s.22) Sistem denetimi, işletmenin denetlenen biriminin hedeflerine ulaşmasında iç kontrol sistemlerinin etkinlik ve verimliliğinin değerlendirilmesidir. Sistem denetiminde birim ya da işletme süreci ile ilgili iç kontrollerin tamamı incelenirken, performans denetiminde işletme faaliyetlerinin etkin, verimli ve ekonomik olup olmadığı, mali denetimde ise işletmenin finansal tablolarının güvenilirliğinin sağlanmasına yönelik kontroller incelenir. (İstanbul Üniversitesi, İç Denetim Rehberi, 2013, s.17)

1.3. İç Denetim ile İlgili Bazı Kuruluşlar

1.3.1. Uluslararası İç Denetçiler Enstitüsü (IIA – The Institute on Internal Auditors)

Uluslararası İç Denetçiler Enstitüsü 1941 yılında ABD'nin Florida eyaletinde kurulmuştur. İç denetim, risk yönetimi, yönetim, iç kontrol, bilgi teknolojileri denetimi, eğitim ve güvenlik alanlarında dünya çapında faaliyet gösteren 185.000'den fazla üyesi bulunan en büyük meslek örgütüdür. Küresel iç denetim mesleği için dinamik liderlik sağlama misyonunu benimsemişlerdir. Bu misyon ile birlikte iç denetimin kuruma kattığı değeri savunmak ve teşvik etmeyi, mesleki eğitim ve gelişim için sertifika programları sağlamayı, iç denetim ve risk yönetimi ile ilgili bilgileri yönetime ileterek teşvik etmeyi, iç denetim uygulama kriterleri konusunda ilgili kişi ve birimleri eğitmeyi, edinilen bilgi ve deneyimleri paylaşmak için tüm ülkelerdeki iç denetçileri bir araya getirmeyi amaçlamışlardır. (<https://global.theiia.org/about/about-the-iiia/pages/about-the-institute-of-internal-auditors.aspx>, 2019, para.1)

1.3.2. Avrupa İç Denetim Enstitüleri Konfederasyonu (ECIIA – The European Conferadation of Institutes of Internal Auditing)

Avrupa İç Denetim Enstitüleri Konfederasyonu 1982 yılında kurulmuştur. Avrupa’da 33 ülkede faaliyet göstermektedir ve merkezi Brüksel’dedir. Amacı üye ülkelerde iç denetim mesleğinin niteliklerini ve standartlarını tanıtarak kamu ve özel kuruluşlarda uygulanmasını sağlamaktır. İç denetim mesleği ile ilgili araştırmalar yapar, raporlar yayımlar, konferanslar verir ve danışmanlık yapar. (<https://icdenetim.ktb.gov.tr/yazdir?B2E057812BFE8E614E7D28626B5DBAE5>, 2019, para.3-5)

1.3.3. Türkiye İç Denetim Enstitüsü (TİDE)

Türkiye İç Denetim Enstitüsü, Türkiye’de 1995 yılında kurulmuştur. Kurumlara iş dünyasında güncel kalabilmek için mesleki gelişim ve yetkinlik eğitimleri ve profesyonel gelişim konusunda fırsatlar sunulmaktadır. Vizyon olarak *‘Meslekte küresel gelişim ve mükemmelliğin paydaşı olmak’* benimsenerek şirketlerin yönetim kurulları, icra kurulu başkanları, denetim komiteleri, iç denetçiler ve düzenleyici kurumlara etkin yönetişim, kontrol ve risk yönetiminin vazgeçilmez bir unsur olduğunu kabul ettirme misyonunu sürdürmektedir. Üyelere uluslararası standartlarda yetkinlik kazandırmak, mesleki gelişim ve tanıtımı sağlamak için hizmet çeşitliliği ve sürekliliğini sağlamak, yakın coğrafi ülkelerde ve Türkiye’de iç denetim mesleğinin etkili bir şekilde uygulanması ve yaygınlaştırılmasında öncülük etmek, kurumsal yönetim, teknolojik ve lojistik altyapı hizmetlerini daha etkin ve verimli hale getirmek TİDE’nin stratejik hedefleri arasındadır. (<https://www.tide.org.tr/page/1/Hakkimizda>, 2019)

1.3.4. Kamu İç Denetçileri Derneği (KİDDER)

Kamu İç Denetçileri Derneği'nin merkezi Ankara'dadır. Kamu kaynaklarının kullanımı ve yönetiminde ekonomiklik, etkinlik ve verimliliğin sağlanmasına katkıda bulunur. KİDDER kamu kurumlarındaki usulsüzlük, yolsuzluk ve suistimallerin önlenmesini, kurum varlıklarının korunmasını, mali tabloların güvenilirliğini, hesap verilebilirlik ve mali saydamlık ilkeleriyle yönetim esasına dayalı mali yönetim ve kontrol sisteminin etkin ve kaliteli bir şekilde geliştirilmesini ve işletilmesini sağlar. Kamu idarelerindeki yöneticilere iç kontrol, risk yönetimi ve yönetim süreçlerinin yeterliliğinin ve etkinliğinin değerlendirilmesi ve geliştirilmesiyle ilgili objektif ve tarafsız bir yaklaşımla güvence sağlama ve danışmanlık hizmeti verilmesi misyonuyla kuruma değer katma geliştirme fonksiyonunu güçlendirmeyi amaçlar. Belirlenen amaçlar doğrultusunda tüm üyelerin hak ve menfaatlerini koruyacak, ülke menfaatleri ve kamu yararı ilkelerini gözeterek şekilde bağımsız ve tarafsız bir yaklaşımla faaliyetlerini gerçekleştirmeyi benimsemişlerdir. (KİDDER, md.2-4)

1.4. İç Denetçinin Özellikleri

İç denetçiler, işletmenin yönetim süreçlerini, faaliyet sürdürdüğü sistemleri ve kurum kültürünü anlayarak çözümlene yaparlar. İşletmede uygulanan yönetim süreçleri ve riskleri azaltmak için sürdürülen iç kontrol uygulamalarının yeterli olduğu konusunda üst düzey yönetim birimine güvence verirler. Bununla birlikte, son teknolojik gelişmeleri yakından takip ederek fırsatları analiz eder ve işletmenin gelişebilmesi için çeşitli tavsiyelerde bulunup danışmanlık hizmeti sunarlar. (TİDE, İç Denetim: Güvence, İç Görü, ve Nesnellik, 2019, s.2) İç denetim faaliyetlerini yürüten kişilerin sahip olması gereken bazı özellikler vardır. Mesleki şüphecilik, iletişim becerileri, bağımsızlık, sürekli gelişim, doğrudan ısrarcı olma, meslek örgütlerine üyelik, mesleki sertifikasyon, standart ve mevzuatlardaki değişiklikleri

ve geliřmeleri takip etmek, takipçi olmak gibi özellikler iç denetçilerde bulunması gereken özellikler arasındadır. (İSMMM, İç Denetime Genel Bir Bakış, 2015, s.25)

İç kontrol sisteminin yetersizliđi ya da iç denetim komitesinin etkin çalışmamasından kaynaklı ortaya çıkarılan yolsuzlukları önleme sorumluluđu öncelikle işletme yönetimi ve iç denetçilerin görevidir. (İSMMM, İç Denetime Genel Bir Bakış, 2015, s.25) İç denetçiler kendilerine yol göstermesi amacıyla Türkiye İç Denetim Enstitüsü tarafından yayınlanan iç denetçiden beklenen davranış tarzı için ‘Etik Davranış Kuralları’ ve iç denetim mesleğinin uygulanmasına yönelik yayınlanan ‘Etik İlkeler’ yönetmeliklerini rehber olarak kullanmalıdır. (TİDE, Etik Kurul Yönetmeliđi, 2019, s.4) İç denetçiler, hızla deđişen dünyada deđişen iş ortamı ve çevresine karşı esnek olmalıdır. Riskleri deđerlendirmek için, yeni geliřen teknolojiler, uluslararası ticaret ve küresel iş yerleri, birleşmeler ve satın almalar gibi konularda geliřmeleri yakından takip etmeli ve bunlara ayak uydurmaları gerekir. İç denetçilerin sahip olduđu yetkinlikler sayesinde maruz kaldığı riskleri dođru tanınmasına yardımcı olur. Etkili ve verimli bir risk yönetimine odaklanarak, sadece güncel sorunlara çözüm üretmekle kalmayıp, gelecekte oluşabilecek problem veya fırsatları önceden tespit ederek işletme yönetimine bildirirler. (TİDE, Etik Kurul Yönetmeliđi, 2019, s.4)

1.4.1. Etik İlkeler

Türkiye İç Denetçiler Enstitüsü tarafından etik ilkeler ařağıdaki gibi açıklanmıştır (TİDE, Etik Kurul Yönetmeliđi, 2019, s.4):

- **Dürüstlük:** İç denetçiler dürüst davranarak güven oluşturur ve söylediklerine itimat edilmesine yönelik zemin oluştururlar.

- **Objektiflik:** İç denetçiler iç denetim faaliyeti ile ilgili bilgi toplama, değerlendirme ve raporlama aşamalarında üst seviyede mesleki objektiflik tutumu sergilerler ve bütün durum değerlendirmelerini dengeli bir şekilde yaparak başkalarının ve kendi menfaatlerinden etkilenmezler.
- **Gizlilik:** İç denetçiler edindikleri bilginin değerlerine ve saygı gösterir ve mesleki ve hukuki zorunluluk olmadığı sürece gerekli yetkilendirme olmadan bilgiyi paylaşmaz.
- **Yetkinlik (Ehil Olma):** İç denetim faaliyetini sürdüren kişiler denetim faaliyetinin yürütülmesinde gerekli olan beceri, bilgi ve tecrübeyi ortaya koyar.

1.4.2. Etik Davranış Kuralları

Türkiye İç Denetçiler Enstitüsü tarafından etik davranış kuralları aşağıdaki gibi açıklanmıştır: (TİDE, Etik Kurul Yönetmeliği, 2019, s.2-3)

- **Dürüstlük:** İç denetçiler sorumluluk, doğruluk ve dikkat duygusuyla hareket ederek çalışmalarında hukuku gözetir ve mesleğin ve hukukun gerektirdiği özel durum açıklamalarını yapar, kanun dışı olaylara isteyerek ve bilerek taraf olmaz, yüz kızartıcı olaylara kalkışmazlar. İşletmenin etik hedeflerine katkıda bulunurlar ve saygı duyarlar.
- **Objektiflik:** İç denetçiler tarafsız değerlendirmede bulunmalarına zarar verebilecek veya verebileceğini düşündükleri ve işletmenin çıkarlarıyla çatışan herhangi bir faaliyete katılmazlar. Denetim faaliyeti boyunca elde ettikleri açıklanmayan raporlarını etkileyen tüm bulguları açıklarlar.
- **Gizlilik:** İç denetçiler denetim faaliyetinde sahip oldukları bilgilerin korunması ve kullanılması konusunda ileriye düşünerek ölçülü davranırlar ve bu bilgileri kendi çıkarları ve hukuka aykırı olacak veya işletmenin etik amaçlarına zarar gelebilecek yönde kullanmazlar.

- **Yetkinlik (Ehil Olma):** İç denetçiler görevlerini uluslararası standartlara uygun olarak gerekli beceri, bilgi ve tecrübeye sahip oldukları görevi üstlenmelidirler. İç denetçiler hem kendi yetkinliklerini hem de denetim faaliyetinin etkinlik ve kalitesini geliştirmelidir.

1.5. İç Denetim ve Bağımsız Denetim İlişkisi

Bağımsız denetçinin amacı işletmenin finansal tablolarının durumunu ve değişimlerini, nakit akışlarını ve faaliyet durumlarını genel kabul görmüş muhasebe standartlarına uygun ve dürüst bir biçimde yansıtıldığına dair bir görüşe ulaşmaktır. Dolayısıyla iç denetçi ile bağımsız denetçi arasındaki ilişki son derece önemlidir. (Adiloğlu, 2011, s.27)

İşletmede bağımsız denetim yapılırken bağımsız denetçi, işletme faaliyetlerini incelerken yapılmış olan iç denetim çalışmalarına ihtiyaç duyulabilir ve iç denetim raporlarını inceleyebilir. Aynı şekilde iç denetçi de daha önceden yapılmış olan bağımsız denetim çalışmalarından etkilenerek denetim plan ve programını oluşturabilir. İç denetim ve bağımsız denetimin ortak amacı işletme varlıklarının kullanımında saydam ve hesap verilebilir olmasını sağlamak, iyi bir yönetime sahip olmak için ekonomik, etkin ve verimli işletme yönetimini teşvik etmektir. Bu nedenle, iç denetçi ile bağımsız denetçi arasındaki ilişki ne kadar iyi olursa bilgi alışverişinin sağlanması da o denli iyi olur. Aralarındaki iş birliği sayesinde denetimin etkinliği artırılabilir. Bağımsız denetçilerin iç denetimin etkinliğini değerlendirme konusunda sorumluluğu vardır. Etkin bir iç denetim sisteminin varlığı bağımsız denetçinin yükünü hafifletebilir. Bağımsız denetçi, ayrıntılı denetim yapmak suretiyle iç denetçi ile uygun bir iş paylaşımı ya da görevlendirme yapılmasına yönelik öneride bulunabilir. İç denetçi ve bağımsız denetçi aralarındaki iş birliğini ve üstlenmiş oldukları denetim sürecini bağımsızlık ve tarafsızlık çerçevesinde yürütürler. Ortak çalışma ile gereksiz tekrar edilebilecek denetim çalışmasının olma olasılığının azaltılmasını, işletmede oluşabilecek

aksaklıkların asgari seviyeye indirilmesini, risk deęerlendiresi ve risklerin tespit edilmesi yöntemiyle denetimin kapsamının geliştirilmesini ve denetimin etkinliğini arttırmak için tavsiyelerde bulunulmasını sağlayarak birlikte çalışmanın vermiş olduęu fayda ile işletmenin katma deęerini azami seviyeye çıkarmasında katkıda bulunurlar. (Akyel, 2010, s.9-10)

Baęımsız denetçi ile iç denetçi ortak bir amaç doğrultusunda hareket etseler dahi görev ve sorumlulukları arasında farklılıklar mevcuttur. Baęımsız denetçi işletmenin çalışanı deęildir ve yapılan sözleşme kapsamında denetim faaliyetlerini yürütür. Baęımsız denetçi finansal tablolar hakkında görüş oluştururken, iç denetçi risk yönetimi ve iç kontrollerin yeterlilięi ve etkinlięi hakkında görüş ve tavsiyelerde bulunur. Baęımsız denetim sadece finansal tablolar ve olayları kapsarken iç denetim işletmenin bütün faaliyet alanını kapsar. İç denetim kontrol sisteminin etkinlięine odaklanır, baęımsız denetim ise iç kontrole ilişkin testlerin azaltılıp azaltılmayacaęı konusuna odaklanır. İç denetim bütün bir yıla yayılabilirken, baęımsız denetim genellikle yıl sonunda gerçekleştirilir. (<https://teolupus.com/teo/ic-denetim-ile-bagimsiz-denetim-arasindaki-farklar-nelerdir/>, 2017)

1.6. İç Denetim ve Kurumsal Risk Yönetimi (KRY) İlişkisi

COSO (Committee of Sponsoring Organizations of the Treadway Commission) 2017 yılında yayınlanan çerçeveye göre kurumsal risk yönetimi; işletmede deęer yaratma ve risklerin yönetilmesi için stratejilerin belirlenmesi ve yürütülmesine ilişkin güvenilir kültür ve imkan uygulamalarıdır. (Çaęlayan, 2018, s.12) Bir işletmedeki kurumsal risk yönetiminin var olma sebeplerinden birincil olanı işletmedeki paydaşlara deęer sağlamaktır. İşletmedeki varlıklar belirsizlikle karşı karşıya kalır ve belirsizlięin kabul edilebilir seviyesinin belirlenmesi gerekir. Belirsizlik işletme için hem risk hem de fırsat sunar. KRY, işletmede belirsizlikten

kaynaklanan sebeplerle meydana gelen ve/ya meydana gelebilecek risk ve fırsatlarla etkin ve verimli bir şekilde başa çıkarak şirkete değer katma potansiyelini arttırır. (COSO, ERM-Executive Summary, 2004, s.1)

Günümüzde maruz kalınan risk ortamında işletmelerin başarı sağlamak ve elde ettikleri başarıyı sürdürebilmek için gelişmiş risk yönetimi süreçlerine duyulan ihtiyaç yadsınamaz hale gelmiştir. Kurumsal Risk Yönetimi'nin amacı işletmenin performansını arttırmaktır. Bu bağlamda, iç denetim süreçleri işletmenin yönetim ve kontrol yapısı ile finansal işlemleri, risk yönetim süreçleri ise yönetim ve kontrol süreçlerinin etkinliğini ve verimliliğini değerlendirmesi ve geliştirmesi açısından sürekli, sistematik ve disiplinli yaklaşımlar benimsenerek genel kabul görmüş standartlara uygun bir şekilde gerçekleştirilmesini sağlar. (Bozkurt, 2010, s.24-25)

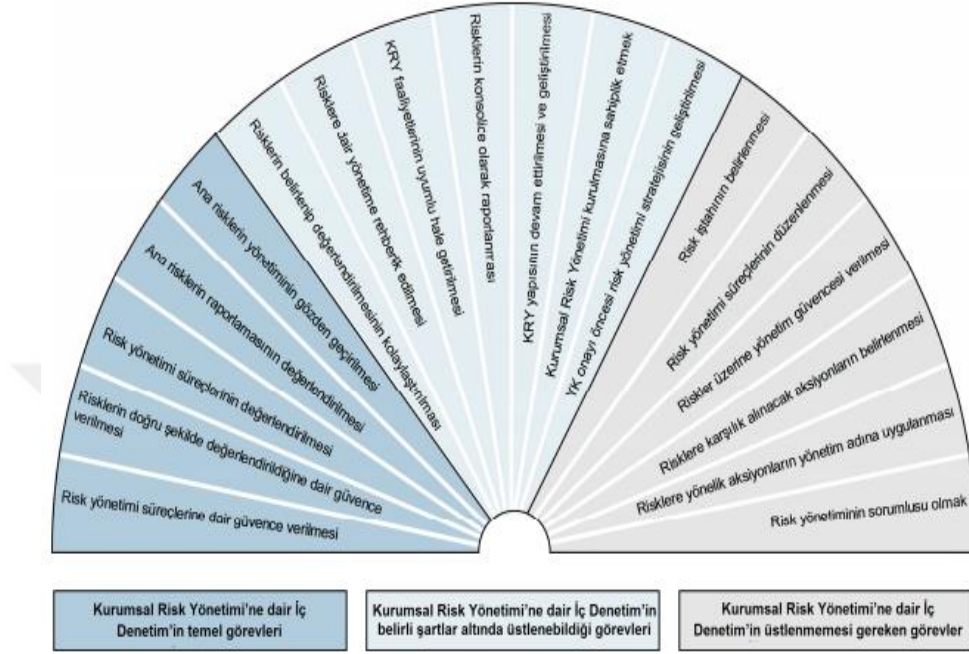
İç denetçiler işletmedeki mevcut risk yönetimi süreçlerinin etkinliğini ve yeterliliğini inceleyerek elde ettiği verileri yönetime iyileştirici önlemler sunarak raporlamalıdır. İşletmenin kurumsal risk yönetimi ve kontrol süreçlerinde üst yönetimin sorumluluğu bulunurken işletme içerisinde güvence ve danışmanlık rolünü üstlenen iç denetçilerin risklerin tanımlanması, değerlendirilmesi, risk yönetimi için belirlenen yöntemlerin uygulanması ve kontrol edilmesi gibi süreçlerde sorumlulukları vardır. Kurumsal risk yönetimi açısından iç denetçilerin işletme yönetiminin asıl sorumluluklarından biri olan 'riskleri fiilen yönetme' konusunda herhangi bir sorumluluğu yoktur. İç denetçiler risk yönetim süreçleri tespit ettikleri bilgiler ve alınması gereken tedbirler ile ilgili yönetime tavsiyelerde bulunabilir, yönetimin kararlarını destekleyebilir ya da sorgulayabilir. (Bozkurt, 2010, s.24-25)

KRY işletmenin faaliyet yapısına uygun olarak belirlenmeli ve uygulanmalıdır. İşletmenin kullandığı risk yönetimi süreci işletme kültürüne, hedeflerine ve yönetim tarzına uygun olmalıdır. İç denetçi, belirlenen yönetimin işletme faaliyet yapısına uygunluğunu ve kapsamını ortaya koyar. İç denetim faaliyeti kurumsal risk yönetimi açısından, işletmedeki varlıkların korunması,

faaliyetlerin etkinlik ve verimliliđi, kanunlara, düzenlemelere ve sözleşmelere uyum konusunda iç kontrol sisteminin verimliliđi ve yeterliliđini deđerlendirme niteliđine sahiptir. Burada unutulmaması gereken husus, iç denetçiler risklerin tespit edilmesi, tanımlanması, minimum seviyeye indirilmesi ve izlenmesi konularında iç denetim süreçlerini oluşturabilecek yetkiye sahiptir fakat belirlenmiş risklerin yönetim sürecinde kesinlikle rol üstlenmemeleri gerektiđi hususudur. (Bozkurt, 2010, s.26)

İç denetimin işletme içerisinde verimliliđi arttırmaya yönelik fonksiyonu da bulunmaktadır. İşletmenin hedeflerine ulaşp ulaşmaması, tespit edilen risklerin ortaya konulması ve kaynakların verimli kullanılıp kullanılmaması gibi süreçlerde iç denetim rehberlik görevi üstelenmiştir. Bu çerçevede, iç denetim ve kurumsal risk yönetiminin aynı amaca ulaşma doğrultusunda benzer görevler üstlenildiđi görölmektedir. Şeffaflık, eşitlik ve hesap verilebilirlik ilkeleri doğrultusunda bu süreçler başarılı bir şekilde hayata geçirilerek işletme başarısının olumlu yönde gelişmesi sağlanmaktadır. (Bozkurt, 2010, s.28)

Şekil 1.1: Kurumsal Risk Yönetimi ve İç Denetim İlişkisi



Kaynak: IIA, İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol, s.4

1.6.1. COSO Kurumsal Risk Yönetimi Çerçevesi

Kurumsal risk yönetimi, işletmenin değer yaratma, koruma ve realize etmede riski yönetmek için güvenilir stratejilerin belirlenmesi ve yürütülmesine entegre edilen imkan, kültür ve uygulamalardır. Bu çerçeve aşağıdaki unsurları içermektedir. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.iii)

- Strateji belirlerken ve yürütülürken kurumsal risk yönetiminin değeri hakkında daha fazla bilgi sağlar.
- Performans hedeflerinin belirlenmesini iyileştirmek ve riskin performans üzerindeki etkisini anlamak için performans ve kurumsal risk yönetimi arasındaki uyumu geliştirir.

- Pazarların ve operasyonların küreselleşmesini ve coğrafyalar arasında özel olarak tasarlanmış olsa da ortak bir yaklaşım uygulama ihtiyacını kabul eder.
- Daha fazla iş karmaşıklığı bağlamında hedefler belirleme ve bunlara ulaşma riskini görmenin yeni yollarını sunar.
- Karar vermeyi desteklemede gelişen teknolojileri ve veri analitiklerinin çoğalmasını barındırır.
- Kurumsal risk yönetimi uygulamalarının tasarlanması, uygulanması ve yürütülmesinde yer alan tüm yönetim seviyeleri için temel tanımları, bileşenleri ve ilkeleri belirler.

Yönetim işletmede genel anlamda riski yönetme sorumluluğuna sahiptir. Bu nedenle üst yönetim riskin açık bir şekilde değerlendirilmesinin strateji seçimini nasıl etkilediğini daha iyi anlayacaktır. Kurumsal risk yönetimi, koşullar değiştikçe stratejinin güçlü ve zayıf yönlerine, misyon ve vizyonuna ne kadar uyduğu bakış açısını ekleyerek yönetim diyalogunu geliştirir. Üst yönetimin alternatif stratejileri değerlendirerek işletmeye en uygun stratejileri uygulamak için gerekli olan girdileri göz önünde bulundurdıklarından emin olmalarını sağlar. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.2)

1.6.1.1. Yönetişim ve Kültür

Yönetişim kurumsal risk yönetimi sürecinin önemini vurgular ve gözetim sorumluluklarını oluşturarak işletmenin tavrını belirler. Kültür ise işletmedeki risk anlayışı, etik değerler ve davranışlar ile ilgilidir. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.6) Yönetişim ve kültür aşağıdaki 5 unsurdan oluşmaktadır.

- **Yönetim kurulu risk gözetimini yerine getirir (exercises board risk oversight);** yönetim kurulu işletme stratejilerinin gözetimini sağlar ve

işletmenin strateji ve iş hedeflerine ulaşmasını desteklemek için yönetim sorumluluklarını yerine getirir.

İşletmede güçlü ve etkin bir iç kontrol sisteminin olup olmadığı değerlendirilerek işletmenin karşı karşıya kalabileceği risklerin doğası ve şiddeti göz önünde bulundurulmalıdır. İşletmenin katlanacağı risklerin doğası ve boyutunu, risklerin oluşma olasılığını ve işletmeye olan etkilerini azaltabilme yeteneği göz önünde bulundurulmalıdır. (Güler ve Arkın, 2018, s.50)

- **Operasyonel yapıyı oluşturur (establishes operating structures);** işletme strateji ve iş hedeflerinin peşinde koşan işletme yapıları kurar.
- **Arzu edilen kültürü tanımlar (defines desired culture);** organizasyon kurumun arzu edilen kültürünü ve davranışlarını tanımlar.
İşletmenin müşterileri gibi kilit noktalara ilişkin güncel değerlerini içermektedir. İşletmenin arzu edilen ya da ideal kültürü formüle edilir. Bu kültür işletmenin stratejik gelişimini desteklemesini hedeflediğinden işletme kültürü olarak benimsenebilir. (Güler ve Arkın, 2018, s.51)
- **Temel değerlere bağlılık gösterir (demonstrates commitment to core values);** organizasyon temel değerlere bağlılık gösterir.
İşletmede güçlü bir kültüre sahip olmak için değerlerin geniş bir biçimde paylaşılması ve güçlü olarak tutulması kritik noktadır. (Güler ve Arkın, 2018, s.51)
- **Yetenekli personeli çeker, geliştirir ve elde tutar (attracts, develops, and retains capable individuals);** strateji ve iş hedeflerine uyumlu insan sermayesi oluşturmaya kararlıdır.
İnsan Kaynakları departmanının en temel stratejik görevlerinden biri, yetenekli çalışanları işletmeye dahil etmek ve elde tutmak için gerekli olan motive edici ve bağdaştırıcı işletme kültürünü geliştirmeye katkı sağlamasıdır. (Güler ve Arkın, 2018, s.51)

2018’de yayınlanan çerçeveye göre yönetim veya iç gözetim, kararların alınma şeklini ve bu kararların nasıl yürütüldüğünü belirler. KRM ile ilgili risklere KRM uygulamak, Yönetim Kurulunun ve üst yönetimin ESG (Governance and Culture for ESG-related risks) ile ilgili riskler konusundaki farkındalığını artırmayı ve ESG konularının risk yönetiminden sorumlu olanlar arasında bir iş birliği kültürünü desteklemeyi içerir. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.8)

Risk kültürü ve risk tutumu yönetim ve kültürün en önemli bileşenidir. İşletme faaliyetlerinde aynı şartlar altında aynı kararların alınması bakımından risk kültürü önemli rol oynar ve işletmede risk kültürü ve risk tutumunun oluşturulması bir yönetim faaliyetidir. Risk stratejileri ve risk politikalarına ilişkin belgeler, finansal tablolar, işletme planları ve stratejileri yönetim ve kültür anlayışının anlaşılmasına katkı sağlayan belgelerdir. Yönetim ve kültür faaliyetleri aşağıdaki gibi sıralanabilir (Pehlivanlı, 2020, s.19):

- Süreçlerin tanımlanması,
- Dış kaynaklardan gelen belgeler ve bilgiler, süreçlerin çıktıları, anahtar girdilerin belirlenmesi, iç sistemlerden veriler ile anahtar girdilerin belirlenmesi,
- İşletme dışına gönderilen belgeler, iç kullanıcılar için raporlar, süreçler için veriler, bilgisayara depolanan veriler, fiziksel olarak depolanan belgeler ile anahtar çıktılarının belirlenmesi,
- Kontrol ve izleme görevleri, tamamlanmış işletme faaliyetlerinin analizi, sistem güncelleştirmeleri, alınan kararlar, görevleri yerine getiren anahtar personel ve görevler için gerekli olan zaman ile anahtar adımların belirlenmesi,
- Anahtar kontroller ve yönetilebilir risklerin belirlenmesi.

1.6.1.2. Strateji ve Hedef Belirleme

Kurumsal risk yönetimi stratejik planlama sürecinde strateji ve hedef belirleme ile birlikte çalışır. Bir risk iştahı oluşturularak strateji ile uyumlu hale getirilir; iş hedefleri stratejiyi uygulamaya koyarken riski belirleme, değerlendirme ve riske yanıt verme için bir temel oluşturur. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.6) Strateji ve hedef belirleme aşağıdaki 5 unsuru içermektedir.

- **İş ortamını analiz eder (analyzes business context);** iş bağlamının potansiyel etkilerini dikkate alır.
İşletme iş ortamının risk profili üzerindeki potansiyel etkileri analiz etmelidir. Risk profili, belirlenen strateji veya hedefler ile ilgili risk çeşitleri, şiddeti ve bağımlı olduğu alanların performans üzerindeki etkileri hakkında bütünlük bir bakış açısıdır. (Güler ve Arkin, 2018, s.50)
- **Risk iştahını tanımlar (defines risk appetite);** işletme risk iştahını değer yaratma, koruma ve gerçekleştirme bağlamında tanımlar.
İşletmeler, önceden hedeflenen risk iştahı ile tutarlı bir artık risk oluşturan kontrolleri ve azaltıcı uygulamaları tasarlayarak gerekli olduğunda geri bildirim ve süreci izleyerek tüm riskleri hedeflerine göre tanımlamalıdır. Risk iştahı, işletmenin hedef ve amaçları doğrultusunda maruz kalmayı kabul ettiği en yüksek risk seviyesidir. İşletmelerin bu risk iştahı seviyesindeki riskler için önlem alınması gerekmektedir. (Güler ve Arkin, 2018, s.52)
- **Alternatif stratejileri belirler (evaluates alternative strategies);** işletme alternatif stratejileri ve risk profili üzerindeki potansiyel etkiyi değerlendirir.
Çevresel tehditler veya fırsatlar alternatif stratejiler ile çoğaltılmalı ve değerlendirilerek işletme için seçilen strateji en iyi alternatif olmalıdır ve

risk profili üzerinde etkileri değerlendirilmelidir. (Güler ve Arkın, 2018, s.52-53)

- **İş hedeflerini oluşturur (formulates business objectives);** organizasyon stratejisi uyumlu hale getiren ve destekleyen çeşitli seviyelerde iş hedeflerini oluştururken riski göz önünde bulundurur.

İşletme stratejisi, işletme hedeflerinin tanıtılmasında destekleyici bir rol oynamalıdır. İşletme hedefleri oluştururken hem yatay hem de dikey seviyedeki riskleri göz önünde bulundurur. (Güler ve Arkın, 2018, s.53)

Tüm kuruluşların doğa ve toplum üzerinde etkileri ve bağımlılıkları vardır. Bu nedenle, iş bağlamı, stratejisi ve tüm KRM faaliyetleri ve risklerin etkin yönetimi için bir çapa görevi gören güçlü bir anlayıştır. KRM ile ilgili risklere KRM uygulamak, kısa, orta ve uzun vadede bu etkileri ve bağımlılıkları anlamak için değer yaratma sürecini incelemeyi içerir. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.8)

Stratejik açıdan işletme hedefleri faaliyet ve raporlamaya ilişkin uyum veya uygunluk temellerine dayanarak oluşturulabilir. İşletme hedeflerinin belirlenme sürecinde, işletme stratejileri, risk alma istekliliği ve sınırları, risk toleransı ve işletmenin misyon ve vizyonu göz önünde bulundurulmalıdır. Strateji ve hedeflerin belirlenmesi kurumsal risk yönetimi uygulamaları için işletmede sağlam bir alt yapı oluşturmaktadır. (Pehlivanlı, 2020, s.20)

1.6.1.3. Performans

İşletmede strateji ve iş hedeflerine ulaşılmasını etkileyebilecek risklerin belirlenmesi ve değerlendirilmesi gerekir. Risk iştahına bağlı riskler önem derecesine göre önceliklendirilir ve işletmeler risk yanıtını seçer ve üstlendiği risk miktarının portföyünü belirler. Bu sonuçlar kilit risk paydaşlarına rapor edilir.

(COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.6)

- **Riskleri belirler (identifies risk);** organizasyon strateji ve iş hedeflerinin performansını etkileyen riskleri tanımlar.

Risklerin tanımlanması kurumsal risk yönetiminin uygulanmasında temel bir süreçtir. Risk tanımlaması karar vericiler için belirsizlik yaratan olaylar hakkında bilinçlenme sağlar. Risk tanımlama sürecinin odak noktası belirsizlik yaratan olayların proaktif olarak yönetilmesi için belirsizliklerin tanımlanmasıdır. (Güler ve Arkın, 2018, s.53)

2018’de yayınlanan çerçevede risk belirleme, kuruluşlar, ESG ile ilgili riskleri belirlemek için mega trend analizi, SWOT analizi, etkiler ve bağımlılık haritalaması, paydaş katılımı ve ESG önemlilik değerlendirmeleri gibi birden fazla yaklaşım kullanır. Bu araçlar, bir riskin bir kurumun stratejisine ve iş hedeflerine ulaşmasını nasıl tehdit ettiği açısından ESG konularının belirlenmesine ve ifade edilmesine yardımcı olabilir. Risk yönetimi ve sürdürülebilirlik uygulayıcıları arasındaki iş birliği yoluyla bu yaklaşımların uygulanması, ESG ile ilgili riskleri risk envanterine yükseltir ve bunları uygun değerlendirme ve yanıt için konumlandırır. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.9)

- **Risklerin şiddetini değerlendirir (assesses severity of risk);** organizasyon riskin ciddiyetini değerlendirir.

Kurumsal risk yönetimi, riskleri tanımlamak, şiddetini değerlendirmek, ölçmek ve azaltmak için üst seviyedeki fırsatlardan yararlanmaktır. İşletme olması muhtemel risklerin şiddetini değerlendirir. (Güler ve Arkın, 2018, s.53-54)

- **Riskleri önceliklendirir (prioritizes risks);** organizasyon risklere verilecek yanıtları seçerken bir temel olarak risklere öncelik verir.

Risk tanımlamasından sonra riskleri değerlendirmek ve önceliklendirmek uygun yönetim uygulamasının seçilebilmesi için önemlidir. Sonuçları ve olasılıkları değerlendirerek ve karşılaştırarak risk matrisi oluşturulmaktadır. (Güler ve Arkın, 2018, s.54)

2018'de yayınlanan kurumsal risk yönetimi çerçevesinde riskleri değerlendirme ve öncelik sırasına koyma aşamaları birleştirilerek açıklanmıştır. Şirketler sınırlı kaynaklara sahiptir, bu nedenle kurum genelinde tanımlanan tüm risklere eşit şekilde yanıt veremezler. Bu nedenle önceliklendirme için risklerin değerlendirilmesi gerekmektedir. KRM ile ilgili risklere KRM uygulamak, risklerin önceliklerini belirlemek için yönetimin kullanabileceği bir dilde risk ciddiyetinin değerlendirilmesini içerir. Ortaya çıkan veya daha uzun vadeli ESG ile ilgili risklerin göz ardı edilmemesini veya iskonto edilmemesini, bunun yerine uygun şekilde değerlendirilmesini ve önceliklendirilmesini sağlamak için ESG konusundaki uzmanlıktan yararlanmak kritik öneme sahiptir. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.9)

- **Risk cevaplarını uygular (implements risk responses);** organizasyon risk yanıtlarını tanımlar ve seçer.

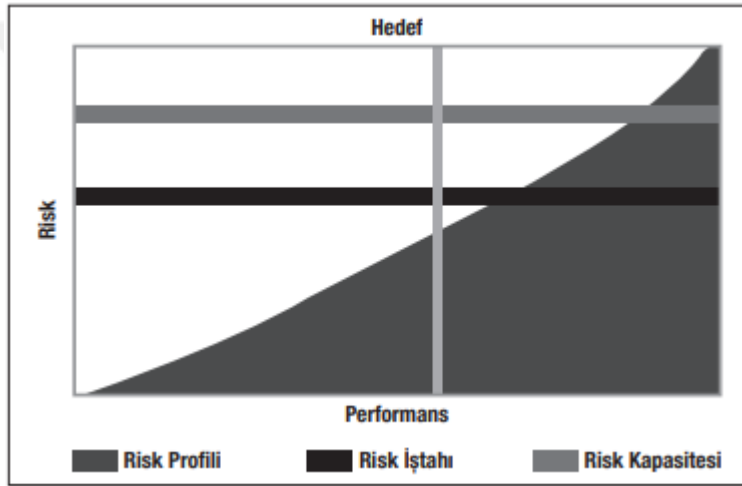
Bir kurumun tanımlanmış risklere nasıl yanıt vereceği, nihayetinde kurumun uzun vadede ne kadar etkili bir şekilde değer koruduğunu veya yarattığını belirleyecektir. Her bir yaklaşımın maliyet ve faydalarının yanı sıra riskin kaynağını da dikkate alan bir dizi yenilikçi ve iş birlikçi yaklaşımları benimsemek, bu yanıtların başarısını destekler. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.9)

Riske cevap olarak risk yönetimi kontrolünü arttırmanın bir yolu da entegre ve yapısal risk yönetimini sağlamaktır. İşletme riske vereceği uygun cevabı seçer ve belirler. Bu cevaplar bir dizi kontrol faaliyeti ya da stratejisi şeklindedir. (Güler ve Arkın, 2018, s.54)

- **Portföy bakış açısı geliştirir (develops portfolio view);** organizasyon bir risk portföyü görünümünü geliştirir ve değerlendirir.

Portföy bakışı, risk profiline benzer ve aşağıdaki Şekil 1.2’de gösterilmiştir. Aradaki fark, işletme stratejisi ve hedefleri ile ilgili risklerin ve performans üzerindeki etkisinin bütünlük bakış açısıdır. (Güler ve Arkın, 2018, s.54)

Şekil 1.2: Risk Profili ve Performans



Kaynak: (Phinicharomna, 2018, i çalışması (Güler ve Arkın, 2018, s.54 den alıntı))

1.6.1.4. Gözden Geçirme ve Düzeltme

Bir işletme performansını gözden geçirerek kurumsal risk yönetimi bileşenlerinin zaman içerisinde ve önemli değişiklikler sonucunda ne kadar iyi çalıştığını ve hangi revizyonların gerekli olduğunu değerlendirir. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.6)

- **Önemli değişimleri değerlendirir (assesses substantial change);** organizasyon strateji ve iş hedeflerini önemli ölçüde etkileyebilecek değişiklikleri tanımlar ve değerlendirir.

Yöneticiler işletme strateji ve hedefleri doğrultusunda önemli bir değişiklik olduğunu düşündüklerinde yönetim modellerinde değişiklik yapmazlarsa gerileme ortaya çıkabilir. Uygun olmayan işletme modelleri ortaya çıkabilecek sorunların algılanmasını engelleyebilir ve etkisi olmayan eylemlere neden olabilir. (Güler ve Arkın, 2018, s.55)

- **Riskleri ve performansı gözden geçirir (reviews risk and performance);**

organizasyon kurum performansını gözden geçirir ve riski dikkate alır.

İşletme risklerini ve risk cevaplarını incelemek için genellikle ölçüm kartı kullanılmaktadır. Yönetime Kurumsal Risk Yönetimi'nin etkin olup olmadığı ve risk profilinin düzeltme ve değerlendirmesinin gerekli olup olmadığını tespit etmek için oluşturulmuştur. Çevresel, sosyal ve yönetim ile ilgili risklerin gözden geçirilerek revize edilmesi sürdürülebilirlik yöneticileri ve risk sahipleri ile gerçekleştirilir. Risklerin performansının gözden geçirilmesi, izlenmesi ve göstergeler oluşturulmasından risk sahipleri sorumludur. (Güler ve Arkın, 2018, s.55)

- **Kurumsal risk yönetiminde iyileştirmeleri takip eder (pursues improvement in enterprise risk management);** organizasyon kurumsal risk yönetiminin iyileştirilmesini takip eder.

İşletmeler Kurumsal Risk Yönetimi olgunluk seviyesini izlemeli ve risk ve uyum tepkilerini geliştirmelidir. (Güler ve Arkın, 2018, s.55)

KRM faaliyetlerinin gözden geçirilmesi ve revize edilmesi, etkinliğin değerlendirmesi ve gerektiğinde yaklaşımların değiştirilmesi için kritik öneme sahiptir. Kuruluşlar, risk tanımlama, değerlendirme ve müdahaleye yansıtılması gereken değişikliklerin yönetimini uyarmak için özel göstergeler geliştirebilir. Bu bilgiler bir dizi iç ve dış paydaşa rapor edilir. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.9)

1.6.1.5. Bilgi, İletişim ve Raporlama

Kurumsal risk yönetimi, aşağı yukarı işletme genelinde akan iç ve dış kaynaklardan gerekli bilgilerin elde edilmesi ve paylaşılması için sürekli bir süreç gerektirir. (COSO, Enterprise Risk Management Integrating with Strategy and Performance, Executive Summary, s.6)

- **Bilgi ve teknoloji avantajlarından yararlanır (leverages information systems);** organizasyon kurumsal risk yönetimini desteklemek için kuruluşun bilgi ve teknoloji sistemlerinden yararlanır.

Bilgi teknolojileri işletmede değer yaratma konusunda verimlilik kavramıyla ilişkilendirilmektedir. İşletmelerde bilgi teknolojilerinden yararlanılarak süreçlere, kurumsal uygulamalara ve işletmedeki gelişmelere yön verilerek bilgi teknolojilerinin işletme için faydası ön plana çıkmaktadır. Bilgi teknolojileri yönetimi işletmeye benzersizlik ve rekabet avantajı sağlayabilecek görüşü ağırlık kazanmıştır. (Güler ve Arkın, 2018, s.56)

- **Risk bilgisinin iletişimini yapar (communicates risk information);** Kurumsal risk yönetimini desteklemek için iletişim kanallarını kullanır.

Büyüme yolundaki işletmeler çok fazla belirsizlikle karşı karşıya kalabilir ve sadece meydana gelen riskler değil fırsatların riskler üzerindeki etkisine bağlı olarak büyümeyi doğru bir şekilde yönlendirmek için iyi bir kurumsal risk yönetimi sağlanmalıdır. İşletmeler kurumsal risk yönetimi için risk yöneticisi atarlar ve işletmeyi tehdit eden durumların tanımlaması ve hafifletmesi beklenir. Bu risk yöneticisinin temel görevlerinden biri Kurumsal Risk Yönetimi strateji ve hedefleri ile ilgili dış paydaşlar ile iletişim kurmasıdır. (Güler ve Arkın, 2018, s.56)

- **Risk, kültür ve performans hakkında raporlama yapar (reports on risk, culture, and performance);** birden çok düzeyde ve kurum genelinde risk, kültür ve performans hakkında raporlama yapar.

Etkin yönetim için Yönetim Kurulunun etkili raporlama hatları oluşturması gerekmektedir. (Güler ve Arkın, 2018, s.56)

KRM ile ilgili risklere KRM uygulanması, risk bilgili karar vermeyi desteklemek için dahili ve harici olarak iletilecek ve raporlanacak en uygun bilgileri belirlemek için risk sahipleriyle istişareyi içerir. (COSO, Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks, s.9)

İşletme hedeflerine ulaşmada yardımcı olacak çalışanların ve yöneticilerin sorumluluklarını yerine getirmelerine yardımcı olacak bilgiler tanımlanmalı ve istenilen zamanda iletişime hazır formatta olmalıdır. İletişim ise bilginin işletme içerisinde yönetim planlarından çalışanların haberdar olması, departmanlar arasında personel iletişimi ve çalışanların yönetimi bilgilendirmesi şeklindedir. Yapılan raporlamaların doğruluğu önemli bir konudur. Dolayısıyla iç denetçi anahtar risk değerlendirmelerini yaparak raporlamalı ve iletişimin ve bilgilerin tam, doğru ve ilgili olup olmadığını belirlemelidir. Kurumsal risk yönetiminin gelişimi için risklerin raporlama zamanı, riskleri oluşturan olaylar ve kontrol hatalarına ilişkin öneriler bir gereklilik oluşturmaktadır. (Pehlivanlı, 2020, s.20-21)

1.7. Kurumsal Risk Yönetiminin Faydaları

KRM işletmelerde stratejik yönetimin merkezini oluşturmaktadır. Kurumsal risk yönetimi yapısına sahip işletmelerde başarı olasılığı artarken hedeflerin gerçekleşmesindeki belirsizlik seviyesi ve başarısızlık olasılığı azalmaktadır. Kurumsal risk yönetiminin faydaları aşağıdaki gibi sıralanabilir. (Baykal, Tunç ve Kasımoğlu, 2016, s.55-56)

- Riske karşı bütünleşik tavır alınmasını sağlar,

- Risklerin belirlenmesi ve alınacak önlemlerin geliştirilmesi için şeffaflığın artırılmasını sağlar,
- İç kontrolü kapsayıcı olması nedeniyle etkinliği artırarak yöneticilerin daha etkili denetim ve kontrol yapmasına imkan sağlar,
- İşletmede sürekli olarak işleyen dinamik ve sistematik bir süreçtir.
- İşletme stratejilerinin oluşturulması ve uygulanması aşamalarında yol göstericidir.
- Kurumsal risk yönetiminin hedeflerinden biri operasyonel risklerin en aza indirilmesidir.
- Belirsizlik ve tehditlere karşı geliştirilmiş ve daha açık kararların verilmesini sağlar.
- İşletme itibarının korunmasını sağlar.
- İşletme hedeflerine ulaşmada makul güvence verir.
- İşletme risklerinin optimum seviyede yönetilmesini sağlar.
- İşletme verimliliğinin ve etkinliğinin artırılmasını ve korunmasını sağlar.
- Yöneticilerin doğru kararlar almasına yardımcı olur.
- Risk etkilerinin proaktif olarak yönetilmesine katkı sağlar.
- Paydaşların memnuniyetlerinin artırılmasını sağlar.
- Risklerin izlenmesi ve etkisinin ölçülmesini sağlar.

1.8. İç Denetim ve İç Kontrol İlişkisi

İç denetim işletmeye hizmet etmek, işletme faaliyetlerini incelemek ve değerlendirmek amacıyla işletme içerisinde kurulmuş bağımsız bir değerlendirme fonksiyonu ve bir kontrol faaliyetidir. Bu yönüyle iç denetim, işletme içerisindeki kontrollerin yeterliliğini ve etkinliğini araştırmaktadır. İç denetimin işletmedeki

amaçlarından bir tanesi üst yöneticilerin ve yönetim kurulunun görev ve sorumluluklarını etkin bir şekilde yerine getirmelerine yardımcı olmaktır. (Sevim ve Eliuz, 2007, s.62)

1978 yılında İç Denetçiler Enstitüsü tarafından yayınlanan “İç Denetim Mesleki Uygulama Standartları” raporunda denetimin faaliyet alanının işletmedeki iç kontrol sisteminin etkinliğinin ve yeterliliğinin değerlendirilmesi ve denetlenmesinden oluştuğu vurgulanmıştır. İç denetim iç kontrolün farklı ancak önemli bir boyutunu oluşturmaktadır. İç kontroller işletmenin belirlemiş olduğu amaç ve hedeflere etkin bir şekilde ulaşacağına dair yeterli güvence verilmesini sağlayan usul ve yöntemler bütünüdür. (Kızılboğa ve Özşahin, 2013, s.226) İç kontrol işletmedeki finansal raporların güvenilirliği, işletme faaliyetlerinin etkinliği ve verimliliği, işletme prosedürlerinin yasa ve diğer düzenlemelere uygunluğunun işletme amaçlarına ulaşılmasını dikkate alarak yeterli ölçüde güvence sağlamak için işletmenin yönetim kurulu, yöneticileri ve diğer personelleri tarafından etkilenen bir süreçtir. (Demirbaş, 2005, s.168)

İç kontroller, işletmede faaliyetleri içerisinde yer alan makul güvence sağlamak için belirlenmiş unsurlardır. İç kontrol süreçleri, işletme yönetim kurulu, yöneticileri ve çalışan personelleri tarafından tasarlanır, yönlendirilir ve yürütülür. İç kontroller, finansal raporların güvenilir olması, işletme faaliyetlerinin etkin ve verimli olması, yasal mevzuatlara yürütülmesi açısından işletme içerisinde önemli bir yere sahiptir. Kontrol faaliyetleri işletmedeki mevcut olan varlıkların korunmasını sağlar. Çünkü işletmeler büyüdükçe varlıkların korunması karmaşık bir hal alır. Bu yüzden işletmeler iç kontrol prosedürlerine ihtiyaç duyar. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.3)

İşletmede organizasyon yapısı, politika ve prosedürler, muhasebe sistemi ve finansal kontrol, bütçe ve raporlama, insan kaynakları yönetimi ve yetkilendirme sisteminin iç kontrol ilkeleri ile uyumlu olması iç kontrollerin yeterliliğini belirleyen temel unsurlardır. İşletmelerde iç kontrollerin yeterliliğinin

değerlendirilmesi iç denetim faaliyetine olan ihtiyacı arttırmıştır. Bu yönüyle iç denetim ve iç kontrol birbirinden farklı aynı zamanda birbirini tamamlayan iki kavram olarak değerlendirilmelidir. (Uzun, 2022, s.303)

Committee of Sponsoring Organizations of the Treadway Commission (COSO)'nun tanımına göre; iç kontrol işletmenin yönetimi, yönetim kurulu ve diğer çalışanları tarafından gerçekleştirilen operasyonlar, raporlama ve uyum konusunda belirlenen hedeflere ulaşılması konusunda makul güvence sağlamak için oluşturulmuş bir süreçtir. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.3) İç kontrol, işletme faaliyetlerinde ve devamlılık temelinde oluşan tekil bir eylem değil bir dizi olay ve aktivitelerdir. İç kontrol işletmede ayrı bir sistem olmaktan ziyade faaliyetlerin düzenlenmesi ve yönlendirilmesinde yararlanılan sistemin ayrılmaz bir parçası olarak kabul edilir. İç denetim iç kontrolden farklı olarak, işletmenin etkinliğini denetlemek, iyileştirmek, geliştirmek ve işletmeye değer katmak amacıyla tarafsız ve bağımsız olarak güvence ve danışmanlık hizmeti veren bir faaliyettir. Hata odaklı yaklaşımdan ziyade süreç odaklı yaklaşımla işletmede işin doğru yapılmasıyla birlikte doğru işin yapılmasını öneren bir yaklaşımla geliştirici ve önceden önlem alınmasını sağlayan stratejik bir rol üstlenmektedir. (Kızılboga, ve Özşahin, 2013, s.226-227)

IIA 2130 Kontrol başlıklı standardına göre, iç denetim faaliyeti, işletmede uygulanan kontrollerin etkinlik ve verimliliğini değerlendirmek ve sürekli gelişimi teşvik etmek amacıyla işletmenin etkin kontrol sürecine sahip olmasına yardımcı olmak zorundadır. Aşağıdaki unsurları dikkate alarak işletmenin faaliyetlerinin, yönetim süreçlerinin ve bilgi sistemlerinin karşı karşıya kaldığı risklere karşı cevap olarak uygulanan kontrollerin etkinliğini ve verimliliğini stratejik hedeflere ulaşma, finansal operasyonel bilgilerin doğru ve güvenilir olması, işletme faaliyetlerinin ve programların etkin ve verimliliği, işletme varlıklarının korunması, politika, prosedür, düzenleme, sözleşme ve kanunlara uyum konularına göre

değerlendirmek zorundadır. (TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.16-17)

İç kontrol sistemi geniş anlamda iç denetimi kapsamakla birlikte sadece finansal kontrol değil denetim faaliyetlerinin dışında kalan bütün kontrol unsurlarını içerir. İç denetim sistemi iç kontrol sistemini etkinlik ve yeterlilik açısından değerlendirerek geliştirmeyi amaçlamaktadır. İç kontrol sisteminin etkinliğinin ölçülmesi ve değerlendirilmesi süreci iç denetçilerin işletmede uygunluk denetimi yapmasını gerektirir. Böylece iç kontrol bilginin doğru ve güvenilir olduğunu sağlarken iç denetim ise bilginin doğru ve güvenilir olduğunu test edip yönetime bilgi verir. İşletmede iç kontrol sistemi ile mevzuata, plan ve programlara uygunluk sağlanırken iç denetçiler tarafından uygunluğun kontrolü yapılmaktadır. İşletmede etkinlik ve verimlilik iç kontrol sistemi ile sağlanırken etkinlik ve verimliliği teşvik ederek işletmeye değer kazandırmak iç denetimin sorumluluğundadır. (Kızılboga ve Özşahin, 2013, s.226-227)

İç kontrol sistemi yönetsel ve muhasebe kontrolleri olmak üzere iki kontrol sürecinden oluşmaktadır.

1.8.1. Yönetsel Kontroller

İşletme planı, yönetim onayı ve yetki aktarımı gerektiren karar işlemleri ile ilgili bütün işlem ve kayıtları içermektedir. Dolaylı olarak mali kayıtlar ile ilgilidir. İşletmenin bütün yönetsel kapsayacak şekilde çalışanların performanslarının belirlenmesi ve değerlendirilmesi ile ilgili bir süreç olarak tanımlanabilir. Yönetsel kontrolün amacı işletme hedeflerinin gerçekleştirilmesi yönünde çalışanları yönlendirmek, teşvik etmek ve performansını değerlendirmek olarak tanımlanabilir. (Celayir, 2021, s.21)

1.8.2. Muhasebesel Kontroller

Finansal kayıtların ve tabloların ve işletme varlıklarının korunması ile ilgili kontrollerdir. Muhasebe kayıtları raporların hazırlanmasını sağlayacak ve hesap verme yükümlülüğünü kuracak şekilde tutulmalıdır. Muhasebe kontrolleri, işlemlerin yönetim yetkilerine uygun olarak yürütülmesi, finansal tabloların genel kabul görmüş muhasebe ilkelerine ve raporlara uygun olarak hazırlanması, belirli aralıklarla varlıklar ile defter kayıtları arasında karşılaştırmalar yapılarak fark varsa soruşturma yapılması ve hata ve hile varsa kimin yaptığıının belirlenmesi hususlarını sağlayacak şekilde tasarlanmalıdır. (Celayir, 2021, s.21)

İç kontrolün amacı işletme varlıklarını korumak, muhasebe bilgilerinin doğru ve güvenilirliğini sağlamak, işletme faaliyetlerinin verimliliği ve politikalara uygunluğunu sağlamak, kaynakların verimli ve ekonomik kullanılmasını sağlamaktır. (Celayir, 2021, s.22-23)

1.8.3. COSO İç Kontrol Çerçevesi

COSO Amerika'da beş bağımsız meslek örgütü; Amerikan Muhasebeciler Birliği (AAA), Amerika Sertifikalı Kamu Muhasebecileri (AICPA), İç Denetçiler Enstitüsü (IIA) ve Yönetim Muhasebecileri Enstitüsü (IMA) tarafından 1985 yılında hileli mali raporlamayı önlemek amacıyla kurulmuştur. COSO işletmeye finansal raporların güvenilirliğini, faaliyetlerin etkinlik ve verimliliğini, yürürlükte olan kanun ve mevzuata uygunluğunu sağlama açısından katkıda bulunur. (Aktaş, 2015, s.31-32)

İlk olarak 1992 yılında yayınlanan COSO Bütünleşik Çerçevesi dünyada yaygın olarak kullanılmaktadır. Küreselleşme ile birlikte gelişen teknolojik olaylar işletmeleri giderek karmaşıklaşan bir yapıya sürüklemiştir. Finansal tablolarda meydana gelmiş olan hata ve hileleri azaltmak için tasarlanmış olan iç kontrol

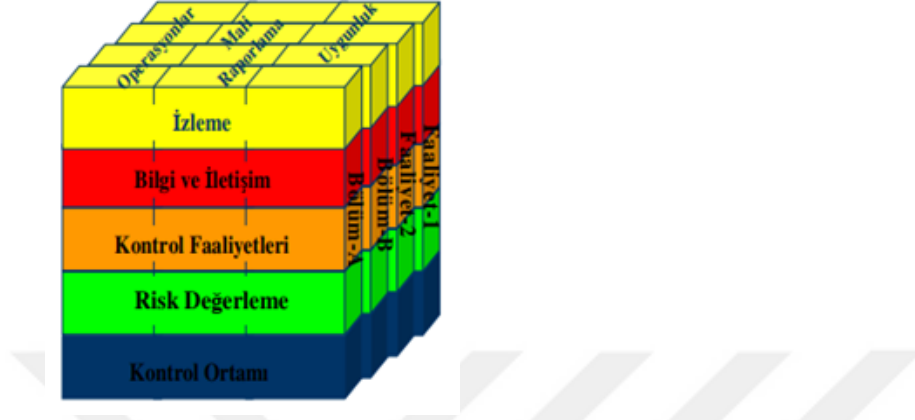
sistemi ve kurumsal risk yönetimi süreçlerine rehberlik etmek için COSO Bütünleşik Çerçevesi oluşturulmuştur. Bu nedenle işletme yönetimi tarafından iç kontrol sisteminin şeffaflık ve hesap verilebilirlik seviyelerini maksimum seviyede tutarak iç kontrol sisteminin tasarlanması, uygulanması ve yürütülmesi aşamalarında etkinlik ve verimliliğin ölçülmesi için önde gelen yardımcı bir çerçeve olarak kabul edilir. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.6)

COSO Bütünleşik Çevresine göre, işletme faaliyetlerinin güvenilir finansal tablolarının mevzuata uygunluğunu, etkinliği ve verimliliğini sağlamak için iç kontrollerin beş temel bileşene göre yapılması öngörülmüştür. Yayınlanan çerçeveye göre iç kontrolün temel tanımı ve kontrol ortamı, risk değerlemesi, bilgi ve iletişim, izleme olarak birbirleriyle ilişkili beş bileşenden oluşmaktadır. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.6)

İşletme ortamı ve yönetim felsefesi kontrol ortamının oluşmasında etkin bir rol oynar. İşletmenin stratejik, finansal ve operasyonel amaçlarına göre tanımlanan riskler kontrol faaliyetlerinin tasarlanmasında belirleyici rol oynar. İzleme, bilgi ve iletişim kontrol faaliyetlerinin etkinliğinin değerlendirilmesi ve gözden geçirilmesine yardımcı olur. İç kontrol ilkeleri ile COSO bileşenleri çerçevesinde yapılan değerlendirmeler işletmenin yeterli kontrol süreçlerinin olup olmadığı hakkında bilgi verir. (Uzun, 202, s.303,)

COSO'ya göre işletmelerin organizasyonel yapısı üç boyutla temsil edilir. İşletmenin hedefleri operations (faaliyetler), reporting (raporlama) ve compliance (uygunluk) sütunlarla temsil edilir. Beş bileşen control environment (kontrol ortamı), risk assessment (risk değerlendirmesi), control activities (kontrol faaliyetleri), information & communication (bilgi ve iletişim) ve monitoring activities (izleme) ise satırlarla temsil edilir. COSO Bütünleşik Çerçevesi Şekil 1.2.'de gösterilmiştir. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.6)

Şekil 1.3: COSO İç Kontrol Bütünleşik Çerçevesi



Kaynak: COSO, COSO Internal Control – Integrated Framework Executive Summary, 2013, www.coso.org

Sütunların temsil ettiği üç aşama aşağıda açıklanmıştır:

Faaliyetler (operasyonlar), işletmenin finansal ve operasyonel hedefleri dahil olmak üzere işletmenin faaliyetlerinin etkinliği ve verimliliği ile varlıkların korunması aşamasıdır.

Raporlama (mali raporlama), iç ve dış finansal ve finansal olmayan verilerin güvenilirlik, zamanındalık, şeffaflık, standartlar ve işletme politikalarına uygun raporlama aşamasıdır.

Uygunluk, işletmenin uymak zorunda olduğu yasa ve düzenlemelerle ilgili olan aşamadır.

Satırların temsil etmiş olduğu beş bileşen aşağıda ana başlıklar altında detaylı bir şekilde açıklanmıştır.

1.8.3.1. Kontrol Ortamı (Control Environment)

Kontrol ortamı diğer dört iç kontrol unsurlarının temelidir. Kontrol ortamı işletmedeki iç kontrol sisteminin önemi ile ilgili üst yönetimin, yöneticilerin ve diğer ilgililerin farkındalıklarını, davranışlarını ve faaliyetlerini içerir. İşletmede iç kontrol sisteminin oluşmasında üst yönetimin tutum ve davranışları ile işletme kültürü çok önemlidir. Eğer üst yönetim iç kontrol sürecinin gerekliliğine inanırsa işletmedeki kişilerin bu karara uymalarını ve oluşturulan kontrol sistemlerinin bilinçli bir şekilde gözlemlenip karar verilmesini sağlar. (Kızılboga ve Özşahin, s.223)

Kontrol ortamı, işletmenin bütünlüğünü ve etik ilkelerini içerir. İşletme içerisindeki iç kontrol sisteminin uygulanmasını sağlayan temel yapılar, süreçler ve standartlardan oluşur. Kontrol ortamı işletme yönetiminin yetki ve sorumluluklarının yerine getirilip getirilmediği ile ilgili performansların hesap verilebilirliğinin ölçülmesi konusunda işletmeye katkı sağlar. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.4)

COSO kontrol ortamını faaliyetler, raporlama ve uygunluk açısından destekleyen ilkeler aşağıdaki gibi açıklanmıştır (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.6)

- İşletme dürüstlük ve etik değerler ilkelerine bağlılık gösterir.
- İşletmenin yönetim kurulu bağımsızlık olarak iç kontrolün performansını ve gelişimini gözetir.
- İşletme yönetimi raporlama hedeflerinin yerine getirilmesinde gerekli yetki ve sorumlulukları inşa eder.
- İşletme yekın olan kişileri seçer, geliştirir ve elinde tutar.
- İşletme çalışanlarını hedeflerin gerçekleştirilmesi için iç kontrol sorumluluklarından sorumlu tutar.

İşletmede güvenilir ve etkin bir iç kontrol sisteminin oluşturulması ve uygulanması için uygun bir kontrol ortamına ihtiyaç vardır. Kontrol ortamı işletme disiplini ve işletme yapısını oluşturur. Bu bağlamda kontrol ortamı; işletme yapısı, yönetim kurulu veya denetim komitesi, yönetim felsefesi ve çalışma tarzı, uzmanlığın değerlendirilmesi, yetki ve sorumluluk verme yöntemleri, insan kaynakları politikaları ve uygulamaları ve dış etkenler gibi faktörleri kapsar. (Kızılboga, ve Özşahin, 2013, s.224)

1.8.3.2. Risk Değerlendirmesi (Risk Assessment)

İşletmeler iş ve dış kaynaklar sebebiyle çeşitli risklere maruz kalırlar. COSO'ya göre risk; hedeflerin gerçekleşmesini olumsuz yönde etkileyen bir olayın meydana gelme olasılığı olarak tanımlanmıştır. Risk değerlendirme, işletmelerin hedeflerine ulaşabilmesi için meydana gelebilecek risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi için temel süreçtir. COSO risk değerlendirmesini, faaliyetler, raporlama ve uygunluk açısından destekleyen ilkeler aşağıdaki gibi açıklanmıştır (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.4):

- İşletme hedeflerine ulaşma konusunda risklerin tanımlanması ve değerlendirilmesi ile ilgili net hedefler belirler.
- İşletme belirlenen hedeflere ulaşmak için riskleri tanımlar ve yönetilmesi için analiz eder.
- İşletme risk değerlendirmesi yaparken hile potansiyelini de dikkate alır.
- İşletme iç kontrol sistemini büyük ölçüde etkileyebilecek değişiklikleri belirler ve değerlendirir.

Bütün işletmeler müşteri ihtiyaçlarındaki değişimler, rekabet tehditleri, faiz oranları ve ekonomik faktörlerdeki ve hukuki düzenlemelerdeki değişimler gibi çeşitli riskle karşı karşıyadır. Üst yönetim bu riskleri değerlendirmeli ve kontrol etmek için gerekli önlemleri almalıdır. (Kızılboğa, Özşahin, 2013, s.224) Risk değerlemesinin ön koşulu işletmenin kuruluş amaçlarının net, açık ve tutarlı biçimde belirlenmesidir. Amaçların gerçekleşmesi ile ilişkili olarak risklerin tanımlanması, analiz edilmesi ve nasıl yönetileceği konusunda ölçütler oluşturulması gereken bir süreçtir. (Demirbaş, 2005, s.169-170)

1.8.3.3. Kontrol Faaliyetleri (Control Activities)

Kontrol faaliyetleri, işletme hedeflerinin gerçekleştirilmesine yönelik riskleri azaltmak için uygulanan politika ve prosedürlerdir. İşletmede önleyici veya dedektif nitelikteki yetkilendirmeler, mutabakatlar, görevlerin ayrılığı, onaylar, mutabakatlar ve işletme performansı gibi otomatik veya manuel işlemleri kapsar. (COSO, Internal Control-Integrated Framework Executive Summary, s.4)

COSO kontrol faaliyetlerini, faaliyetler, raporlama ve uygunluk açısından destekleyen ilkeler aşağıdaki gibi açıklanmıştır (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.7):

- İşletme hedeflerinin gerçekleşmesinde kabul edilebilir seviyedeki riskleri azaltmaya yardımcı olacak kontrol faaliyetlerini belirler ve geliştirir.
- İşletme hedeflerine ulaşabilmesi için teknolojik alt yapıyı kullanarak kontrol faaliyetlerini belirler ve geliştirir.
- İşletme belirlemiş olduğu kontrol faaliyetlerini beklentilerini karşılayan prosedür ve politikalar ile uygular.

İç kontrol faaliyetleri işletmenin amaçlarına ulaşmasını engelleyen risklere karşı oluşturulan politika ve prosedürlerin uygulanmasıdır. Bu politika ve prosedürler hilenin önlenmesini de kapsayacak şekilde işletmenin hedeflerini başarıya götürmesi için makul bir güvence sağlamak için oluşturulur. İşletmedeki etkin iç kontrol faaliyetleri risk değerlendirme süreci ile tanımlanan riskleri azaltmaya yardımcı olur. Kontrol faaliyetleri görevlerin ayrımı, fiziksel ve performans kontrolleri ve bilgi işlem süreci olarak dört aşamadan oluşturulabilir. (Kızılboga, ve Özşahin, s.224-225)

1.8.3.4. Bilgi ve İletişim (Information and Communication)

İşletmelerin iç kontrol faaliyetlerini sürdürürken üstlendikleri rol ve sorumlulukları yerine getirmek için bilgiye ihtiyaç vardır. İşletme yönetimi iç ve dış kaynaklardan elde ettiği bu bilgileri iç kontrol sistemini geliştirmek için üretir ve kullanır. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.5) Örneğin, finansal raporlama açısından bir bilgi sistemi olan muhasebe birimi işletme varlıklarının ve yükümlülüklerinin muhasebeleştirilmesi için verilerin toplanması, kayıt altına alınması, özetlenmesi ve bu özetlerin analiz ve raporlanmasında kullanılan teknik ve yöntemleri kapsar. Muhasebe sistemi en doğru ve yararlanılabilir bilgiyi sunmak için tasarlanır. Doğru bilgiyi üretmek için sistemde bir dizi kontrollerin öngörülmesi gerekir. Bu kontrollerin ayrıntılı bir biçimde oluşturulması etkili bir iç kontrol sisteminin oluşmasına bağlıdır. Muhasebe fişleri ve kayıtları, mizanlar, defterler ve raporlar birbirleriyle bağlantılı ve birbirlerini doğrulayan kontrol noktalarıdır. Bu nedenle muhasebe sistemi kontrol noktaları ile çevrilidir. Üst yönetim, raporlamayı ve karar almayı etkilen durumları değerlendirmek için bu bilgileri veya harici bilgileri kullanabilir. (Kızılboga ve Özşahin, 2013, s.225)

İletişim ise bilgiyi elde etmek ve paylaşmak için bir süreçtir. İletişim üst yönetim ile personel arasında iç kontrolü sağlamak için bir araçtır. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.5) Yani iç kontrol politika ve prosedürlerle ilgili kişilerin sorumluluklarını içerir. İletişim işletmenin büyüklüğüne bağlı olarak sözlü veya yazılı olabilir. (Kızılböğü ve Özşahin, 2013, s.225) COSO bilgi ve iletişimi, raporlama ve uygunluk açısından destekleyen ilkeler aşağıdaki gibi açıklanmıştır (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.7):

- İşletme iç kontrol sisteminin işlemlerini desteklemek için gereken kaliteli bilgileri elde eder ve üretir.
- İşletme iç kontrol süreci sürecini desteklemek amacıyla amaç ve sorumluluklarla ilgili bütün bilgileri iletir.
- İşletme iç kontrol sistemini etkileyen konular hakkında dış kaynaklarla iletişim kurar.

1.8.3.5. İzleme (Monitoring)

İşletmedeki iç kontrol faaliyetlerinin etkin olup olmadığını belirlemek ve değerlendirmek için bir kontrol sürecidir. Risk değerlendirmesine ilişkin süreçler belirli aralıklarla izlenir ve değerlendirilir. Böylece işletme içerisindeki eksikliklerin ve aksaklıkların belirlenerek üst yönetime bildirilmesine yardımcı olur. (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.5) Zamanla işletmedeki iç kontrol sistemi değişir ve uygulanan kontrol prosedürleri geliştirilir. İzleme bu süreçte şartlar değişirken yönetim tarafından sistemde hangi değişikliklerin nasıl yapılacağına belirlenmesine yardımcı olur. Bu bağlamda işletmedeki iç kontrol kalitesinin belirlenmesi için izleme unsuru önemlidir. İç kontrol faaliyetlerinin uygun personel tarafından zamanında yapılıp yapılmadığı, iyileştirme ve düzeltme faaliyetlerinin uygulanıp uygulanmadığı,

gerekli olan faaliyetlerin tamamlanmış olduğunu belirlemek için ihtiyaç duyulan süreçlerin sonuna kadar yürütülüp yürütülmediği gözden geçirilmelidir. İzleme sürecinde çalışanların geri bildirim ve iç denetçilerin hazırladığı raporlar üst yönetime yardımcı olur. Gelişen teknolojiden yararlanarak işletmedeki iç kontrol sisteminin aksayan yönleri belirlenmeli ve işlerliği değerlendirilmelidir. (Kızılböğü ve Özşahin, 2013, s.225-226) COSO izleme sürecini, faaliyetler, raporlama ve uygunluk açısından destekleyen ilkeler aşağıdaki gibi açıklanmıştır (COSO, Internal Control-Integrated Framework Executive Summary, 2013, s.7):

- İşletme iç kontrolün etkinliğini belirlemek amacıyla sürekli değerlendirmeler geliştirir ve uygular.
- İşletme iç kontrol ile ilgili eksiklikleri iyileştirici ve düzeltici önlemler olarak üst yönetime zamanında uygun yolla iletir.

1.9. İç Denetimin Sağladığı Faydalar

İç denetim işletmedeki bütün çıkar gruplarını ilgilendiren ve menfaatlerini koruyan en önemli araçlardan biridir. İşletmedeki olası hile ve usulsüzlüklerin belirlenmesi ve ortaya çıkmasını önleyen önerilerin geliştirilmesi nedeniyle iç denetim faaliyetine ihtiyaç duyulmaktadır. İşletme süreçlerinin doğru ve eksiksiz işleyip işlemediği, etkinlik ve verimliliğe odaklanılarak risklerin ne kadar etkin yönetildiği ve maddi kayıpların meydana gelip gelmediğinin tespit edilmesi ve gerekli iyileştirme önerileri sunulmasında iç denetim birimine sahip olunması işletmeler açısından büyük önem taşımaktadır. (Aktaş, 2015, s.44-45)

Etkili bir iç denetim sisteminin işletmelere değer katmak amacıyla sağladığı faydaları aşağıdaki maddeler halinde saymak mümkündür. (Türedi, Zor ve Gürbüz, 2015, s.5)

- İşletmenin stratejik hedeflerine ulaşmasında karşılaşılabileceği risklerin belirlenmesi ve değerlendirilmesi,
- İşletmenin karar alırken ve karar verirken bilgi ve süreçlerinin eksiksiz ve doğru olduğunun değerlendirilmesi,
- İşletmede kullanılan uygulamaların işletme politikaları ile kanun ve yönetmeliklere uygunluğunun değerlendirilmesi,
- İşletme varlıklarını korumak amacıyla yürütülen iç kontrollerin değerlendirilmesi,
- İşletme içinde kullanılan kaynakların etkin ve verimli kullanılıp kullanılmadığının değerlendirilmesi,
- İşletmede uygulanan faaliyetlerin ve programların işletme amaçlarına uygun olarak yürütülüp yürütülmediğinin değerlendirilmesi,
- Bağımsız denetçilerin iç denetim prosedürleriyle uyumunun etkinliğini değerlendirerek daha kesin ve net güvence sağlamak,
- İşletme idari birim süreçlerinin izlenmesi ve değerlendirilmesi,
- İşletme yönetimine iç kontroller ve risk yönetim süreçleri ile ilgili danışmanlık sağlamak,
- İşletme herhangi bir risk ile karşı karşıya kaldığında ilgili birimlere rapor verilmesini sağlar.

İKİNCİ BÖLÜM

2. RİSK ODAKLI İÇ DENETİM SÜRECİ

2.1. Risk ve Risk Çeşitleri

Risk kelimesi Fransızca ‘riziko’ kelimesinden gelmektedir. Kelimenin sözlük anlamı ise zarara uğrama tehlikesi olarak tanımlanmıştır. Buna göre risk “*istenmeyen sonuçlarla karşılaşma olasılığı*” olarak tanımlanabilir. (Özbilgin, 2012, s.2)

Risk kavramı değişik bilim dallarında farklı şekillerde tanımlanmıştır. Sigortacılık sektöründe risk; yitirme tehlikesinin varlığı, yitirme ihtimali, belirsizlik, gerçekleşen sonucun beklenen sonuçtan farklı olduğu ihtimali, beklenen herhangi bir durumdan başka bir durumun ortaya çıkması ihtimali olarak tanımlanır. Bankacılık sektöründe ise risk; verilen bir kredinin veya bir taahhüdün tahsil edilmesinde ya da yerine getirilmesinde başarısızlık ihtimali olarak tanımlanırken finans sektöründe ise risk; işletmedeki finansal planların veya beklenen herhangi bir durumun meydana gelmesinde ortaya çıkan sapma ihtimali olarak tanımlanır. (Emhan, 2009, s.2)

Risk ile ilgili birçok tanıma ulaşmak mümkündür. Risk, gelecekte meydana gelebilecek ve işletme hedeflerinin gerçekleşmesini engelleyecek olan olaylar, tehditler ve olumsuzluklar veya hedeflere ulaşmayı kolaylaştıracak fırsatlar şeklinde tanımlanabilir. Risk kavramı genellikle tehdit olarak algılanmaktadır ancak risk fırsatları da kapsar. Bunun nedeni risk kelimesinin Çince’de (ideogram) hem tehdit hem de fırsat anlamında kullanılmasıdır. (Derici, Tüysüz ve Sarı, 2007, s.152)

Uluslararası İç Denetçiler Enstitüsü’nün tanımına göre risk; hedeflere ulaşılması konusunda etkisi olacak bir olayın olma ihtimali olarak tanımlanmıştır.

(TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.28) Bu tanıma göre riskler yönetim, strateji ve planlama, operasyonlar ve alt yapı, mevzuata uyum ve raporlama olarak sınıflandırılabilir. İşletmeler çeşitli şekillerde riske maruz kalabilir. Karşılaşılan riskler işletmenin kültürü, faaliyet yapısı, büyüklüğü, iç kontrol sisteminin etkinliğine bağlı olarak değişiklik gösterebilir. (Usul ve Mizrahi, s.10-11)

İşletmelerin karşılaşacağı risklerin çeşitli sebepleri vardır. Bunlar; plansızlık ve methodsuzluk, zaman ve yönetici baskısı, ihmal ve gerekli araçların olmaması, aşırı motivasyon, küçük risk karşısında yüksek kar beklentisi ve çevresel etkiler olarak sayılabilir. (Emhan, 2009, s.212)

Riskleri meydana geldikleri sebeplere göre içsel ve dışsal riskler olarak sınıflandırabiliriz. İşletmeler karşılaşabilecekleri riskleri kabul ederek faaliyetlerini büyütebilirler. Bu nedenle işletmeler meydana gelebilecek riskleri önceden belirlemeleri ve karşılaşılabilecek tehditleri en aza indirebilmek için önlemler almaları gerekir. (Göğüş, 2012, s.17-18)

2.1.1. İçsel Riskler

İçsel riskleri finansal, yasal, itibar, stratejik ve operasyonel olarak beş boyutta incelenebilir.

- **Finansal riskler**, işletmenin finansal süreçleri ile ilgili karşılaştığı tehlikelerdir. Bunlar, kur riski, piyasa riski, kredi riski, faiz oranı riski, likidite riski olarak sınıflandırılabilir.
 - **Kur riski**, işletmenin yabancı para birimlerinin değerlerindeki değişimden kaynaklanan döviz borçları ve alacaklarındaki olumsuz etkilenmesidir. (Usul ve Mizrahi, 2016, s.12)

- **Piyasa riski**, ekonomik dalgalanmalardan kaynaklanan işletmenin karını olumsuz etkileyebilecek risklerdir. Piyasa riski diğer riskleri kredi riski, likidite riski, faiz riski ve kur riskini olumsuz yönde etkiler. Örneğin, piyasadaki dalgalanmalar işletmenin satış gelirini olumsuz yönde etkileyebileceği gibi buna bağlı olarak kur riski, faiz riski ve likidite riski de olumsuz olarak etkilenecektir. (Usul ve Mizrahi, 2016, s.12)
- **Kredi riski**, işletmenin karşı tarafa vermiş olduğu söz ya da sözleşmede yazan yükümlülüklerini gerçekleştirememesinden kaynaklanan risklerdir. (Usul ve Mizrahi, 2016, s.12) Kredi riski finans sektörünün karşı karşıya kaldığı en önemli risk türüdür. Temettü riski, hukuki risk, kredi yoğunlaşma riski ve kredi taraflarının yükümlülüğünü tamamlamama riski olarak dört unsur kredi riskine örnek sayılabilir. (Aktaş, 2015, s.44-45)
- **Faiz oranı riski**, faiz oranlarındaki meydana gelen değişikliklerin işletmenin borç tutarı üzerinde oluşan olumsuz etkidir. (Usul ve Mizrahi, 2016, s.12) Bir başka deyişle, faiz oranlarındaki beklenmeyen yöndeki hareketlerin banka veya yatırımcıların ekonomik kayba uğrama olasılığıdır. Bu risk yüksek tutarda dış kaynak kullanan işletmeleri önemli ölçüde etkilemektedir. (Aktaş, 2015, s.56)
- **Likidite riski**, işletmenin elindeki varlıklarını borçlarını ödemek için nakite dönüştürememe riskidir. Diğer bir deyişle, işletmenin vadesi gelen borç tutarını elinde varlıkları olmasına rağmen istediği zaman nakit çevirememesinden kaynaklanan risklerdir. (Usul ve Mizrahi, 2016, s.12) Yükümlülük vadelerinin varlık vadelerinden daha uzun olduğu durumlarda likidite riski artmaktadır. Kısacası elde tutulan mali varlığın istenilen fiyatta ve zamanda elden çıkarılamaması ya da transfer edilememesi durumunda zarara uğrama olasılığı olarak tanımlanabilir. Buna en iyi örnek bankaların borç ve alacak kalemleri arasındaki vade uyumsuzluğudur. (Aktaş, 2015, s.64)

- **Yasal riskler**, mevzuatlarda meydana gelen deęişikliklere ayak uyduramamak işletme faaliyetini etkileyerek kurum için risk oluşturur. Örneęin, küreselleşme ve teknolojik gelişmeler sonucunda uluslararası işletmeler birçok hukuki düzenlemeye tabi olur. Bu nedenle işletmelerin ulusal düzenlemelere uyum sağlamak dışında yabancı ülkedeki yasal düzenlemelere de uyum sağlama mecburiyetiyle riske maruz kalma olasılığı artar. (Özbilgin, 2012, s.89-90)
- **İtibar riski**, işletme içerisindeki ve dışarısındaki kişilerin kurum itibarına karşı tutumlarıdır. Kurumsal itibar işletme için güçlü rekabet ortamı ve müşteri sadakati sağlar. Böylece işletme Pazar payını arttırarak oluşabilecek kriz ortamını başarılı bir şekilde yönetebilir. İşletme kurum itibarının olumsuz olabileceęi durumlardan kaçınmalıdır. Aksi takdirde riske maruz kalır. (Usul ve Mizrahi, 2016, s.13)
- **Stratejik risk**, işletmelerin deęişen piyasa koşullarına gereken ilgiyi göstermemelerinden veya deęişimi fark edememelerinden kaynaklanan risklerdir. Örneęin, işletmelerin müşteri taleplerinde oluşan deęişimler, rekabet ortamındaki deęişimler ya da müşteri portföy deęişimlerinde oluşan deęişimler nedeniyle karşılaştığı risklerdir. (Usul ve Mizrahi, 2016, s.13)
- **Operasyonel riskler**, işletmede iç kontrol sisteminin eksikliğinden ya da etkin olamamasından kaynaklanan hata ve hilelerin fark edilememesinden, personelin yapılan iş için yetersizliği ve işletme kurallarına uygun hareket etmemesinden, yönetim ve bilgi teknolojilerindeki hata ve aksaklıklardan, deprem, yangın, sel gibi doğal afetlerden kaynaklanan risklerdir. (Usul ve Mizrahi, 2016, s.13-14)

2.1.2. Dışsal Riskler

İşletme dışında beklenmeyen bir anda gerçekleşen ve işletme süreçlerini ve kararlarını etkileyen risklerdir. Dışsal riskler toplumsal gelişmeler, yasalarda

meydana gelen deęişimler, ekonomik gelişimler ve pazardaki gelişmelerden kaynaklanabilir. Bu kaynakların sebepleri aşığıdaki Tablo 1.1. 'de gösterilmiştir. (Göğüş, 2012, s.19)

Tablo 1.1. Dışsal Risklerin Dayandığı Sebepler

Toplumsal Gelişmelere Dayalı Riskler	Ekonomik Gelişmelere Dayalı Riskler	Yasalardaki Gelişmelere Dayalı Riskler	Pazardaki Gelişmelere Dayalı Riskler
<ul style="list-style-type: none"> • Tüketici davranışları • Çalışma ve tatil sürelerinin deęiřmesi • Politik davranışların deęiřmesi 	<ul style="list-style-type: none"> • Fiyatlardaki gelişme • Gelir dağılımı konusundaki gelişmeler • Yeni yatırım olanakları • Sermaye pazar/pazarlarındaki gelişmeler 	<ul style="list-style-type: none"> • Vergi ve iş hukukunun yenilenmesi • Çevreyi koruma konusundaki deęişimler 	<ul style="list-style-type: none"> • Rekabet deęiřimi • Talebin deęiřmesi • Teknolojinin deęiřimi • Global pazarlardaki deęişim • Kalite anlayışı • Tedarik süreleri

Kaynak: (Göğüş, 2012, s.19)

2.2. Risk Yönetimi ve Risk Yönetim Süreçleri

Risk yönetimi kavramı ilk kez Amerika Birleşik Devletleri'nde 1950'li yılların sonlarında kullanılmaya başlanmıştır. Risk yönetimi olasılık planlaması ile birlikte "eđer olursa ne olur" ve "ya olursa" sorularını beraberinde getirir. Risk yönetimi, işletme ve kişilerin finansal pozisyonlarının ne kadar risk taşıdığıнын ölçülmesi ve bu ölçütün kabul edilebilir bir risk seviyesine çekilmesidir. (Emhan, 2009, s.213)

Risk yönetimi, işletme varlıklarına ve personeline yönelik ortaya çıkabilecek tehlikeleri belirleyerek yapılan değerlendirmeler sonucunda oluşabilecek tehlikeleri belirlenen yöntemlerle en az seviyeye indirme süreci olarak tanımlanabilir. (<https://www.hmb.gov.tr/ic-kontrol-okuma-listesi>, 2006, s.2)

Başka bir tanıma göre risk yönetimi, işletme içerisinde meydana gelebilecek zararları ölçmek için kullanılan yöntemler ile zararları engellemek için tedbir alarak üst yönetim ile bilgi akışını sağlayarak hızlı karar alabilme, bulguları raporlama ve değerlendirme sürecidir. Yapılan çalışmalara göre işletme başarısızlığının en sık karşılaşılan sebepleri arasında zayıf işletme yönetimi ve riski yönetmek için kullanılan yetersiz prosedürler gösterilmiştir. (<https://tokkder.org/tokkder-dergi/1080>, 2011, para.13)

Küreselleşme ve gelişen teknolojik imkanlar ile birlikte oluşan yeniliklere ve rekabet ortamına kısa sürede kolaylıkla ayak uydurabilmek işletmenin başarısını etkileyen unsurlardır. Dolayısıyla, değişen çevre faktörüne karşı risk yönetimine duyulan ihtiyaç zamanla artmıştır. (Göğüş, 2012, s.21)

İşletmeler kabul edebilecekleri risklere karşı uygulanacak prosedürleri belirler. Belirlenen prosedürler ile tutarlı ve bilinçli risk ve risk seviyeleri belirlenerek istenmeyen riskler yok edilir. Belirlenmiş olan prosedürlerde prosedürleri uygulayacak personelin nitelikleri, takip edilecek şirket stratejileri, risk ölçme yöntemleri ve risk tolerans seviyelerini yansıtan ilkeler ve risk yönetim ekibinin görev ve sorumlulukları gibi konular yer alır. (<https://tokkder.org/tokkder-dergi/1080>, 2011, para.16)

Risk yönetiminin ana amacı, riskin sonuçlarına karşı farkındalığı arttırarak riskin oluşma sıklığını ve zarar verici etkisini azaltmaktır. (Aktaş, 2015, s.67) Risk yönetiminin amacı işletmede risk oluşmasını tamamen önlemek veya oluşan risklere karşı tamamen koruma sağlamak değil, işletmenin varlığını sürdürmesi ve başarısını arttırmasını sağlamaktır. Risk yönetiminde önemli bir konuda risk maliyetini en aza indirmek için fayda ve maliyet analizinin yapılmasıdır. Risk

maliyetinin işletme için kabul edilebilir bir seviyede olması gerekir. (Göğüş, 2012, s.22)

Riskleri en aza indirmek veya önlemek için işletmenin iç denetim birimi tarafından risk değerlendirmesinin yapılması ve risk odaklı denetim planının oluşturulması ve uygulanması gerekir. (<https://www.hmb.gov.tr/ic-kontrol-okuma-listesi>, 2006, s.2)

Etkin bir risk yönetimi sürecinin risk tanımlaması, riskin ölçülmesi, kontrol edilmesi ve izlenmesi olarak dört bileşeni vardır. (<https://tokkder.org/tokkder-dergi/1080>, 2011, para.18)

Risk tanımlaması sürecinde, ilk olarak işletmenin hangi risk türleri ile karşı karşıya olduğunu belirlemek ve yönetebilmek için riskin tanımlanma sürecidir.

Riskin ölçülmesi süreci, işletmenin karşılaşacağı riskler belirlendikten sonra risklerin işletmede meydana getireceği risk seviyesi sonuçlarının tespit edildiği süreçtir. Burada işletmenin risk hassasiyet durumu belirlenir ve elde edilen sonuçlar yönetim kurulu ve üst yönetime raporlanır. İlgili yönetim birimi risk yönetimi politikalarını ve riske ilişkin sınırlamaları belirlerken bu bilgileri dikkatte alır.

Risklerin kontrol edilmesi süreci, işletmedeki risklerin kontrol edilerek olumsuz etkileri minimum seviyeye indirmek amacıyla riskten kaçınma, riski azaltma ve dengede tutma gibi yöntemlere başvurma sürecidir.

Risklerin izlenme süreci ise risklerin doğru olarak belirlenmesi, ölçülmesi ve meydana gelen risk profillerindeki değişiklikleri izlemek için işletmede yönetim bilgi sistemleri ile risk kontrol sistemlerinde oluşan değişikliklerin tespit edilmesi sürecidir.

2.2.1. Risk Yönetim Stratejileri

Risk yönetiminde kullanılan teknikler riskten kaçınma, riski kontrol altında tutma, riski transfer etme, riski azaltma ve riski sigorta ettirme olarak sıralanabilir.

2.2.1.1. Riskten Kaçınma

Riskten kaçınma; riski artıran maliyetlerle uğraşmama ya da riskli işlemleri terk etme yöntemi olarak tanımlanabilir. Meydana gelebilecek olumsuz olaylara karşı alınması gereken önlemleri kapsamaktadır. Riski kontrol altında tutma; en yaygın kullanılan yöntemdir. Meydana gelebilecek riskler ve sonuçları hesaplanıp ya da tahmin edilerek kontrol altında tutmak yöntemler geliştirilir. (Emhan, 2009, s.218)

Riskin meydana gelme ihtimalini imkansız hale getirerek belirsizliği ortadan kaldırma stratejisidir. İşletmeler kendilerini korumak için riskin sonuçlarını kabul etmeyebilir ve risk içeren durumlara girmeyi göze almayabilir. Riskten kaçınırken dikkat edilmesi gereken nokta büyük bir fırsatın kaçırılmamasıdır. (Celayir, 2021, s.132)

2.2.1.2. Riski Transfer Etme

Riski transfer etme; riski meydana getiren varlık veya durumları transfer etme (devretme) yöntemidir. (Emhan, 2009, s.218)

Etkisi yüksek ama düşük ihtimal olarak değerlendirilen riskler için riski transfer etme stratejisi izlenebilir. Riskin kontrol edilebilmesi için transfer edilmesi

karşılaşılabilecek zararın mali ve hukuki sorumluluğunun da transfer edilmesi anlamına gelmektedir. Riskin transfer edilmesinin başka bir yolu da sigorta ve teminattır. (Celayir, 2021, s.132)

2.2.1.3. Riski Azaltma

Riski azaltma; maruz kalınan riski azaltmaya yönelik uygulanan yöntemdir. Riski sigorta ettirme; karşılaşılan riskin ekonomik sonuçlarını en aza indirmek için belirli bir prim karşılığı riski devretme yöntemidir. (Emhan, 2009, s.218)

Riski azaltma, risklerin ihtimal ve etkisini en aza indirerek riskin kabul edilebilir bir seviyeye getirilmesi için risk boyutlarının küçültülmesi stratejisidir. Risklerin ihtimal ve etkisinin azaltılması kontrollerin iyileştirilmesi noktasında önemli bir süreçtir. Riski azaltmanın başka bir yöntemi de riskin paylaşılmasıdır. Buradaki amaç işletme faaliyeti ve kaynağı ile ilgili herhangi bir kayıp olması durumunda her şeyin aynı anda etkilenmemesi için düzeltici çalışmaların yapılmasıdır. Bir kısım riske maruz kalırken diğer kısım riske maruz kalmadan kurtulmuş olacaktır. (Celayir, 2021, s.132)

2.2.1.4. Riski Kabul Etme

Riski kabul etme; riske karşı uygun ihtimalleri göz önünde bulundurarak riskin getireceği sonuçlara tepki vermeme durumudur. Küçük kayıplara neden olan riskler için riski kabul etme stratejisi en sık tercih edilen stratejidir. Bütün riskler transfer edilemez ve bu yüzden riski kabul etmekten başka çare olmayabilir. Yani, riski kabul etmek riskin gerçekleşme ihtimali ve riskin gerçekleşmesi durumunda herhangi bir şey yapılmaması durumudur. (Celayir, 2021, s.131)

İşletmenin yönetim şekli ve anlayışı ne olursa olsun başarılı bir yönetim için mutlaka işletme içerisinde risk yönetiminin uygulanması gerekir. Her işletmede mutlaka risk vardır ve bu risklerin karşılanması gerekir. (Aktaş, 2015, s.44-45)

Risk kabul edilebilir, transfer edilebilir ve yok edilebilir. Riski azaltmak ve kabul edilebilir bir seviyede tutmak için kontrol faaliyetleri belirlenmektedir. Risk yönetiminin amacı, riskten kaçmak değil risklerin belirlenerek makul bir seviyede tutulmasının güvence altına alınmasıdır. (Celayir, 2021, s.132)

2.3. Risk Odaklı İç Denetim

İşletmeler geçmişte yaşanan skandallar neticesinde geleneksel iç denetim modelinden risk odaklı iç denetim modeline geçişin bir zorunluluk olduğunu benimsemişlerdir. Risk odaklı iç denetim kavramı 1990'lı yıllarda hayatımıza girmiş ve günümüzde göz ardı edilemeyecek bir iç denetim süreci haline gelmiştir.

Risk odaklı denetim, işletme faaliyetlerinin farklı bir bakış açısıyla incelenerek işletme hedefleri ve stratejileri göz önünde bulundurularak işletme süreçlerinin değerlendirilmesi, risk faktörlerinin geliştirilmesi ve başarı faktörlerinin bir bütün olarak incelenmesidir. Başka bir ifadeyle risk odaklı denetim, az risk taşıyan alandan daha fazla risk taşıyan alana odaklanma yaklaşımıdır. (Usul ve Mizrahi, 2016, s.4) Risk odaklı iç denetimin amacı, yönetim kuruluna, işletmenin risk yönetimi süreçlerinin hedeflenen şekilde yürütüldüğünü, risk yönetim sürecinin sağlam ve tutarlı bir tasarıma sahip olduğu, risklere karşı alınan tedbirlerin verimli ve yeterli olduğu ve risklere karşı alınan tedbirlere yönelik sağlam ve tutarlı bir iç kontrol sisteminin uygulanmakta olduğu hususlarında bağımsız güvence sağlamaktır. (Göğüş, 2012, s.47-48)

İşletme hedeflerinin yerine getirilip getirilmediği hususunda en önemli unsurlardan bir tanesi de iç denetimdir. Denetim, yönetime işletme faaliyetlerine

ilişkin değerlendirme ve düzeltme süreçleri ile ilgili imkan sağlayan bir faaliyettir. Denetimin amacı, işletme içerisinde oluşabilecek hata ve geliştirilmesi gereken zayıf noktaları belirleyerek ortaya çıkartmak ve düzeltilmesi yönünde önlemler olarak tekrar meydana gelme olasılığını engellemektir. Dolayısıyla, iç denetimin işletme amaçlarına ulaşmasındaki karşılaşılabileceği, risklerin azaltılarak yönetilmesi beklenir. Bu nedenle riski tamamen yok etmek mümkün değildir. Risk odaklı iç denetim faaliyeti yürütülürken işletmenin bütün faaliyet süreçlerinin değerlendirilmesi gerekir. İşletmedeki birbiriyle ilişkili risklerin tanımlanması ve işletmenin olabileceği gibi risk oranı ile karşılaştırılarak değerlendirilmesi esastır. Değerlendirme yapılırken işletmenin risk iştahı ve risk toleransının belirlenmesi gerekir. Sonuç olarak, risk odaklı denetim kurumsal risk yönetimi açısından, işletmenin bütün departmanları tarafından tam anlamıyla benimsenerek eşit oranda risk yönetim uygulamasının var olmasını sağlaması konusunda yardımcı olur. Risk odaklı iç denetim, iç denetimin kurumsal risk yönetimi üzerinde geliştirilmiş hali olarak düşünülebilir. (Göğüş, 2012, s.48-50)

2.4. Geleneksel İç Denetim ile Risk Odaklı İç Denetimin Karşılaştırılması

Risk odaklı iç denetimi geleneksel iç denetimden ayıran en önemli özelliği amacının işletmeye değer katması olmasıdır. İç denetimin bakış açısı risk odaklı iç denetim ile birlikte geleceğe yönelik olarak değişmiştir. İşletmede gelecekteki olaylara odaklanarak işletmenin hedeflerine ulaşmasını engelleyebilecek bütün riskler risk odaklı iç denetimin kapsamını oluşturmaktadır. İşletmede iç kontrol faaliyetlerinin planlanan şekilde yürütüldüğünü doğrulamak, işletme faaliyetlerinin işletme politikalarına uygun yürütüldüğünden ve işletme varlıklarının korunduğundan emin olmak geleneksel iç denetim anlayışında olduğu gibi risk odaklı iç denetimin de başlıca amaçları arasında yer alır. Her iki yaklaşımın ortak noktası ise kontrol değerlendirmelerinin ilgili birim yöneticileri ile denetim komitesine rapor olarak verilmesidir. Her iki yaklaşımın arasındaki fark ise

amaçlara ulaşmak için tercih edilen yöntemlerin kapsamı ile ilgilidir. Risk odaklı iç denetim süreci risk değerlendirme ve denetimin planlama aşamalarının belirlenmesiyle oluşur. (Türedi, Zor ve Gürbüz, 2015, s.12-13)

Geleneksel iç denetimde iç kontrol faaliyetlerinin etkinliğini ve verimliliğini denetlemek amacıyla işletme faaliyetlerinin belirlenmiş olan politika ve prosedürlere uygun olup olmadığı araştırılmaktaydı. Risk odaklı iç denetim ile birlikte uygunluk denetimi anlayışından risk denetimi anlayışına geçilmiştir. Risk odaklı iç denetim ile geleneksel iç denetim arasında iş yoğunluğu açısından da farklılıklar mevcuttur. Geleneksel iç denetimde iç denetçi zamanının birçoğunu planlama, kullanılacak teknik ve iç kontroller ile ilgili ayrıntılara ayırıyorken, risk odaklı iç denetimde işletme faaliyetlerinin anlaşılması, maruz kalınan ya da kalınacak risk ve risk yönetimi süreçlerine daha fazla zaman ayırıyor. Geleneksel iç denetimde geçmiş faaliyetler üzerindeki hata ve hilelerin ortaya çıkarılmasına odaklanılırken, risk odaklı iç denetim işletmede hatalı veya hileli işlemlerin oluşmasını önlemeye odaklanır. Geleneksel iç denetimde iç denetçi iç kontrol sürecine odaklanarak fayda maliyet etkinliğinin sağlanıp sağlanmadığına ilişkin tavsiyelerde bulunur. Risk odaklı denetimde iç denetçi riskler çeşitlendirilmiş mi, paylaşılmış mı, transfer edilmiş mi ve risklerden sakınılmış mı gibi sorulara cevap aramaya odaklanır. (Kishalı ve Pehlivanlı, 2006, s.80-82)

Aşağıdaki Tablo 2.1.'de risk odaklı iç denetim ile geleneksel iç denetim arasındaki farklar özetlenmiştir.

Tablo 2.1. Risk Odaklı İç Denetim ile Geleneksel İç Denetimin Karşılaştırılması

Özellikler	Geleneksel İç Denetim	Risk Odaklı İç Denetim
İç Denetimde Odak Nokta	İç Kontrol	Risk
İç Denetim	Düzeltilici yaklaşım, olaylardan sonra harekete geçme, aralıklı gözetim	Önleyici yaklaşım, sürekli gözetim
İç Denetim Testleri	Kontrol odaklı	Risk odaklı
Risk Değerleme	Risk unsurları	Senaryo planlaması
İç Denetim Yöntemleri	Kontrol testlerindeki ayrıntılar eksiksiz olarak uygulanmalıdır	İşletme risklerinin sınırları geniş bir şekilde belirlenmelidir
İç Denetim Önerileri	İç kontrole yönelik olarak titiz bir şekilde fayda-maliyet etkinliği sağlanmalıdır	Risk yönetimine yönelik olarak risk çeşitlendirmesi, riskten sakınma, riskin paylaşımı ve riskin aktarılması
İşletmede İç Denetimin Rolü	Bağımsız denetim konumu	Risk yönetimi ve üst yönetimle bütünleşik konum

Kaynak: Türedi, Zor ve Gürbüz, 2015, s.13

2.5. Risk Odaklı İç Denetim Süreci

Risk odaklı denetim sürecinde, iç denetçiler işletmenin maruz kaldığı risklere karşı önleyici stratejiler geliştirmeye yönelik çalışmalarda bulunurlar. İç denetçiler, işletmedeki var olan riskleri anlayarak işletme kaynaklarını buna göre yönetirler. Böylece işletmenin iç kontrol sistemindeki etkinlik ve verimliliğini ölçerek risklerin ortaya çıkartılması konusunda sigorta görevi üstlenerek güvence verirler. İşletme risk yönetimi süreci başarılı bir şekilde gerçekleştirilmiş olur. Risk odaklı denetim süreci, işletmede maruz kalınabilecek riskin analiz edilmesiyle başlar. Risk analizi, riskin işletmeye etkisini tahmin etme, riskin meydana gelme olasılığını değerlendirme ve riskin nasıl yönetilmesi konusunda inceleme yapma

işlemdir. Risk değerlendirmesi yapılırken dikkat edilmesi gereken husus risklerin birbirleriyle kıyaslanmayacak derece farklılıklar göstermesidir. Bu sebeple risk analizi iyi yapılmalı ve orta çıkma olasılığı yüksek ve etkisi büyük olan riskler yakından takip edilmeli ve daha sıkı kontrol mekanizmaları kurularak etkin bir iç denetim sistemi oluşturulmalıdır. (Usul ve Mizrahi, 2016, s.5-6)

Özetle, risk odaklı iç denetim süreci iç denetim kavramı ile risk yönetimi sürecinin geliştirilmiş hali olarak yorumlanabilir. (Göğüş, 2012, s.49) Risk odaklı iç denetim süreci riskin tanımlanması, riskin değerlendirilmesi, denetim planının oluşturulması, denetimin yapılması, raporlama ve izleme aşamalarından oluşur.

2.5.1. Riskin Tanımlanması

Risk odaklı iç denetim sürecinde ilk aşama işletmenin amaçlarına ulaşmasını engelleyen risklerin tanımlanmasıdır. Riskin tanımlanması, işletme süreçlerinin değerlendirilerek karşılaşılabilecek tehlike ve fırsatların belirlenmesidir. Başarılı bir risk analizi için işletmeyi etkileyen iç ve dış risklerin tanımlanması gerekir. Riske eğilimli olan alanlar belirlenerek yoğun yüksek riske sahip alandan düşük riske sahip alana doğru bir yaklaşım benimsenmelidir. (Usul ve Mizrahi, 2016, s.9)

İşletme riskleri tanımlarken dikkat edilmesi gereken en önemli hususlardan biri riskin türüdür. İşletmede karşılaşılan ve yönetilmesi gereken riskleri doğal ve kalıntı risk olarak iki grupta inceleyebiliriz. Doğal risk, işletmenin hiçbir önlem almadığı takdirde maruz kaldığı risk türüdür. Kalıntı risk ise işletmede doğal riske karşı önlem alındıktan sonra maruz kaldığı risk türüdür. (Türedi, Zor ve Gürbüz, 2015, s.9)

Tanımlanan riskler sıralanır ve yüksek, orta ve düşük olarak seviyelerine göre önceliklendirilir. Bu seviyeye risk derecelendirmesi denilmektedir.

2.5.1.1. Yüksek Risk Düzeyi

Yüksek riskli faaliyetlerin, çok fazla sayıda işlemlerin olduğu, faaliyet yapısının karmaşık olduğu ve riskli faaliyetlerin yoğun olduğu risk durumlarının işletme kaynak durumuna göre büyük olduğu durumları ifade etmektedir. İşletme gelirini ve sermayesini olumsuz yönde etkileme olasılığı yüksektir. (Celayir, 2021, s.171)

2.5.1.2. Orta Risk Düzeyi

Risk durumunun işletme kaynaklarına göre makul bir seviyede olduğu, makul seviyede işletme faaliyetlerinin bulunduğu durumu ifade etmektedir. İşletme gelirini ve sermayesini olumsuz yönde etkileme durumu makul seviyededir. İşletmede zarar olması durumunda mali yapıyı olumsuz etkilemeden telafi edilebilmektedir. (Celayir, 2021, s.172)

2.5.1.3. Düşük Risk Düzeyi

İşletmede riskin meydana gelmesi durumunda mali yapıya etkisi küçük ve sınırlıdır. (Celayir, 2021, s.172)

2.5.2. Riskin Değerlendirilmesi

Risk odaklı denetim, riskin analiz edilmesi ve tanımlanması süreciyle başlar. Riskin işletmede meydana gelme olasılığını değerlendirme, meydana

getireceđi etkisini tahmin etme ve riskin yönetilmesine ilişkin inceleme yapma sürecidir. Risk deđerlendirmesi yapılırken karşılaşılabilecek zorluk, risklerin birbirleriyle kıyaslanamayacak farklılıklar göstermesidir. Bu yüzden, işlemedeki risk analizi iyi yapılmalı, risk olasılığı etkisi orta ve yüksek çıkan risk türleri yakından takip edilerek, sıkı kontrol mekanizmaları uygulanmalı ve etkin bir iç denetim sistemi kurulmalıdır. Bu nedenle risk odaklı denetimi gerçekleştirecek olan iç denetçiye büyük sorumluluk düşmektedir. İç denetçi, işletme süreçlerine ve kontrollerine, stratejik ve finansal risk tahminlerine odaklanmalıdır. (Usul ve Mizrahi, 2016, s.51-52)

IIA 2210 Görev Amaçları başlıklı standardına göre, iç denetçi işletme hedeflerine uygun olarak işletmenin iç denetim faaliyetlerinin önceliklerini belirleyen risk esaslı denetim planı yapmak zorundadır. (TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.12)

Basel Komitesi tarafından 2000 yılında yayınlanan rapora göre risk odaklı iç denetimin kapsamı aşağıdaki gibi sıralanabilir: (Kışalı ve Pehlivan, 2006, s.79-80)

- İç kontrol sisteminin yeterliliđi ve etkinliđinin deđerlendirilmesi ve incelenmesi,
- Risk yönetimi ve risk deđerlendirme uygulamalarının etkinliđinin incelenmesi,
- Finansal bilgi, yönetim ve elektronik bilgi sistemlerinin gözden geçirilmesi,
- Finansal tablolar ve muhasebe kayıtlarının güvenilir ve doğru doğruluđunun incelenmesi,
- Risk tahmini ile işletmenin kendi sermayesini deđerlendirme sisteminin incelenmesi,
- İç kontrol sistemi ve işletme süreçlerinin işleyişinin denetlenmesi,
- Raporların güvenilirlik, doğruluk ve zamanındalıđının kontrolü.

İç denetçiler, işletme yönetiminin uyguladığı risk yönetim süreçlerinin etkinliğini ve verimliliğini inceleyip değerlendirerek üst yönetime rapor verirler. Böylece işletme için iyileştirici önlemler geliştirip önererek hem üst yönetime hem de denetim komitesine yardımcı olmalıdırlar. (Kishalı ve Pehlivan, 2006, s.83) İç denetçi denetim çalışması sırasında işletmenin risk değerlemesini yaparak riske karşı makul bir güvence vermek için inceleme yapar. Elde edilen sonuçlara göre riskler kategorize edilir. (Usul ve Mizrahi, 2016, s.58-59)

Riskin değerlendirilmesi aşamasında, işletmede tanımlanmış risk düzeyini ve işletme süreçlerine yönelik kontrol prosedürlerinin uygunluğunu belirlenir. İşletmenin yönetim yapısı, ticari profili, örgütsel yapıdaki değişiklikler, üst yönetim ve denetim komitesindeki değişiklikler gibi alanlarda incelemeler yapılarak riskli alanlar derecelendirilir. İşletme içerisinde yapılan denetimlerin ve kontrollerin belirlenen kriterlere göre çalışıp çalışmadığının değerlendirilmesi yapılır. (Türedi, Zor ve Gürbüz, 2015, s.9) Değerlendirme yapılırken öncelikle işletmenin risk iştahı ve risk toleransının belirlenmesi gerekir.

Risk iştahı, risk alma istekliliği olarak da tanımlanırken, işletmenin başarısını artırma yolunda hedeflerine ulaşması için göze aldığı risk miktarıdır. Risk iştahı işletme kültürüne göre işletme yönetim felsefesini oluşturulmasına katkı sağlar. (Göğüş, 2012, s.49) İşletmede değerlendirme sonuçlarına göre denetçi yüksek, orta veya düşük risk derecelendirmesini yapar. (Usul ve Mizrahi, 2016, s.23) Risk iştahı, işletme stratejisini oluşturmasında önemli rol oynar. Örneğin, yüksek risk iştah seviyesine sahip işletmeler sermayesinin büyük bir kısmını yeni gelişmekte olan piyasalara yatırabilirken, düşük risk iştahına sahip işletmeler sadece istikrarlı bir şekilde ilerleyen piyasalara yatırım yapmayı tercih edebilir. Bu yönüyle risk iştahı ile kurumsal risk yönetimi bir araya geldiğinde işletmede beklenen katma değer ile işletmede risk iştahının uyumlaştırılmasına yönelik strateji belirlemede yol gösterici görevini üstlenirler.

Risk toleransı, işletme içerisinde belirlenen hedeflerin gerçekleşme sürecinde kabul edilebilir bir sapma derecesidir. İşletmede risk toleransı belirlenirken, belirlenen hedefin gerçekleşme riskine karşı gerekli önlemler alınarak risk iştahı ile çarpıştırılır. Risk toleransı olarak risk iştahı içerisinde kalması işletmenin amaçlarına ulaşmasını sağlar. (Göğüş, 2012, s.49)

Risk değerlendirme süreci; riskin önem derecesinin ve etkisinin tahmini, riskin oluşma olasılığının ve oluşma sıklığının değerlendirilmesi ve riskin nasıl yönetileceği ve hangi eylemlerin dikkate alınacağını belirlenmesi aşamalarından oluşur. (Kızıboğa ve Özşahin, s.224) Özetle risk değerlendirmesi, işletmedeki riskli alanların belirlenmesi ve riskleri engellemek amacıyla önlem alınması için gerekli adımların atılmasını sağlayan süreçtir. Risk değerlendirme süreci kayıp senaryoları geliştirmek, kontrol prosedürleri ve riskleri belirlemek, risk kategorilerini tanımlamak, risklerin oluşma sıklığını ve meydana gelebilecek zararların boyutunu değerlendirmek, risk seviyelerini ve risk kontrol maliyetlerini belirlemek olarak sıralanabilir (Usul ve Mizrahi, 2016, s.24) :

Risk değerlendirme süreci aslında işletmede meydana gelebilecek risklerin uygun bir şekilde ölçülmesini sağlar. Yani işletmede riskin gerçekleşme olasılığı ile riskin gerçekleştiği durumda yarattığı etkinin hesaplanmasıdır. Risk ölçülmesi yapılırken, işletmenin finansal performansı gözden geçirilir, uygulanan muhasebe prosedürleri değerlendirilir, prosedürlerde değişiklik yapıldıysa nedeni tespit edilir, işletme faaliyetlerinin analitik incelemesi yapılır, bütçe hazırlama ve kullanma seviyeleri belirlenir, işletmenin performansı sektördekiyle karşılaştırılır. (Usul ve Mizrahi, 2016, s.29) İşletmede risk değerlendirme sürecinde dikkat edilmesi gereken hususlardan bir tanesi de riske karşılık verme yöntemlerinin belirlenmesidir. Bu yöntemler riski kabul etmek, azaltmak amacıyla kontrol etmek, devretmek ve kaçınmak şeklinde dört aşamadan oluşmaktadır. (Türedi, Zor, ve Gürbüz, s.10-11)

- **Riski kabul etmek**, eğer doğal sebeplerden kaynaklanan risk işletmenin üstlendiği risk iştah seviyesi içinde kalıyorsa, işletmeye sağlanan faydanın alınacak önlemlerin maliyetinden düşük olduğunun anlaşılması durumunda ve yönetimin kontrolü dışında gelişen riskler işletme yönetiminin riski üstlenmeyi uygun bulduğu yöntemdir. Örneğin, bazı riskler işletme faaliyeti sonlanmadıkça ortadan kalkmaz bu durumda faaliyeti sonlandırmak mümkün olmayabilir, dolayısıyla risk kabul edilir.
- **Riski kontrol etmek**, işletmede kontrol faaliyetleri ile riskleri kabul edilebilir bir seviyede tutulması açısından riske cevap verme yöntemidir. Bu yöntem, yönlendirici kontroller, önleyici kontroller, tespit edici kontroller ve düzeltici kontroller olarak dört aşamada değerlendirilir.

Yönlendirici kontroller, bir işin doğru bir şekilde tamamlanabilmesi için gerekli olan niteliği kazandırmak için uygulanan kontrol sürecidir. Örneğin, yeni bir sistem geliştirme üzerinde çalışan bilişim teknolojileri personeline verilerin doğru bir şekilde aktarılmasını sağlamak için yeterli bilgi ve deneyimin kazandırılmasıdır.

Önleyici kontroller, işletmede oluşabilecek risklere karşı kontrol için alınan önlem sürecidir. Örneğin, sistem üzerinden verileri aktarırken verilerin bozulma ya da yok olma riskine karşı bilgisayar sistemi üzerinde test yapılmasıdır.

Tespit edici kontroller, işletmede var olan sistemin doğru işleyip işlemediğini anlamak için yapılan kontrol sürecidir. Örneğin, işletme faaliyetleri içerisinde yeni bilişim sistemini kullanmaya başladıktan sonra eski sistemden yeni sisteme aktarılan bilgilerin doğru olup olmadığını anlamak için test yapılmasıdır.

Düzeltilici kontroller, işletmede meydana gelmiş olan yanlış işlem veya hatanın düzeltilmesine yönelik uygulanan kontrol sürecidir. Örneğin, işletmedeki eski sistemden yeni sisteme aktarılan veriler karşılaştırılırken ortaya çıkan hatalı aktarımın düzeltilmesidir.

- **Riski devretmek**, işletmede meydana gelebilecek risklere karşı bazı uygulamalar ile karşılık verilmesidir. İşletme faaliyetlerinin belirli bir kısmını uzmanlığı olan başka bir işletmeye devretme sürecidir. Örneğin, işletmede meydana gelecek risklin oluşturduğu zarara karşı sigorta anlaşması yapılarak riskin devredilmesidir. Burada risk devredilse de işletme yönetiminin sorumluluğu halen devam etmektedir.
- **Riskten kaçınmak** ise, işletmenin kabul edilebilir risk düzeyini aşan risk seviyesi için uygulanan kontrol sürecidir. Bu süreçte işletme risk değerlendirmesi sonucunda risk teşkil eden faaliyetlerden ya da iş anlaşmalarından vazgeçebilir.

Özetlemek gerekirse, işletmeler hedeflerine ulaşabilmek için iç kontrol ve iç denetim sistemlerinin etkinliğini ve verimliliğini ölçmek için etkili bir risk yönetim süreci oluşturmalıdırlar. Bu sayede işletmede oluşabilecek riskleri önceden tespit ederek, riski kabul etme, azaltma veya devretme ya da kaçınma yollarından işletmeye değer katacak en uygun yöntem belirlenerek uygulanır. İşletme başarıya ulaşabilmek için yönetim kurulu ve diğer çalışan personelleri ile iç kontrol sisteminin etkin ve verimli kullanılması yönünde gerekli önlemleri almış olur.

Usul ve Mizrahiye göre, riskin değerlendirilmesi süreci işletmeye sağladığı faydalar aşağıda maddeler halinde özetlenmiştir. (2016, s.23)

- İşletmenin amaçlarına ulaşmasını kolaylaştırır.
- İşletmede sürprizlerle karşılaşmayı azaltır ve başarılı iş planları yapılmasını ve uygulanmasını sağlar.
- İşletme içindeki iş birliğini ve tutarlılığı güçlendirir.
- Kamuoyunun işletme imajı hakkında olumlu düşünmesini, açıklığı, daha fazla kazanmayı, bilgilendirmeyi sağlar.
- İşletmede pozitif kültür ortamının oluşmasını sağlar.

2.5.2.1. Risk Matrisinin Oluřturulması

Risk odaklı denetimde řiřletmenin maruz kalacađı riskler tanımlanır ve ađırlık seviyesine gre sıraya konularak risk seviyeleri belirlenir. Risklerin azaltılmasına ynelik nlemler alınarak uygulamaya konulur. Risk yaratacađı etki ve gerekleřme olasılıđı ile llmektedir. Etki ve olasılık deđerlendirmesi riskin ne kadar zarar veya etkisi edebileceđinin tespit edilerek gerekli nlemlerin alınması řiřletme amalarına ulařmada nemli katkı sađlar. (Aksoy, 2018, s.14)

Tablo 2.2. Risk Etki ve Olasılık Derecesi

Risk Etki Derecesi		Risk Olasılık Derecesi	
Olası Etki	Puanı	Riskin Olma Olasılıđı	Puan
ok Yksek	5	ok Yksek	5
Yksek	4	Yksek	4
Orta	3	Orta	3
Dřk	2	Dřk	2
ok Dřk	1	ok Dřk	1

Kaynak: Aksoy, 2018, s.15

Risklerin oluřma olasılıđı ve risklerin etki derecesi ok yksek, yksek, orta, dřk, ok dřk olarak 5’li likert derecelendirme ile deđerlendirilmektedir. Ařađıdaki tabloda risk sonularının llmesi gsterilmiřtir.

Tablo 2.3. Risk Etki ve Sonuçlarının Ölçülmesi

Risk Sonucu	Risk Olma Olasılığı	Risk Ölçülmesi
İşletmenin uzun süreli veya tamamen kapanması	Neredeyse kesin	Çok Yüksek 5
İşletme amaçlarının kesintiye uğraması	Muhtemel	Yüksek 4
İşletmenin belirli amaçlarının kısa süreli kesintiye uğraması	Mümkün	Orta 3
İşletme hedeflerinde etkisi yok ama sakınca oluşturur	Düşük Olasılık	Düşük 2
İşletme amaçlarına ulaşmada engel oluşturmaz, kısıtlı sakınca oluşturur	Seyrek	Çok Düşük 1

Kaynak: Aksoy, 2018, s.15

Risk değerlendirmesi yapılan her alanın risk sonucu risk seviyesine göre risk matrisine yerleştirilir. Risk matrisi, işletmenin risk durumunu, risk yönetiminin etkinliğini, net risk seviyesini ve risk durumundaki değişiklikleri gösteren esnek ve dinamik bir araçtır. Risk seviyesi düşük olan riskler incelenmeyebilir, risk seviyesi yüksek olan riskler ayrıntılı incelemeye alınabilir. Yüksek risk seviyesindeki riskler detaylı olarak incelendikten sonra sıralama yapılarak yüksek risk seviyesine ait risklerin azaltılması ya da sona erdirilmesine karar verilir. Hangi riske öncelik verilerek müdahale edileceği kararı verilir. En öncelikli risk en önce çözümlenmesi gereken risktir. (Celayir, 2021, s.173-174).

Tablo 2.4. Örnek Risk Matrisi

RİSK MATRİSİ		ETKİ				
		1 Önemsiz	2 Düşük	3 Orta	4 Yüksek	5 Çok Yüksek
OLASILIK	1 Çok Küçük	Anlamsız 1	Düşük 2	Düşük 3	Düşük 4	Düşük 5
	2 Küçük	Düşük 2	Düşük 4	Düşük 6	Orta 8	Orta 10
	3 Orta	Düşük 3	Düşük 6	Orta 9	Orta 12	Yüksek 15
	4 Yüksek	Düşük 4	Orta 8	Orta 12	Yüksek 16	Yüksek 20
	5 Çok Yüksek	Düşük 5	Orta 10	Yüksek 15	Yüksek 20	Tolere Edilemez 25

Kaynak: Maliye Bakanlığı, Kamu İç Kontrol Rehberi, Risk Değerlendirme Standartları, s.2, https://www.ktu.edu.tr/dosyalar/16_00_00_5d20f.pdf

Risk matrisi riskin meydana gelme olasılığı ve meydana geldikten sonra yaratacağı etki olarak iki değişkeni analiz etmek için tercih edilen risk değerlendirme aracıdır. Etki ve olasılık seviyesi en düşük olan riske 1, en yüksek risk seviyesi için 5 verilerek kadar etki ve olasılık değeri verilmektedir ve etki ve olasılık değeri çarpılarak risk değeri ve risk skoru tespit edilmektedir. Bu sonuçlar yukarıdaki örnek 5x5 risk matrisinde gösterilmiştir. (Maliye Bakanlığı, Kamu İç Kontrol Rehberi, Risk Değerlendirme Standartları, s.2, https://www.ktu.edu.tr/dosyalar/16_00_00_5d20f.pdf)

- **Olasılık Derecelendirme;**

1 Çok Küçük: Risk beklenmiyor, risk meydana gelme olasılığı çok zayıf, hiç yok gibi, ihmal edilebilir.

2 Küçük: Risk meydana gelme olasılığı çok az, yılda bir kez tekrarlanabilir, mevcut kontrol sistemi sürdürülmelidir.

3 Orta: Risk meydana gelme olasılığı az da olsa mevcut, yılda bir veya altı ayda bir tekrarlanabilir. Hedeflere ulaşmada zorluklar yaşanabilir.

4 Yüksek: Risk var, ayda bir veya haftada bir tekrarlanabilir, yeniden yapılanma ihtiyacı oluşturur.

5 Çok Yüksek: Risk her gün ve her an olabilir. Hedeflere ulaşmayı engeller.

- **Etki Derecelendirme;**

1 Önemsiz: Riskin etkisi zararsız, herhangi bir kayıp oluşturmaz.

2 Düşük: Riskin etkisi önemli bir değer kaybı oluşturmaz.

3 Orta: Riskin olası etkisi, zarar var ama telafi edilebilir.

4 Yüksek: Riskin etkisi mevcut, önemli zarar ve kayıp oluşturur.

5 Çok Yüksek: Riskin etkisi kesin, telafi edilemeyecek kadar büyük zarar oluşturur.

1-4 skor aralığı kabul edilebilir risk seviyesidir. Riskin en düşük olduğu ve var olan kontrollerin yeterli olduğu seviyedir. 5-8 skor aralığı maliyetsiz tedbir risk seviyesidir. Küçük çaplı kontrollere ihtiyaç duyur ama bu kontroller için maliyet gerekmez. 9-13 skor seviyesi tedbir alınması gereken risk seviyesidir. Yeni kontrol mekanizmasına ihtiyaç duyulmaktadır. Mevcut kontroller yetersizdir ve yeni kontrol uygulamaları ya da mevcut uygulamaları düzenlemek gereklidir. 14-25 skor aralığı kabul edilemez risk seviyesidir. Risk mutlaka önlenmelidir ve riske karşı

yeni kontrol uygulamaları oluşturulmalıdır. Riskli olan faaliyet varsa vazgeçilmelidir. (Duran, 2013, s.48)

2.5.3. Denetim Kaynaklarının Ayrılması

Denetim kaynakları işletme çalışanları, var olan teknolojik imkanlar, dış hizmet sağlayıcıları ve yönetimin finansal desteği olarak sıralanabilir. İç denetim sürecinde iç denetçiler tarafından kaynakların etkin ve verimli kullanılması esastır. Kaynaklar denetimin niteliği, karmaşıklığı ve zaman kısıtlamaları dikkate alınarak denetim alanlarına tahsis edilmelidir. Kaynak dağılımı denetim yöneticisi tarafından en riskli olan alanlara öncelik verilmek üzere belirlenir. Daha fazla riskli alanlar daha fazla personel ihtiyacı ve zaman gerektirir. Denetim kaynaklarının yeterliliği ve risk düzeyleri denetim sıklığını da etkilemektedir. Böylece riskli alanların denetlenme sıklığı diğer alanlara göre daha fazla olması gerektiği için iç denetim ekibi tarafından bu durumlar göz önüne alınarak iç denetim planı oluşturulur. (Adiloğlu, 2011, s.76)

2.5.4. Denetim Plan ve Programının Hazırlanması

İç denetçi denetimin uygulama aşamasına başlamadan önce denetlenecek birim yöneticisi diğer personeller ile denetimin amacı, kapsamı, denetim süresi, kullanılacak yöntemler, denetim sürecinde yardımcı olacak personel ve personelden beklentiler, yönetimin beklentileri, sonuçların raporlanması gibi konularda görüşmeler yapar. Bu görüşmeler neticesinde iç denetçi çalışma planını ve programını hazırlayarak denetime başlar ve bu çalışma planına göre denetim sürecini yürütür. İç denetim planı iç denetim sürecinin etkili, verimli ve ekonomik bir şekilde yürütülmesini sağlamak amacıyla denetimin alanı, konuları, ihtiyaç duyulan kaynaklar ve iş gücünü içerecek şekilde üst yönetim ve birim yöneticileri

ile görüşülerek hazırlanır. Denetim planı, denetime başlamadan önce üst yönetim tarafından onaylanır. Denetim planının revize edilmesi gerekiyorsa üst yönetimin onayı ile değişiklikler gerçekleştirilir. (Adilođlu, 2011, s.76-77)

İç Denetim Standartları bölümünde yer verilen IIA 2010 Planlama başlıklı standardına göre İç Denetim Yöneticisi işletmenin amaçlarına uygun denetim faaliyetinin önceliklerinin belirlenmiş olduğu risk odaklı plan yapmak zorundadır. Risk odaklı iç denetim planı oluşturulması için, İç Denetim Yöneticisi işletme hedeflerini, stratejilerini, risk ve risk yönetim süreçlerini anlamak için üst yönetim ve yönetim kurulu ile iletişime geçer. İşletme faaliyetlerinde, operasyonlarında, sistemlerinde, programlarında ve risklerde meydana gelen değişikliklere yönelik İç Denetim Yöneticisi gerekli durumlarda denetim planını gözden geçirmek ve değişikliklere göre düzenlemek zorundadır. Standardın ilgili maddesine göre; iç denetim planı yılda en az bir kez yapılan yazılı bir risk değerlendirmesine dayanmak zorundadır. İç denetim yöneticisi, denetim görüşleri ve sonuçlar açısından üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerini anlamalı ve dikkate almalıdır. Böylece, işletmeye katma değer yaratma, faaliyetlerini geliştirme potansiyelini değerlendirme ve risk yönetim sürecini geliştirmesinde danışmanlık görevini üstlenmelidir. (TİDE, Uluslararası İç Denetim Standartları, 2017, s.12)

IIA 2200 Görev Planlaması başlıklı standardında, iç denetçiler her görev için amaçları, kapsamı, kaynak dağılımı ve zamanlama konularını dikkate alarak ayrı bir denetim planı hazırlamak ve yazılı hale getirmekle yükümlüdür. Denetim planı, işletmenin hedeflerini, stratejilerini ve riskleri içermelidir. IIA 2201 Planlamada Dikkate Alınması Gerekenler başlıklı standardında ise denetim planında dikkate alınması gereken hususlar aşağıdaki gibidir (TİDE, Uluslararası İç Denetim Standartları, 2017, s.17)

- İşletme faaliyetlerinin hedefleri, stratejileri ve performansını kontrol etmesinin yolları,

- İşletme faaliyetinin hedeflerine ve kaynaklarına yönelik önemli riskler ve bu risklerin etkisinin ve ihtimallerinin kabul edilebilir seviyede tutmanın yolları,
- İşletme faaliyetinin risk yönetimi, kontrol ve yönetim süreçlerinin etkinliği ve verimliliği.

Risk odaklı iç denetim programı öncesi planlama aşamasına yönelik çalışmalara yön veren en önemli unsurlardan bir tanesi işletmenin denetim stratejisidir. İşletme denetim stratejisi, üst yönetimin iç kontrol faaliyetlerine yönelik beklentilerine, uygulanan risk yönetim sürecinin etkinliğine ve denetçiden beklenen destek ve danışmanlık beklentilerine göre belirlenir. Risk odaklı iç denetim programı öncesi planlama aşamasına yönelik çalışmalara yön veren en önemli unsurlardan bir diğeri ise risk envanteridir. Risk envanteri, işletmenin karşılaşacağı risklerin denetim planına yansıtan ve riskleri bir bütün olarak ele alıp değerlendiren rapordur. Rapor, işletmede risk yönetimi kapsamında risklerin belirlenmesi, değerlendirilmesi ve risk iştahı çerçevesinde risk tutumunun belirlenmesi süreçlerinin sonuçlarını kapsar. Risk yönetiminin bir yansıması niteliğinde olan risk envanteri, iç denetçi tarafından işletmedeki önemli riskleri içerip içermediğini, riske karşı alınan önlemlerin yeterli olup olmadığı açısından değerlendirilir. Saptanmış olan riskler denetim raporunda belirtilir ve alınması gereken önlemler ile ilgili tavsiyelerde bulunulur. (Göğüş, 2012, s.54-56)

IIA 2120 Risk Yönetimi başlıklı standardına göre, iç denetim işletmedeki risk yönetimi süreçlerinin etkin olup olmadığını değerlendirmek ve iyileştirilmesi yönünde katkıda bulunmak zorundadır. Etkin bir risk yönetimi süreci için işletme amaçları, işletme misyonunu destekleyici ve aynı paralelde olması, önemli risklerin belirlenmiş ve değerlendirilmiş olması, risklere işletmenin risk iştahı ile aynı seviyeye getiren gerekli risk cevapları seçilmeli ve işletme yönetiminin, yönetim kurulunun, denetim komitesinin ve personellerin sorumluluklarını yerine getirmesine yardımcı olan risk ile ilgili bilginin elde edilmesi ve zamanında işletme

genelinde yayınlanması unsurlarının işletmede var olması gereklidir. (TİDE, Uluslararası İç Denetim Standartları, 2017, s.16)

Standartlar ve yol gösterici genel bilgiler çerçevesinde risk odaklı denetim programı oluşturulurken denetçi aşağıdaki maddeleri dikkate almalıdır. (Usul ve Mizrahi, 2016, s.46-47)

- Denetim ekibindeki kişilerin bilgi ve becerilerine göre iş atamalarının yapılması ve uzman bir kişiye ihtiyaç olup olmamasının belirlenmesi,
- Denetim plan ve tekniğinin oluşturulması için risk değerlemesinin yapılması,
- Güncel risk değerlendirmeleri ile sürekli risk seviyelerini izlemek,
- Neden ve ne için sorularına yönelik test yöntemlerinin belirlenmesi ve kontrol testlerinin ve güven seviyesinin belirlenmesi,
- İletişim stratejilerini belirlemek,
- Sorunların tanımlanamaması gibi gerekli durumlarda ek yöntemlerin belirlenmesi.

Denetim planının oluşturulmasının ana amacı işletme kaynaklarının etkin ve verimli kullanılmasını sağlayarak hatalı sonuca ulaşma riskini azaltmaktır. Denetim planı hazırlanırken işletmenin stratejik amaçları, risk yönetim politikaları, denetim komitesi görüşleri, denetim stratejileri ve denetim için ayrılan kaynaklar dikkate alınmalıdır. Bu bağlamda, yıl içerisinde hangi faaliyet alanlarının denetleneceği, denetimlerin kapsamı ve ne sıklıkla yapılacağı, denetim sürecini kimin yürüteceği ve ihtiyaç duyulan personel sayısını, içerdiği riskler ve denetim zaman planını kapsar. Denetim planı yıllık değil çeyrek dönemleri kapsayan üçer aylık planlandığında riskin ortaya çıkma olasılığını belirleme olasılığını arttırmaktadır. Yapılan denetim sonucunda, hiçbir faaliyet alanı için mutlak seviyede güvence verilememektedir. Verilen güvence seviyesini denetimin kapsamı, denetime ayrılan bütçe, işletmenin içinde bulunduğu sektör riski ve üst yönetimin risk alma istekliliği gibi birçok faktör etkilemektedir. İşletmede istenen güvence seviyesine bağlı olarak

denetim kapsamı ve uygulanacak test miktarı da deęişiklik gösterecektir. Yüksek önem derecesine sahip alanlar için iç denetimden beklenen güvence normal önem derecesine sahip alanlara göre daha yüksektir. (Göğüş, 2012, s.54-55)

İşletmede denetim programının yapılabilmesi için risk analizinin gerçekleştirilmiş risk envanterinin oluşturulmuş olması gerekir. (Göğüş, 2012, s.54-55) İşletme süreçlerinde yapılan risk analizi ve değerlendirilme işlemi yapıldıktan sonra denetim programının oluşturulması aşamasına geçilir. Risk odaklı iç denetim programı oluşturulurken işletmenin büyüklüğü, risk profili ve faaliyet alanları göz önünde bulundurulur. Denetim programı ve riskin değerlendirme süreci denetimi yapan kişinin uygulayacağı tekniklere ve tecrübesine bağlıdır. Denetim programı işletmenin prosedürlerini, niteliğini ve risk değerlendirme yöntemlerini içerecek şekilde oluşturulmalıdır. (Usul ve Mizrahi, s.41) Risklerin önem derecesine göre yüksek risk derecesine sahip alanlar her yıl, orta derecede riskli alanlar iki yılda bir ve az riskli alanların ise üç yılda bir denetiminin yapılmasının uygun olduğu kabul edilebilir. Her yıl yapılan risk değerlendirmelerinin sonuçlarına göre denetim programı güncellenmeli ve deęişiklik varsa denetim planı yeniden tasarlanmalı ve geliştirilmelidir. (Türedi, Zor ve Gürbüz, 2015, s.115)

Denetim programı hazırlanırken önemlilik arz eden dięer bir konu ise risk odaklı iç denetim süreci için görevlendirilecek kişilerin sorumluk, mesleki teknik bilgi, yetenek ve deneyimleri açısından görevlerin açıkça belirlenmesidir. Denetçi ataması yapılırken, ekibin lideri belirlenmeli, beyin fırtınası yapılmalı, işletme bilgisayarları ve yerel ağları birbirine bağlayan sistemler araştırılmalı, eski yapılmış olan denetim raporları ve yönetim raporları araştırılarak incelenmeli, istatistikler ve trendler araştırılmalı, risk analizleri ve işletme yapısında meydana gelen deęişiklikler araştırılmalı, ekip ile karşı karşıya kalınacak riskler tartışılmalı, çalışma kağıtları hazırlanmalı ve paylaşılmalı, toplantı öncesinde müşteri ile ilişki kurulmalı ve denetim programı hazırlanmalı, amaca uygun iş çizelgesi hazırlanmalı

ve elde edilen bilgiler ışığında atamalar gerçekleştirilmelidir. (Usul ve Mizrahi, s.49-50).

İşletmedeki riskli alan ve konulara öncelik verilerek ve denetim maliyetleri de göz önüne alınarak yöneticilerle ve gerektiği takdirde çalışanlarla görüşerek iç denetim planı ile uyumlu iç denetim programı hazırlanır. Hazırlanan iç denetim programının içeriği denetlenecek alanlar ve konular, zaman çizelgesi ve iç denetçilerin isimlerinden oluşur. İç denetim programı için üst yönetim tarafından onay alınması gerekir. Adiloğlu'na göre iç denetim programında aşağıdaki hususlar yer almalıdır. (2011, s.77-78)

- Denetimin amaçları ve denetimin çalışma kapsamının belirlenmesi,
- Denetlenecek işletme faaliyetleri hakkında bilgi edinilmesi,
- Denetimin uygulama aşaması için gerekli kaynakların belirlenmesi,
- Denetim süreçleri hakkında bilgi sahibi olması gereken kişiler ile görüşülmesi,
- Denetlenecek işletme faaliyetleri ve kontrol prosedürleri ile ilgili bilgi sahibi olunması,
- Denetim alanlarının belirlenmesi ve denetlenen kişilerin fikirlerinin alınması için ön inceleme yapılması,
- Ön inceleme tamamlandıktan sonra işletmedeki kontrol amaçlarının ve bu amaçlara ulaşmak için uygulanan kontrol önlem ve prosedürlerinin incelenmesini, denetlenecek faaliyet alanlarının ve kanıt toplama yaklaşımlarının içeriği hakkında açıklamalara yer verilmesi,
- Denetim sonuçlarının ne zaman, kime ve nasıl iletileceğinin belirlenmesi,
- Denetim çalışma planının onayının alınması.

Tüm süreçler tamamlanıp uygun denetim planı ve programı oluşturulup denetim teknikleri belirlenerek denetçi atması görev ve sorumlulukları belirlendikten sonra uygun risk odaklı iç denetimin uygulanma aşamasına geçilir.

2.5.5. Denetimin Yapılması

Denetimin yapılma aşaması uygulama hazırlığı, kontrol testlerinin uygulanması ve test sonuçlarının yorumlanması olarak üç aşamada incelenmiştir.

2.5.1.1. Uygulama Hazırlığı

Uygulama hazırlığı aşamasında, denetimin etkinliği yönünden planlanan faaliyetlerin belirli bir sıralamada gerçekleştirilmesi önemlidir. Bu sıralama, görev planının hazırlanması, denetim personelinin tahsisi, denetim konusunun araştırılması, geçmiş döneme ait denetim raporları ve çalışma kağıtları, istatistik ve trendler, denetime ilişkin çalışma kağıtlarının tasarlanması ve denetimin kapsam ve hedefinin belirlenmesi olarak sıralanabilir. (Pehlivanlı, 2008, s.111)

Denetimin başlangıç ve bitiş tarihini de içeren yıllık denetim planı daha detaylı olarak gerçekleştirilen denetim çalışmalarıdır. Denetim planı aşamasında aşağıdaki hususlar takip edilebilir. (Göğüş, 2012, s.60)

- Denetim süreci ile ilgili bilgi temin edilmesi
- İşletme yöneticileri ve üst yönetim ile ön görüşmeler yapılması
- Başlangıç aşamasında temin edilecek evraklar ve denetim süreci ile ilgili olan kişilerin sağlayacağı şartların belirlenmesi.
- Denetim süreç haritasının çizilmesi, risk ve kontrol aşamalarının belirlenmesi.

İç denetçiler, denetimin uygulama aşamasına geçmeden önce denetlenecek süreç ile ilgili hazırlanmış süreç tanımları ve süreç haritaları, prosedürler ve yönetmelikler, eğer varsa daha önce yapılmış iç denetim faaliyet raporları ve bilgi içeren diğer dökümanlar, bağımsız denetim raporları, kullanılacak sistemlerin teknik özellikleri ile ilgili uzmanlarla görüşmeler, bilgi teknolojileri alt yapısını

geliştirmeye yönelik var olan projeler, yakın zamanda gerçekleşmiş işletmenin finansal ve operasyonel yapısını etkileyen bilgi kaynakları ve belgelerden yararlanabilirler. (Göğüş, 2012, s.60-61)

İç denetçinin hazırlık aşamasında işletmede yürütülen süreçlerin yöneticileri başta olmak üzere üst yönetim ve yöneticiler ile görüşmeler yapması önemli bir husustur. Bu görüşmelerin en önemli amaçlarını yürütülen denetim sürecinin amacının işletmeye açıklanması, işletmenin içinde bulunduğu risklerle ilgili oluşabilecek farklılıklar, işletmede yakın gelecekte gerçekleşebilecek sistemsel, operasyonel ve organizasyonel değişiklikler ile ilgili bilgi edinilmesi, üst yönetimden işletme faaliyetleri ve birimleri ile ilgili özellik arz eden konular hakkında bilgi alınması, denetim sürecinde yardım alınacak personel bilgisi ve denetim zamanlaması olarak belirtebiliriz. İşletme faaliyetleri ile ilgili gerekli bilgilerin elde edildiğinden emin olunduktan sonra uygulanacak denetim sürecinin hangi işlevleri kapsayacağını belirlenerek belgelendirilmesi gerekir. Bu belgede denetimin faaliyet alanı, hangi işletme süreçlerinin denetleneceği, denetlenen birim ile iç denetçilerin sorumlulukları, planlanan denetim süresi ve denetim kapsamı dışında kalan alanlara yer verilir. Aşağıdaki Tablo 2.5’de denetim çalışma örneği yer almaktadır. (Göğüş, 2012, s.60-61)

Tablo 2.5. Denetim Çalışma Programı Örneği

ÇALIŞMA PROGRAMI					
Tarih:					
Denetlenen Birim	Denetim Alanı	Denetim Türü	Risk Derecesi	Denetçi	Denetim Süresi
Denetim Alanı Detay Analizi					
Süreç	Alt Süreç	Riskler	Risk Derecesi	Riskin Tanımı	
Denetim Dışı Bırakılan Alanlar					
Süreç	Alt Süreç	Risk Derecesi			
Hazırlayan			Göden Geçiren		
[Tarih]	[Paragraf]	[Tarih]	[Paragraf]		

Kaynak: Göğüş, 2012, s.62

2.5.5.2. Kontrol Testlerinin Uygulanması

Kontrol testlerinin uygulanma sürecini tespit edici, önleyici ve düzeltici olarak üç aşamada incelemek mümkündür.

Tespit edici kontroller, işletme faaliyetleri sürecinde meydana gelebilecek hataların ortaya çıkarılmasına yönelik uygulanan kontrollerdir. Tespit edici kontrollere ilişkin testlerin uygulanmasında elde edilen kanıt ve kanıt miktarları için değerlendirme yapılır. İşletmede kontrol süreçlerinin etkin olarak uygulanıp uygulanmadığı yüksek güven derecesinde test edilir. Örnek olarak gün sonunda gelir kaydedilen işlemlere ait alınan vergilerin kontrolü verilebilir.

Düzeltilici kontroller, tespit edici kontrol sonrasında meydana gelen aksaklıkların düzeltilmesine yönelik uygulanan kontrollerdir. Örnek olarak disk hatası nedeni ile bozulan veya erişilemeyen verilerin arşivden sisteme geri yüklenmesi işlemi verilebilir.

Önleyici kontroller, işletme faaliyetleri iş akışı sırasında yapılan her işlem için meydana gelebilecek hataların önlenmesi için kullanılan kontrollerdir. Uygulanan kontrollerin etkin olup olmadığının test edilebilmesi için iç denetim sürecinde yeterli güvenilir kanıtların toplanması gereklidir. Önleyici kontrole ilişkin hata bulunmaması kontrol sürecinin etkin uygulandığını göstermez. İşletmede önleyici kontrollerin var olmasına rağmen, uygulanıp uygulanmadığı nasıl ve kim tarafından uygulandığına dair fiziki kanıtlar elde edilemeyebilir. Ya da bazı durumlarda kanıt elde edilse de etkin bir kontrol sisteminin varlığından söz edilemeyebilir. Kısacası, işletmede istenmeyen olayları gerçekleşmeden önce önlemeyi ve caydırmayı amaçlar. Örnek olarak sistem yetkilendirmeleri ile görev ve sorumlulukların dağılımı verilebilir. (Göğüş, 2012, s.62-63)

Denetçiler denetim çalışmalarını yürütürken kanıt toplayabilmek için çeşitli araç ve yöntemlerden yararlanırlar. Bu araç ve yöntemlere denetim teknikleri adı verilir. Gözlem, analitik inceleme, görüşme izleme, doğrulama, ana kütle, işlem ve uygunluk testleri uygulanan başlıca kontrol test yöntemleridir. İşletmede denetlenen birimin risk seviyesine, önem seviyesine ve diğer ilgili faktörlere göre test seviyeleri belirlenir. Uygulanan test yöntemi sorumlu iç denetçi ve İç Denetim Yöneticisi tarafından belirlenerek gözden geçirme şeklinde olabileceği gibi kapsamlı bir denetim faaliyeti de olabilir. Aşağıda uygulanabilecek test yöntemleri açıklanmıştır. (Göğüş, 2012, s.58-63)

- **Fiziki İnceleme:** İşletmedeki belge ve kayıtlarda gösterilen işletme fiziki varlıklarının gerçekten var olduklarını ve işletmeye ait olduğunun belge ve kayıtlarla doğrulanmasıdır. Bu yöntemle işletme varlıklarının kalitesi de ölçülebilmektedir.

- **Doğrulama:** İşletme dışındaki bağımsız kişilerden işletme ile ilgili yazılı bilgi alınır. Bilgi bağımsız kaynaktan geldiği için güvenilir bir kayıt niteliğindedir. Olumlu, olumsuz ve boş bakiyeli olarak üç çeşit teknik vardır. **Olumlu doğrulama**, işletme dışındaki üçüncü kişilerden gelen bilgi veya kayıtların aynı ya da farklı olup olmadığına dair yanıt beklenir. **Olumsuz doğrulama**, işletme dışındaki üçüncü kişilerden sadece bilgi ya da kayıtların sadece yanlış olması durumunda cevap vermesi beklenir. **Boş bakiyeli doğrulama**, doğrulama mektubunda doğru olup olmadığı sorgulanan bilgi ile ilgili bir şey paylaşmadan üçüncü kişiden kendi kayıtlarında görünen bilginin paylaşılması istenir.
- **Belge İnceleme:** Muhasebe kayıtlarının doğruluğuna dair kanıt aranır. Atılan muhasebe kaydının dayandığı belgeler incelenerek karşılaştırmalar yapılır. Bu teknikte, işletmede bulunan bütün belgeler incelenemeyeceği için örnekleme yoluyla inceleme tercih edilir.
- **Kayıt Sürecinin İncelenmesi:** Belge inceleme tekniğindeki örnekleme yoluyla kaynak belgeler seçilerek kayıtların her aşamasının incelendiği denetim teknik türüdür. İleriye doğru ve geriye doğru inceleme olarak iki ayrı aşamada uygulanır. İleriye doğru incelemede, incelenen belgeden başlayarak tüm kayıtlar kontrol edilip mali tablolara doğru uzanan bir süreçtir. İşletmede kayıt düzeni ya da eksikliği ile ilgili bir durum varsa başvuru bir yöntemdir. Geriye doğru inceleme sürecinde ise mali tablolardan incelenecek belgeye doğru bir yol izlenir.
- **Yeniden Hesaplama:** Muhasebe sisteminde yer alan işlemlerin doğruluğunu test etmek için gerekli görüldüğü durumlarda yeniden hesaplama tekniği uygulanır. Örneğin, faiz, reeskont ve amortisman hesaplarında tercih edilen bir denetim tekniğidir.
- **Gözlem:** İşletme faaliyetlerinin kim tarafından nasıl ve ne zaman yapıldığını anlamak için kullanılan izleme tekniğidir.

- **Derinlemesine Araştırma:** Tecrübeli denetçiler tarafından gerçekleştirilir. İşletmede atılan bir kayıt, bir hesap veya finansal tablonun ayrıntılı bir biçimde incelenmesidir.
- **Soruşturma:** İşletmede yapılan bir işlemin kim tarafından nasıl yapıldığına dair birçok konuda çalışan personele soru sorulması tekniğidir. Cevaplar yazılı ya da sözlü olabilir, ama kanıt olması açısından yazılı cevap alma yöntemi tercih edilir.
- **İlgili Hesaplar Arasında İlişki Kurma:** Alacaklar, şüpheli alacaklar, şüpheli alacaklar karşılığı gibi muhasebe hesapları arasında bazı ilişkiler bulunmaktadır. Bu nedenle denetçi bu hesapları karşılaştırmak nedeniyle hesapların doğruluğunu araştırma yolunu seçebilir.
- **Analitik İnceleme:** İşletmede periyodik olarak hazırlanan raporlar ve sonuçlarının finansal ve finansal olmayan çeşitli veriler dikkate alınarak işletmenin hedeflerine uygun olup olmadığı belirlenir.

2.5.5.3. Test Sonuçlarının Yorumlanması

Uygulanan testler sonucunda iç denetçi işletmenin kontrol sistemini yeterlilik, etkinlik ve verimlilik açısından değerlendirir. Etkin bir kontrol olabilmesi için kontrol sisteminin işleyiş sürecinde herhangi bir eksikliğin tespit edilmemiş olması gerekir ya da eksiklik tespit edilmişse de kontrol eksikliğine neden olmaması gerekir. Bu durum bilgi teknolojisi sistemleri ile işletme süreçleri kontroller açısından değerlendirilmelidir. Bu durumda test sonucu raporlanırken “*kontrol var ve test edildi*” ibaresi kullanılır. Kontrol süreçlerinin var olduğu ama etkinliğinin ölçülemediği durumlarda ise raporda “*kontrol var ama test edilmedi*” ibaresi kullanılır. Bu durumda kontrol sürecinin test edildiği sonucuna ulaşmak için izleme yönteminin birden fazla örnek üzerinde uygulanmış olması gerekir. Etkinliğin ve yeterliliğin söz konusu olmadığı durumlarda önemli kontrol eksikliği, kayda değer kontrol eksikliği ve kontrol zayıflığı gibi durumlardan bahsedilir. Örneğin, denetimi

yapılan işletmenin mali verilerin güvenilirliğinin, tutarlılığının ve bütünlüğünün, gizliliğinin sağlanmasında ve işletme faaliyetlerinin sürekliliğini olumsuz etkileyebilecek olaylar “kontrol zayıflığı” ve birden fazla kontrol zayıflığının bir araya gelmesi sonucunda oluşan durumlar “kayda değer kontrol eksikliği” olarak raporda tanımlanır. Mali verilerin genel kabul görmüş muhasebe standartlarına uygun olarak güvenilir bir şekilde kayıt altına alınması, işlenmesi ve raporlanması aşamalarında meydana gelen hataların önlenmesine olumsuz etki eden eksiklikler de bu kapsamda değerlendirilir. Bir önceki örnekteki gibi finansal süreçlerde meydana gelen olumsuz etki yaratan durum veya durumlar “önemli kontrol eksikliği” ibaresi ile raporlanır. Kontrollerin var olmadığının belirlenmesi durumunda “kontrol yok” olarak raporda belirtilir. Özetle uygulanan testler, işletmede tanımlanmış olan risklere karşı uygulanması gereken kontrol süreçlerinin eksiksiz ve yeterli olarak uygulanıp uygulanmadığını ortaya çıkarır. Testlerin doğruluğu işletmedeki iç denetim etkinliği ile ilgili bilgi edinmemize yardımcı olur. (Göğüş, 2012, s.64-65)

2.5.5.4. Bulguların Tespit Edilmesi ve Öneri Sunulması

Uygulanan testler sonucunda elde edilen bulgular iç denetçi tarafından yeterli kanıtlarla destekleyecek şekilde değerlendirmeler yapar ve işletmenin katma değerini arttıracak tavsiyeler geliştirir. İç denetçi, denetim süreci boyunca tespit ettiği bilgileri önem derecesine göre sınıflandırır ve bulgu formunda belirtir. Bulgu formu aşağıdaki bilgileri içerir. (Adiloğlu, 2011, s.82-83)

- Tespit bölümünde “yanlış veya sapma nedir” sorusuna cevap verir.
- Neden bölümünde yanlış veya sapmanın nedeni nedir sorusuna cevap verir.
- Riskler ve etkileri bölümünde, işletmenin yanlış veya sapma sonucunda maruz kaldığı riskleri ve bu risklerin olası risklerini yansıtır.

- Kriterler bölümünde, standart, mevzuat ve uygulamalar çerçevesinde olması gerekenleri belirtir.
- Öneriler bölümünde ise, işletmenin olması gereken duruma gelebilmesi için nasıl ulaşacağını yollarını söyler.

Denetim çalışmasının sonunda denetim ekibi bulguları birleştirir. Denetim süreci boyunca iç denetim ekibinin bildirimlerine gönderilen yanıtlar dikkate alınarak elde edilen bulgular işletmenin bütünü için doğru kanaatlere dönüşmesi çok önemlidir. Yetersiz ve zayıflık bulgularının yanında olumlu işleyişlerde motive etmek için bildirilmelidir. Zayıflık ve yetersizliğin giderilmesine yönelik yapıcı ve uygulanabilir öneriler geliştirilmelidir. (Demirbaş, 2005, s.181)

2.5.5.5. Kapanış Toplantısı

Kapanış toplantısı denetim raporu sunulmadan etkinlik, verimlilik ve kontroller ile ilgili geliştirici öneri ve tavsiyelerde bulunmadan önce orta ve üst düzey yöneticiler ile iç denetim ekibi ile gerçekleştirilmelidir. İç denetçi ile yönetim arasında bilgi alışverişi yapılarak fikir birliğine varılır. (Türedi, Zor ve Gürbüz, 2015, s.16)

İç denetçi kapanış toplantısında görüşülmesi için elde etmiş olduğu bulguları bir yazı ekini denetlenen birim ile paylaşır. Dolayısıyla, denetlenen birim ile iç denetçi kapanış toplantısında elde edilen bulgular ve geliştirilen öneriler üzerine görüşerek bir karara varırlar. Varılan karar bir tutanağa bağlanır. (Adiloğlu, 2011, s.84)

2.5.6. Raporlama

IIA 2060 Üst Yönetim ve Yönetim Kuruluna Raporlamalar başlıklı standardına göre, İç Denetim Yöneticisi iç denetimin amacı, iç denetçinin görev ve sorumlulukları, yetkileri ve oluşturulan iç denetim plan ve programının performansına yönelik standartlar ve etik kurallar ile uyumu konusunda üst yönetim ve Yönetim Kuruluna dönemsel raporlar sunmaktadır. Raporlamanın içeriği ve sıklığı İç Denetim Yöneticisi, üst yönetim ve kurul ile birlikte belirlenir ve iletilen bilginin önemi ve alınacak tedbirlerin aciliyetine bağlıdır. Yönetim Kurulu ve üst yönetime sunulan raporun içeriği, denetim yönetmeliği, kaynak gereksinimleri, iç denetimin bağımsızlığı, denetim planı ve plan ile karşılaştırmalı ilerleme, denetim faaliyetlerinin sonuçları, standart ve etik kurullara uyum ve uyum ile ilgili önemli konulara ait aksiyon planları ve İç Denetim Yöneticisi tarafından işletme için kabul edilemez olarak değerlendirilebilecek riske karşı üst yönetimin yanıtı bilgilerini içermelidir. (TİDE, Uluslararası İç Denetim Standartları, 2017, s.14)

Etkin bir iç denetim raporu daha önce yapılmış inceleme, gözden geçirme ve değerlendirme aşamalarının kalitesine bağlıdır. Çünkü raporlama, bahsi geçen aşamalardan geçmiş bilgiler sonucunda düzenlenecektir. Bu yüzden, eğer raporlama yetersiz veya zayıf olursa yapılan iyi bir denetim çalışması tüm değerini yitirebilir. İyi yapılmış bir iç denetim raporu, uygulanan iç denetim faaliyetinin yansıtan güçlü bir araçtır. Bu nedenle iç denetim raporunun üç temel amacı vardır (Adiloğlu, 2011, s.84-85)

- **Bilgilendirme:** Bulguların açıklanması
- **İkna:** Bulguların geçerli ve etkin olduğunun inandırıcılığı
- **Sonuçlar Elde Etme:** Üst yönetimi işletmeyi iyileştirmek ve değiştirmek için yönlendirmek

İç denetim raporunun hazırlanma süreci taslak iç denetim raporu ve kesinleşmiş iç denetim raporu olmak üzere iki aşamada gerçekleştirilir.

Taslak iç denetim raporunun hazırlanması aşamasında, iç denetçi denetim süreci boyunca elde etmiş olduğu bulgular ile kapanış toplantısında yapılan görüşmeleri de dikkate alarak bir taslak rapor hazırlar. Taslak iç denetim raporunu belirli bir süre içerisinde denetlenen bölüm tarafından cevaplandırılmak üzere bir yazı ekinde iletir. İlgili birim yöneticisi gerektiğinde çalışanlarından veya ilgili kişilerden görüş alır ve raporu istenilen süre içerisinde cevaplandırarak iç denetçiye gönderir. (Adiloğlu, 2011, s.85-86) Taslak raporda yer alan bulgu, sonuç ve önerilerin değerlendirilmesi için iç denetim ekibi tarafından üst yönetime makul bir süre içerisinde gönderilir. Rapor üzerinde yapılacak tartışmaların hangi tarih ve saatlerde, nerede yapılacağı ve toplantıya kimlerin katılacağı gibi durumlar işletmenin üst yönetimi ile önceden planlanır. Yapılacak toplantıda bulgu, sonuç ve önerilere üst yönetim ile tartışılarak netleştirilir. Taslak iç denetim raporunun üst yönetim ile görüşülmesi, elde edilen bulguların doğrulanması niteliğini taşır. Taslak iç denetim raporundan sonra üst yönetim ile görüşülmesi; elde edilen bulguların doğruluğundan emin olma, iç denetim sürecindeki hatalı bilgi ve değerlendirmeleri son defa düzeltme imkanı verme açısından, üst yönetimin açıklamalarını dikkate alma, iç denetim raporu içeriğinin tutarlı olup olmadığını anlayabilmek ve iç denetim ekibinin üst yönetime sunulan önerilerin gerçekçi ve uygulanabilir nitelikte olmasına katkıda bulunma gibi faydalar sağlar. (Demirbaş, 2015, s.181)

Kesinleşmiş iç denetim raporunun hazırlanması ve sunum aşamasında, iç denetçi denetlenen birim yöneticisinden alınan cevaplar ve cevaplara ilişkin değerlendirmelerini de içeren kesinleşmiş iç denetim raporunu iç denetim birimi aracılığı ile üst yönetime sunar. İç denetim yöneticisi raporun ilgili kişilere iletilmesinden sorumludur. (Adiloğlu, 2011, s.85-86)

IIA 2400 Sonuçların Raporlanması başlıklı standardına göre, iç denetçiler denetim sonuçlarını raporlamak zorundadır. Sonuçların işletme dışındaki kişilere dağıtılması ve bu kişiler tarafından kullanılması durumlarındaki sınırlamalar da raporun içeriğinde yer almak zorundadır. İç denetim yöneticisi kesinleşmiş iç

denetim raporunun sunumundan önce gözden geçirilmesinden, onaylanmasından, kime ve nasıl dağıtılacağı konusunda sorumludur. İç denetçi raporda görüş bildirirken işletme hedefleri, stratejileri, riskleri ve üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerini dikkate almak zorundadır. Denetçi görüşünün güvenilir, yeterli, ilgili ve yararlı bilgi ile desteklemesi gerekir. Dolayısıyla raporlama *objektif, doğru, açık, yapıcı, özlü, tam olmalı ve zamanında sunulmalıdır*. Nihai iç denetim raporunun sahip olması gereken kıstaslar aşağıda açıklanmıştır. (TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.20-21)

- **Objektif raporlama**, tarafsız, ön yargısız, adil ve ilgili bütün gerçeklerin ve şartların dengeli bir şekilde değerlendirilmesinin sonucudur.
- **Doğru raporlama**, hata ve çarpıtmalardan uzak ve dayandırıldığı gerçekliklere sadıktır.
- **Açık raporlama**, mantıklı ve kolay anlaşılabilir. Gereksiz teknik terimler kullanılmasından kaçınılarak önemli ve ilgili bütün bilginin net olarak verilmesini sağlar.
- **Yapıcı raporlama**, işletmede gerekli olan faaliyet alanlarının iyileştirilmesi konusunda denetim faaliyetinin işletmeye denetlenen kişilere yardımcı olmasıdır.
- **Özlü raporlama**, konuyu gereksiz ayrıntılardan ve tekrarlardan kaçınarak doğrudan anlatan raporlardır.
- **Tam raporlama**, hedef kitleye bütün ilgili ve önemli bilginin, tavsiye ve sonuçları destekleyen gözlemlerin eksiksiz bir şekilde iletilmesidir.
- **Zamanında raporlama**, işletmede oluşabilecek sorunlara karşı üst yönetimin alınabilecek düzeltici önlemleri almasını sağlayan yararlı ve tam zamanında yapılan raporlamalardır.

Nihai rapor denetimin hedeflerini, kapsamını ve sonuçlarını içermek zorundadır. (TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.20) Aşağıdaki

kesinleşmiş iç denetim raporunun içermesi gereken bölümler açılanmıştır. (Adiloğlu, 2011, s.88-90)

- 1. Raporlama Tarihi:** Raporda denetim çalışmasının bitirildiği tarihin yazılması gerekir.
- 2. Gönderilen Kişi:** Rapor genellikle üst yönetime gönderilir. Ancak bazı durumlarda rapor gözden geçirilmesi için denetimden sorumlu olan yöneticiye de gönderilebilir. Bu nedenle, rapor doğrudan ilgili olan kişilere gönderilmelidir. Gönderilecek kişiler arasında iç denetimin raporlandığı üst yönetim, rapora cevap vermesi gereken kişi veya kişiler, raporu gözden geçirme sürecinden sorumlu olan kişiler ve düzeltici kontrolleri yapan kişiler sayılabilir.
- 3. Giriş Paragrafı:** Yapılan denetim süreci ile ilgili hangi birim birimlerin denetlendiği, denetimin düzeli mi yoksa özel bir sebeple inceleme mi yapıldığına dair genel bilgiler verilir.
- 4. Amaç Paragrafı:** İç denetimin hedefleri “Amaçlar” başlığı altında açıklanmalıdır. Bu kısımda iç denetimin neden yapıldığı ve beklentilerin neler olduğu konusunda bilgi verilir.
- 5. Kapsam Bölümü:** İşletmede denetlenen faaliyetler ile ilgili alanlar ve zaman dilimi gibi bilgiler “Kapsam” başlığı altında belirtilmelidir. Gerekirse iç denetimin sınırlarını açıkça belirtmek için denetim sürecine dahil olmayan faaliyetler de belirtilmelidir. İç denetimin konusu, niteliği ve kapsamı bu bölümde tanımlanmalıdır.
- 6. Tespit ve Öneriler:** Tespit, elde edilen bulgular ile ilgili açıklamalardır. İç denetçinin ulaştığı sonuçları ve önerilerini desteklemek ve yanlış anlaşılmasını önlemek için nihai raporda gerekli görülen tespitlere yer verilmelidir. Elde edilen tespitler “olanlar” ve “olması gerekenler” ile karşılaştırıldığında ortaya çıkar. Bu tespitler raporunun temelini oluşturur. Tespit ve öneriler aşağıdaki özelliklere dayandırılmalıdır:

- **Kıstas:** Bir Őeye iliŐkin deęerlendirme ya da doęrulama yapmak iin kullanılan ller, standartlar ve beklentilerdir.
- **Tespit:** İ denetinin denetim srecinde elde ettięi bulgu ve belgelerdir.
- **Sebep:** Mevcut koŐullar ile beklenen koŐullar arasındaki tespit edilen farklılıklara ait sebeplerdir.
- **Etki:** Tespitlerin belirlenen kriterlere uygun olmadığı durumda maruz kalınan risk derecesidir. İ deneti bu risk ve maruz kalma derecesinin belirlenmesinde yaptıęı gzlem ve tavsiyeler neticesinde iŐletmenin finansal tabloları zerindeki etkisini dŐnmelidir.

7. Sonu ve GrŐler: İ denetinin denetim sreci ile ilgili tespit ve tavsiyelerinin yol aabileceęi durumların deęerlendirilmesinin yasılmasıdır. Bu kısımda tespit ve tavsiyeler oluŐabilecek genel etkiler gz nne alınarak yansıtılır. Sonular, iŐletmenin ama ve hedeflerine uygun olup olmadığı ve bunlara ulaŐıp ulaŐmadıęını ve iŐletme faaliyetlerinin amacına uygun alıŐıp alıŐmadıęını kapsayabilir. İ deneti ama ve hedeflere ulaŐmak iin i kontrollerin yetersizlięi ve eksiklięinden kaynaklı bir nedene ulaŐırsa iŐletmeye i kontrol ile ilgili tavsiyelerde bulunabilir. st ynetimde bu tavsiyelere iliŐkin dzeltici nlemler alma alıŐmalarını baŐlatabilir.

Btn bu raporların verilme sebebi iŐletmedeki dzensizlik, hata ve hile gibi riskleri ortadan kaldırmak iin daha iyi bir i kontrol yntemleri belirleyerek bu kontrollerin sreklilięini saęlamak, iŐletmedeki maliyetleri azaltıp karı artırarak iŐletme baŐarisını arttırmaktır. (Adiloęlu, 2011, s.90)

BaŐarılı bir i denetim raporu aŐaęıdaki zellikleri iermelidir. (DemirbaŐ, 2005, s.180)

- Elde edilen bulgular yeterli denetim kanıtlarıyla desteklenmelidir.

- Raporda yeterli olan bilgiler yer almalı ve gereksiz ayrıntılardan kaçınılmalıdır.
- Tarafsızlık ilkesine bağlı kalındığının göstergesi olarak olumlu ve olumsuz durumlar ön yargısız ifadelerle raporda sunulmalıdır ve uygulama örnekleri verilmelidir.
- Raporda verilen öneriler uygulanabilirlik, meydana gelen veya gelebilecek sorunların aşılması ve bu alacağı zaman konusunda gerçekçi olunmalıdır.
- Rapor kısa ve öz olmalıdır. Sade ve anlaşılır bir dil kullanılmalıdır. Gerekli durumlarda sayısal ve grafiksel verilerle desteklenmelidir. Teknik ve anlaşılması zor kelimeler kullanılmaktan kaçınılmalı ve kullanılıyor ise ne anlama geldiği açıklanmalıdır.

2.5.7. İzleme

IIA 2500 İlerlemenin Gözlenmesi başlıklı standardına göre, İç Denetim Yöneticisi rapor edilen sonuçlarına göre üst yönetimin aldığı tedbirler ve riski kabul ettiğinden emin olmak için işletmedeki gelişmeleri gözlemek amacıyla takip sistemi kurmak zorundadır. (TİDE, IIA Uluslararası İç Denetim Standartları, s.23)

Daha detaylı anlatmak gerekirse Adiloğlu'na göre iç denetim raporu, farkına varılmayı yaratmak amacıyla bilgilendirme, kabul edilmeyi sağlamak amacıyla ikna etme, harekete sevk etmek amacıyla sonuçlar elde etme hedeflerine yönelmelidir. Denetçi, iç denetim raporunda işletme için düzeltici işlemler önerebilir ve tavsiyelerde bulunabilir. İlgili birim tarafından ilgili öneri ve tavsiyelerin yerine getirilmesi beklenir. Eğer bu işlemler zaman alan bir durum ise iç denetçiye gönderilen cevapta bildirilir ve gözlenen gelişmelerde iç denetçiye iletilir. Bu yüzden iç denetçi sonuçların işletme tarafından değerlendirmeye alınıp alınmadığını anlamak için bir sistem kurmalı ve uygulamalıdır. (Adiloğlu, 2011, s.92)

Tablo 2.6. Bulgu Takip Planı

Madde No	Risk Derecesi ve Kategorisi	Bulgu	Öneri	İlgili Birim	Birim Görüşü	Tamamlanma Tarihi	Tamamlanma Durumu

Kaynak: Göğüş, 2012, s.62

2.6. Risk Odaklı İç Denetimin Sağladığı Faydalar

Risk odaklı iç denetimin işletmelere sağlayacağı birçok yararı bulunmaktadır. Bunlardan bazılarını aşağıdaki gibi sıralayabiliriz. (Tanç, 2009, s. 151-152):

- Risk odaklı iç denetim, işletmenin sınırlı iç denetim kaynakları ile önemli tehdit oluşturan risklerin değerlendirilmesi ve yönetilmesi açısından köprü görevi görür.
- İşletmede etkin bir risk yönetimi mevcut değilse, risk odaklı iç denetim açıkça uyarılarda bulunur.
- Risk odaklı iç denetim, işletmede kaynakların gereksiz yere kullanılan kontrol risklerini tespit eder.
- Risk odaklı iç denetim, işletmedeki iç denetim faaliyetinin ne kadar kaynak ihtiyacı olduğunu belirlenmesinde güvence sağlar.
- Risk odaklı iç denetim, işletmedeki bütün risk yönetimi süreçleri üzerinde güvence verir.
- Risk odaklı iç denetimin en etkili risk güvence yöntemlerinden biri olduğunu birçok kurum ve kuruluş tarafından kabul edilmektedir.
- Risk odaklı iç denetim, işletmenin riskleri daha iyi bir şekilde göğüsleyerek ve işletme yönetiminin risk yönetimi süreçlerindeki görev ve sorumluklarını destekleyerek işletmenin daha sağlam bir yapıya kavuşmasına yardımcı olur.

Risk odaklı iç denetim felsefesinde işletme yönetimine; iç denetim faaliyetleri ile ilgilenmesi, işletmede içerisindeki riskleri tanınması, iç denetim amaçlarını formüle etmesi ve kontrol etmesi, iç denetim personel donanımını kontrol etmesi, denetim süreci boyunca iç denetçilere gereken desteęi saęlaması ve faaliyet sonuçlarını içeren iç denetim raporlarını anlaması gibi görevleri yüklemektedir. (Demirbaş, 2005, s.186)



ÜÇÜNCÜ BÖLÜM

3. RİSK ODAKLI İÇ DENETİM VE TÜRKİYE'DEKİ İŞLETMELER ÜZERİNDE BİR UYGULAMA

3.1. Literatür Taraması

Literatürde risk odaklı iç denetim ile ilgili birçok çalışma yapılmış yapılan çalışmalar tarih sırasına göre aşağıda belirtilmiştir.

Beste Akyürek (2006): “*Bankacılık sektöründe risk odaklı iç denetim sistemi*” adlı çalışmasında bankacılık sektöründeki risk odaklı iç denetim yapısını incelemiştir. Bankacılık sektöründe risk odaklı iç denetimin faydasını sektörü düzenleyici yasa, yönetmelik, diğer kural koyucuların iç denetim sisteminin çalışmasına imkan verecek hale getirilmesi ve bankalar kurumsal risk anlayışının uygulanmasıyla olacağı görüşünü belirtmiştir. Dünya ekonomisinde büyük kayıplara yol açan birçok finansal bunalımların ortak nedenlerinden birinin geleneksel iç denetim modelinin yetersizliği olduğunu ve Basel II ile genel çerçevesi çizilmiş olan risk odaklı iç denetim sisteminin geleneksel iç denetim yapısındaki eksiklikleri gidereceği sonucuna ulaşmıştır.

Niyazi Kurnaz (2007): “*Kurumsal yönetim ekseninde risk odaklı iç denetim adlı çalışmasında Türkiye'nin 500 büyük sanayi işletmesinde risk odaklı iç denetim uygulama analizi*” adlı çalışmasında İstanbul Sanayi Odası'nın 2004 yılı 500 büyük sanayi işletmesi sıralamasına girmiş işletmelerin iç denetim sistemleri hakkında bilgi sahibi olmak için amacıyla anket çalışması yapmıştır. Araştırma sonucunda risk odaklı iç denetimin hem iç hem de dış denetçiler tarafından yaygın olarak kabul edilmesine rağmen üst yönetim tarafından benimsenmediği görüşüne ulaşmıştır. Ancak denetçilerin ve işletme yöneticilerinin risk odaklı iç denetimin kaçınılmaz olabileceği görüşünü savundukları görüşüne ulaşmıştır.

Aptullah Özer (2008): “*Risk odaklı iç denetim ve bir uygulama*” adlı çalışmasında iç denetimde risk değerlendirmesi ve risk odaklı iç denetim uygulamalarının ne ölçüde kullanıldığını belirlemek ve Türkiye’deki iç denetim profilini ortaya koymayı amaçlamıştır. İç denetim, iç kontrol, risk ve risk yönetimi kavramları ile geleneksel iç denetim ve risk odaklı iç denetim karşılaştırılarak risk odaklı iç denetimin önemi vurgulanmıştır.

Ahmet Tanç (2009): “*Risk odaklı iç denetim yaklaşımı ve tekstil sektöründe bilgisayar destekli bir uygulama*” adlı çalışmasında risk odaklı iç denetim konusunda işletmelere pratik çözümler sunan bilgisayar yazılımı sayesinde hammadde kabul ve depolama sürecine ilişkin örnek risk odaklı iç denetim uygulamasıyla yazılım sisteminin işletmeye sağladığı faydaları ortaya koymuştur.

Ömer Görener (2010): “*Risk odaklı iç denetim: olasılık etki analizi çerçevesinde bir uygulama*” adlı çalışmasında risk odaklı iç denetim süreci hakkında bilgiler vererek kurgulanmış bir işletmenin pazarlama biriminde risk odaklı iç denetimin nasıl olması gerektiği ile ilgili uygulama örneği vermiştir.

Ertuğrul Bertan Kaya (2010): “*Risk odaklı iç denetim ve uygulaması*” adlı çalışmasında beş yıldızlı bir otel işletmesinde risk odaklı iç denetimin hissedarların haklarının korunması, maliyetlerin azaltılması ve kurumsal yönetimin desteklenmesi amaçlarına yönelik işlevselliğini değerlendirmiştir.

Gültaç Akkaya (2011): “*Risk odaklı iç denetim ve risk odaklı iç denetim planlamasında risk matrisinin oluşturulmasına yönelik örnek bir uygulama*” adlı çalışmasında hizmet sektöründe faaliyet gösteren bir otelin mali işler biriminde iç odaklı iç denetim planlamasında risk matrisi oluşturulması süreci anlatmış, vergi muhasebesi ve tahsilat yönetimi konularının yüksek risk seviyesine sahip olduğunu, raporlama ve nakit yönetimi konularının ise en düşük risk seviyesine sahip olduğunu tespit etmiştir.

Özlem Doğan (2011): “*KOBİ’lerde iç kontrol sisteminin yeri ve risk odaklı iç denetim: Denizli ili uygulaması*” adlı çalışmasında KOBİ’lerdeki iç denetim ve iç kontrol sistemi ile ilgili yöneticilerin görüşlerini ortaya koymayı amaçlamıştır. Denizli Organize Sanayi Bölgesi’nde faaliyet gösteren işletmelerle görüşmesi sonucunda etkili bir iç kontrol sisteminin olmadığı, iç kontrolün gerekli bir sistem olarak görülmediği, iç denetim ekiplerinin bulunmadığı ve eğitimli kişilerin sayısının az olduğu görüşüne ulaşmıştır.

Fahrettin Yahşi (2014): “*Katılım Bankalarında risk odaklı iç denetim ve bir model önerisi*” adlı çalışmasında Türkiye’de ve Dünya’da katılım bankacılığının gelişimi, bankalarda meydana gelebilecek risk ve risklerin yönetilmesi, risk odaklı iç denetim incelenerek katılım bankalarında risk odaklı iç denetim anlayışının benimsenerek iç denetim faaliyetinin sürdürülmesi için bir model önerisinde bulunulmuştur.

Zafer Anadolu (2015): “*Yeni Türk Ticaret Kanunu kapsamında risk odaklı iç denetim etkisi ve meslek mensupları üzerine bir anket çalışması*” adlı çalışmada işletmelerin operasyonel riskleri ile risk odaklı iç denetim arasındaki ilişkiyi ölçmek için melek mensupları ile anket çalışması yapılmıştır.

Aysun Atagan Çetin (2016): “*Kurumsal sürdürülebilirliğin sağlanmasında risk odaklı iç denetim ve bir araştırma*” adlı çalışmada risk odaklı iç denetimin kurumsal sürdürülebilirliğin sağlanmasındaki rolünü açıklamak amacıyla Türkiye’deki işletmelerin iç denetçileri ile görüşülerek anket çalışması yapılmıştır. Risk odaklı iç denetimin süreç boyutu ile ele alınmasında çevresel ve sosyal sürdürülebilirlik arasında anlamlı ve pozitif ilişki, fayda boyutu ile ele alındığında sosyal ve ekonomik sürdürülebilirlik arasında anlamlı ve pozitif ilişki tespit edilirken çevresel sürdürülebilirlik arasında anlamlı ve negatif ilişki olduğu saptanmıştır. Süreç ile ekonomik sürdürülebilirlik arasında anlamlı bir ilişki olmadığı tespit edilmiştir.

Ersin Kurnaz (2016): “*Risk odaklı iç denetim yaklaşımı: Türkiye’de kamu sektöründeki iç denetçilere yönelik bir araştırma*” adlı çalışmada Türkiye’deki kamu kurumlarında risk odaklı iç denetim uygulamasının hangi düzeyde olduğunu belirlemek amacıyla kamu iç denetçileri ile anket çalışması yapılmıştır. Araştırmanın sonucunda iç kontrol sisteminin etkin olmaması, risk tespiti ve değerlendirmesi konusunda eksikliklerin olduğu ve üst yönetimin tutumuna bağlı olarak risk odaklı iç denetimin uygulanma seviyesinin düşük olduğu tespit edilmiştir.

Büşra Kevser Saruhan (21017): “*Risk odaklı iç denetim ve bir bankanın denetim planlaması ve risk matrisinin oluşturulması*” adlı çalışmada risk odaklı iç denetim yapısı, gelişimi, faydaları, bankalardaki iç denetim yapıları incelenerek şubelerde risk odaklı iç denetim anlayışının benimsenerek denetim faaliyetinin sürdürülmesinde yol gösterici bir model önerisi sunulmuştur.

Maşuk Cahit Uysal (2017): “*Kamu kurumlarında kurumsal risk yönetimi ve risk odaklı iç denetim ve bir model önerisi*” adlı çalışmada kamu iç denetçilerinin kurumsal risk yönetimi ve risk odaklı iç denetim konularındaki farkındalıkları tespit edilmiş ve Türkiye Tarım Kredi Kooperatiflerinde risk odaklı iç denetim sürecinin nasıl olması gerektiğine yönelik model önerisinde bulunulmuştur.

Gül Yılmaz (2018): “*Otel işletmelerinde risk odaklı iç denetim ve bir uygulama*” adlı çalışmada otel işletmelerinde risk odaklı iç denetim profilinin belirlenmesi amacıyla Konya ve Antalya merkezindeki dört ve beş yıldızlı otel işletmelerine yönelik anket çalışması yapılmıştır. Araştırma sonucunda otel işletmelerinde iç kontrol ve iç denetim yapısının etkin olduğu görüşüne ulaşılmıştır.

Mehmet Yaşar (2019): “*Yatırım ve kalkınma bankalarında risk odaklı iç denetime yönelik uygulama önerisi*” adlı çalışmada Türkiye’deki yatırım ve kalkınma bankası örnek senaryo üzerinden risk tespiti, değerlendirmesi ve risk matrisi oluşturulması açısından uygulamada bulunarak benzer çalışmalara yol gösterici olması hedeflenmiştir.

Ruhi Yelken (2019): “*Holdinglelerde risk odaklı iç denetim ve bir uygulama*” adlı çalışmada iç denetim yapısı ve işleyişini incelemek ve karşılaştırmak amacıyla 20 holdingin üst yöneticileri ve denetim çalışanları ile anket çalışması yapılmış, risk yönetim sürecinin etkin bir şekilde uygulanıp uygulanmadığının tespit edilmesi amaçlanmıştır.

Umut Can Bektaş (2019): “*Uluslararası iç denetim standartları çerçevesinde risk odaklı iç denetim ve uygulamaya yönelik bir araştırma*” adlı çalışmada iç denetim yaklaşımları ve işleyişine uluslararası standartlar çerçevesinde görüş ölçeği ve yeterlilik ölçeği bağlamında farklı değişkenlere göre iç denetim mekanizmalarının incelenmesi ana konudur.

Melek Damla Mandalas (2019): “*Kurumsal risk yönetimi kapsamında risk odaklı iç denetim analizi; Marmara bölgesindeki devlet üniversitelerine yönelik bir araştırma*” adlı çalışmada kurumsal risk yönetiminin benimsenmesiyle risk odaklı iç denetimin etkinliğini tespit etmek için Marmara Bölgesi devlet üniversitelerindeki iç denetçiler ile anket çalışması yapılmıştır.

Eda İlkün (2019): “*Risk odaklı iç denetim kalitesini etkileyen faktörlerin kamu sektöründe incelenmesi: İstanbul Büyükşehir Belediyesi’nde bir araştırma*” adlı çalışmada iç denetçilerin bakış açısıyla risk odaklı iç denetim faaliyetini etkileyen faktörlerin belirlenmesidir. Denetim sürecine ilişkin faktörler, teknoloji kullanımı ve kalite kontrol sistemi, yasa, mevzuat, yönetmelik, prosedür, amaç ve plan faktörleri, mesleki ahlak kuralları, mesleki belge ve denetim türleri büyükşehir belediyelerinde denetimin kalitesini etkileyen faktörler olduğu sonucuna ulaşılmıştır.

Zeynep Tıraş (2020): “*KOBİ’lerde risk odaklı iç denetim: bir uygulama*” adlı çalışmada KOBİ’lerin, yöneticilerin ve diğer üst düzey personellerin risk odaklı iç denetime bakış açısını ortaya çıkartmak ve var olan sisteme farklı bir bakış açısı geliştirmek amaçlanmıştır. Kırıkkale Ticaret ve Sanayi Odasına bağlı 177

işletmeyle anket çalışması yapılmış ve KOBİ'lerde risk yönetim uygulamasının var olduğu, en fazla finansal riske odaklanıldığı sonucuna ulaşılmıştır.

Gökhan Ömer Karlıdağ (2020): “*Risk odaklı iç denetim: enerji sektöründe bir uygulama*” adlı çalışmada amaç kurumsal risk yönetiminin sağlanmasında risk odaklı iç denetim faaliyetinin risk belirleme ve ölçme aşamalarındaki rolünün incelenmesidir.

İbrahim Çidem (2021): “*Katılım sigortacılığı şirketlerinde risk odaklı iç denetim: bir vaka çalışması*” adlı çalışmanın amacı risk odaklı iç denetimin uygulama aşamaları ve faydasını katılım sigortacılığı hizmeti sunan işletme üzerinde test etmektir. Araştırmanın sonucunda iç denetim sürecini kapsayan bir model oluşturulmuştur.

Emine Gamze Can (2021): “*Risk odaklı iç denetim: risk değerlendirmesi üzerine örnek bir uygulama*” adlı çalışmada ahşap sektöründe faaliyet gösteren işletmenin finansal biriminin risk odaklı iç denetim planının nasıl oluşturulduğunun, hangi aşamaların gerçekleştirildiğinin ve risk matrisi oluşturma aşamalarının açıklanması amaçlanmıştır.

3.2. Araştırmanın Amacı

Geleneksel iç denetim anlayışının evrilmesiyle risk odaklı iç denetim modeline geçiş yaşanmıştır. İşletmelerin risk odaklı denetim yaklaşımlarını anlamaya yönelik aşağıdaki konular tespit edilmeye çalışılmıştır.

- Risk odaklı iç denetim planının hazırlık aşamasında izlenen adımlar
- Risk odaklı iç denetim faaliyetinin meydana gelebilecek riskleri önleyip önlemediği

- İç denetçilerin riskin yönetilmesinde görev ve sorumluluğunun olup olmadığı
- Denetimin sonunda elde edilen bulgulara yaklaşım
- İç denetimin performansının denetlenip denetlenmediği
- İç denetimin sağladığı faydalar

3.3. Araştırmanın Kapsamı ve Kısıtları

Örnekleme yöntemiyle rastgele olmayan, görüşmeyi kabul eden 13 şirketin iç denetçileri ile görüşülerek Türkiye’deki şirketlerde risk odaklı iç denetim anlayışına yönelik sorulara cevap vermeleri istenmiştir.

Uygulamada elde edilen görüşler Kişisel Verileri Koruma Kanunu kapsamında kişi ve kurum adı verilmeden şirketler alfabetik sıraya göre harf ile kodlanarak aktarılmıştır. “A Katılımcısı, B Katılımcısı, C Katılımcısı, D Katılımcısı, E Katılımcısı, F Katılımcısı, G Katılımcısı, H Katılımcısı, I Katılımcısı, J Katılımcısı, K Katılımcısı, L Katılımcısı, M Katılımcısı olarak 13 şirket kodlanmıştır. Bu bölümde mülakat soruları alt konulara göre gruplandırılarak elde edilen bulgular aktarılmıştır.

3.4. Araştırmanın Yöntemi

Uygulama yöntemi olarak nitel veri toplama tekniği olan mülakat çalışması yapılmıştır.

Nitel araştırmalarda görüşme, gözlem, söylev veya metin analizleri gibi yöntem ve teknikler kullanılabilir. Görüşme tekniği, insanların olaylara bakış açılarının, tecrübelerinin, duygularının, algı ve değerlerinin belirlenmeye çalışıldığı durumlarda detaylı bilgi sağlanması nedeniyle çoğunlukla tercih edilen bir

arařtırma tekniđidir. (Fossey, Harvey, McDermott, ve Davidson alıřması (Baltacı, 2019, s.370-371'den alıntı))

Betimsel analiznin amacı gzlem veya grřme sonucunda elde edilen verilerin dzenlenmiř ve yorumlanmıř bir řekilde aktarılmasıdır. Betimsel analiz tekniđinde veriler belirlenmiř konulara gre sınıflandırılır, sınıflandırılan veriler zetlenir ve yorumlanır. (Fossey, Harvey, McDermott, ve Davidson alıřması (Baltacı, 2019, s.379'dan alıntı))

3.5. Elde Edilen Bulgular

Elde edilen bulgular demografik zellikler, i denetimin genel yapısı, hazırlık ařaması, risklerin nlenmesi ve ynetilmesi, i denetimin performansı ve i denetimin faydası olarak altı bařlık altında zetlenerek aktarılmıřtır.

3.5.1. Demografik zellikler

Katılımcıların demografik zellikleri ve kurumun sektr, toplam alıřan sayısı ve kurumdaki i deneti sayıları ařađıdaki tabloda gsterilmiřtir.

Tablo 3.1. Katılımcıların ve İşletmelerin Demografik Özellikleri

Katılımcı	Yaş	Eğitim	Toplam Çalışma Süresi	Kurumda Çalışma Süresi	Kurumun Sektörü	Kurumun Çalışan Sayısı	İç Denetçi Sayısı
A Katılımcısı	35	Lisans	12 yıl	3,5 yıl	Lojistik, Sigorta, Depolama	1.200-1.500 arası	2
B Katılımcısı	30	Lisans	6 yıl	6 yıl	Gaz	Yaklaşık 1300	3
C Katılımcısı	29	Lisans	5 yıl	2 yıl	Spor	1.900+	4
D Katılımcısı	33	Yüksek Lisans	9 yıl	6 yıl	Sağlık, yapı ve tüketim ürünleri	Yaklaşık 11.000	15
E Katılımcısı	34	Lisans	10 yıl	1,5 yıl	Enerji	10.000-11.000 arası	12
F Katılımcısı	38	Lisans	16 yıl	1 yıl	Alkollü içecek	1.000+	2
G Katılımcısı	33	Yüksek Lisans	8 yıl	4 yıl	Sigorta	260	4
H Katılımcısı	38	Yüksek Lisans	12 yıl	2 yıl	Perakende	1.200	9
I Katılımcısı	45	Yüksek Lisans	22 yıl	3 yıl	Kuruyemiş	1.000	3
J Katılımcısı	31	Yüksek Lisans	6 yıl	1 yıl 2 ay	Giyim perakende	4.086	5
K Katılımcısı	38	Yüksek Lisans	14 yıl	9 yıl	Havacılık	15.000+	8
L Katılımcısı	35	Lisans	11,5 yıl	4,5 yıl	Otomotiv	6.500	3
M Katılımcısı	29	Lisans	8 yıl	3 yıl	Telekomünikasyon	5.000+	2

Yukarıdaki Tablo 3.1.'de görüldüğü üzere 13 iç denetçiden 7'si Lisans mezunu ve 6'sı ise Yüksek Lisans mezunudur. Toplam en düşük iş tecrübesi 5 yıl iken en yüksek iş tecrübesi 22 yıldır. Kurumda çalışma süresi en düşük 1 yıl iken en fazla çalışma süresi 9 yıl olduğu görülmektedir. İşletmelerin farklı sektörlerde faaliyet gösterdikleri ve en az çalışan sayısının sigorta sektöründe en fazla çalışan

sayının havacılık sektöründe olduğu görülmektedir. İç denetçi sayısının da en az 2 ve en çok 15 olduğu görülmektedir.

3.5.2. İç Denetimin Genel Yapısına İlişkin Bulgular

Öncelikle işletmelerde hangi denetimlerin yapıldığını anlamak amacıyla sorulan soruda genellikle süreç bazlı ve mali denetimlerin yapıldığı görüşüne ulaşılmış ve işletmelerin vermiş oldukları cevaplar aşağıda aktarılmıştır.

A Katılımcısı süreç bazlı ve takip denetimlerinin yapıldığı görüşü belirtmiştir. Takip denetimi altında aksiyon takip planında mutabık kalınan konular için gerekli aksiyonların alınıp alınmadığını takibi yapılmaktadır.

B Katılımcısı muhasebe denetimi ve süreç bazlı denetimlerin yapıldığı gerektiğinde iştirak bazlı denetimlerin de yapıldığı görüşünü belirtmiştir.

C Katılımcısı süreç, mali ve uyum denetimleri yapıldığı, özel incelemeler olursa suistimal denetimlerinin de yapıldığı görüşünü belirtmiştir.

D Katılımcısı mali ve süreç denetimlerinin yapıldığı, daha çok satış ve satın alma süreçlerine odaklanılarak tedarik zinciri denetimine evrilme olabildiği görüşünü belirtmiştir.

E Katılımcısı süreç denetimi, IT (information technology-bilişim teknolojileri) denetimi ve etik, soruşturma ile ilgili suistimal denetimi olarak üç denetimin yapıldığı görüşünü belirtmiştir.

F Katılımcısı ise süreç denetiminin yanında mali denetim altında SOX (Sarbanes Oxley) denetiminin yapıldığı görüşünü belirtmiştir.

G Katılımcısı ise mali işler denetimi, MASAK (Mali Suçları Araştırma Kurulu) denetimi, tahsilat, idari işler, hasar ve lojistik denetimi, acente denetimi,

'assurance' denetimi, insan kaynakları gibi mali ve süreç denetimlerinin yanında katastrofik denetim ile performans denetimi yapıldığı görüşünü belirtmiştir.

H Katılımcısı ise operasyonel, süreç ve mali denetimlerin yapıldığı görüşünü belirtmiştir.

I Katılımcısı hangi denetimlerin yapılacağı ihtiyaca göre değiştiği ve daha çok mali denetimlerin yapılmasının yanında bilgi güvenliği ve süreç denetimlerinin yapıldığı görüşünü belirtmiştir.

J Katılımcısı ise süreç denetimlerinin dışında mağaza ve etik denetimlerinin yapıldığı görüşü belirtilmiştir.

K Katılımcısı ise süreç denetimlerinin yanında uyum, bilgi güvenliği ve havalimanlarına özel operasyonel denetimlerin yapıldığı görüşü belirtmiştir.

L Katılımcısı ise üretim, tedarik zinciri, satış, satın alma gibi şirkette ne yapılıyorsa hepsi denetimin bir parçası olduğu görüşünü belirtmiştir.

M Katılımcısı ayırım yapılmadan bütün denetimlerin yapıldığı, IT ve 'business' ayırımının olmadığı görüşünü belirtmiştir.

İşletmelerde denetim planının hangi sıklıkla oluşturulduğunu anlamak için sorulan soruda her işletmenin uymak zorunda olduğu standartlara ve mevzuata uygun bir iç denetim yönetmeliği olduğu anlaşılmış ve denetim evrenine bağlı kalınarak yıllık risk odaklı iç denetim planı oluşturulduğu görüşüne ulaşılmıştır. İşletmelerin hepsinde denetim planı oluşturulurken risk odaklı şirketin maruz kalabileceği stratejik, operasyonel, finansal, idari, uyum ve yasal olmak üzere risk derecelerine göre en yüksek öngörülen risk süreçlerinden başlamak üzere yıllık denetim planı hazırlanarak değişiklik varsa denetim planında güncellemelerin yapıldığı görüşüne ulaşılmıştır. Cevaplar aşağıda detaylı olarak belirtilmiştir.

A Katılımcısı bir süreç denetimi için iki üç kişilik bir denetim ekibi ile 20-30 iş günü kapsayan bir denetim programı hazırlanarak elde edilen bulgulara katma

değerli öneriler geliştirilerek denetim raporunun tamamlanıp Yönetim Kuruluna sunulduğu görüşünü belirtmiştir.

B Katılımcısı yıl başında hangi birimlere odaklanmaları gerektiği belirlenerek, bağlı oldukları holdingin de denetim planı dikkate alınarak yılda en az üç ya da dört kez denetim yapıldığı görüşünü belirtmiştir.

C Katılımcısı yıllık denetim planı dahilinde özel incelemelerle birlikte 15-20 denetim yapıldığı görüşünü belirtmiştir.

D ve F Katılımcıları çeyrek dönemlerde gözden geçirmelerle durum bildirimleri yapılarak yıllık denetim planı oluşturulduğu görüşünü belirtmiştir.

E ve M Katılımcıları ise denetim evreninin gözden geçirilerek gerekli güncellemelerin yapılarak ve risk bölümünün hazırladığı risk envanteri gözden geçiliyor, CEO, direktör, müdür, genel müdür ve yardımcılar seviyesindeki kişilerle bir araya gelerek gündemdeki konular ve riskli alanlar dikkate alınarak denetim planı oluşturulduğu görüşünü belirtmiştir.

G, J ve L Katılımcıları gerekli görüldüğü zamanlarda güncellemelerin yapılarak yıllık denetim planının oluşturulduğu görüşüne ulaşılmıştır. J Katılımcısı pandemi nedeniyle fiziki yapılan denetimlerin sarktığı görüşünü belirtmiştir.

H Katılımcısı yönetim kurulunun isteği doğrultusunda 250 mağazanın senede üç kere denetleneceği şekilde yıllık denetim planı oluşturulduğu görüşünü belirtmiştir.

K Katılımcısı risk değerlendirmesi, mevcut kaynak ve çalışma gün sayısına göre yıllık denetim planı oluşturulduğu görüşünü belirtmiştir.

İşletmelerde iç denetim biriminin kime bağlı olduğunu anlamak için sorulan soruda A, B, C, D, E, G, H, I, L ve M Katılımcıları işletmelerinde Denetim Komitesi aracılığı ile üst yönetime dolayısıyla Yönetim Kuruluna bağlı iç denetim faaliyeti

sürdürüldüğü, J ve K Katılımcıları fonksiyonel olarak denetim komitesine, idari olarak CEO'ya bağlı iç denetim faaliyetlerini sürdürdüğünü belirtmişlerdir. F Katılımcısı ise direk CEFO'ya bağlı iç denetim faaliyetini sürdürdüğü tespit edilmiştir.

Raporlama sıklığını tespit etmek için sorulan soruda, işletmelerin çoğunda raporlama sıklığı ayda bir ya da bir buçuk ayda bir rapor olmak üzere her denetimin sonunda denetim raporu yayınlanmaktadır. F ve M Katılımcıları işletmelerinde ise çeyrek dönemlerde denetim sonunda raporlama yapıldığı görüşünü belirtmiştir.

İşletmelerde iç denetim faaliyetini yürütürken kullanılan test yöntemlerinin yapılan denetim türüne göre değiştiği görüşüne ulaşılmıştır. Örnek olarak gözlem, yeniden hesaplama, analitik inceleme, kontrol testleri, detay testler, örneklem metotlarının kullanıldığı tespit edilmiştir. J Katılımcısı ise bu test yöntemlerinin yanı sıra sızma ve oltalama (fishing) yöntemlerinin kullanıldığı görüşünü belirtmiştir.

İç denetimin sürekliliği konusunda ise hemen hemen her şirkette süreklilik algısının benzer olduğu anlaşılmıştır. Şirketlerde yıl içerisinde yapılan süreç denetimlerinin devamlı olması ve her denetim sürecinden sonra yayınlanan rapor sayısı denetimin sürekliliğini sağladığı görüşü belirtilmiştir. A Katılımcısı süreklilik ile ilgili yönetimin iç denetimden biriminden beklentisinin ne olduğu ile ilgili görüş belirtmiştir. İç denetim birimi olarak bir şeyleri tespit eden ve icrai fonksiyonları kontrol altında tutan ya da korkutan bir yapı olmanız mı yoksa verimlilik esasıyla çalışan danışmanlık rolünün mü beklendiği bu bağlamda iç denetimin sürekliliği tamamen yönetimin görüşüne bağlanmıştır. Ayrıca dijital denetimlerin başladığı ve iç denetçilerin tespit edeceği şeyleri artık yapay zeka teknolojileri sayesinde belki de birine ihtiyaç duyulmayacağı ve bu yüzden sürekliliği sağlamak için Dünya'ya ayak uydurulmasının gerektiği görüşü belirtilmiştir. F Katılımcısı ise sürekliliğin sağlanması günlük operasyonel işlemlerin içine girdiği departmanın uygulanması zorunlu olan kontrollerin

işlerliğinden sorumlu olunması nedeniyle sık sık raporlamaların yapılarak günlük operasyonların değişmez bir parçası olduğu görüşünü belirtmiştir. J Katılımcısı ise süreklilik alınan önemli sorumluluklar ve katma değerli çıktılar ile güven verilmesi şeklinde açıklamıştır. Katma değerli çıktı üretildiğinde iç denetimden farklı çalışmalar için danışmanlık yapılması beklendiği ve bu şekilde sürekliliğin sağlandığı görüşü belirtilmiştir. K Katılımcısı ise sürekliliğin yasal mevzuat zorunluluğu ya da kurumsallaşmak isteyen şirketlerin yasal olarak değil profesyonel olarak iç denetim faaliyetini sürdürdükleri gibi iki şekilde sağlanacağı görüş belirtmiştir. Burada her iki görüşün de benimsenerek ve şirket büyüklüğü göz önünde bulundurularak hem de yabancı şirket ortaklığının olmasıyla sürekliliğin sağlandığı görüşü belirtilmiştir.

İşletmelerde “personellere iç denetim ve risk yönetimi konularında eğitim veriliyor mu?” sorusu sorulduğunda çoğu şirkette personellere eğitim verildiği tespit edilmiştir. A Katılımcısı iç denetim faaliyetini yürüten kişi aynı zamanda iç eğitmen olduğu için şirket içerisinde risk yönetimi iç denetim iki alanda periyodik olarak personellere pandemiye kadar fiziki olarak ama pandemiden sonra artık online eğitimler verildiği görüşünü belirtmiştir. B Katılımcısı ise kalite biriminin altında direk iç denetim gibi değil, tesis denetimi ile ilgili bilgi güvenliği konusunda evraksal konuların denetimine hazırlık olması amacıyla 30-40 kişilik gönüllü iç denetçilerin olduğu ve mevzuatsal denetime başlamadan bu ekibin sahaya inerek kontrol yaparken aynı zamanda iş süreci ile bilgilendirmelerin yapıldığı görüş belirtmiştir. C Katılımcısı ise eğitimin İnsan Kaynakları departmanı tarafından yürütüldüğü ve bağlı bulunulan holding ile birlikte pandemi sebebiyle online eğitim platformu üzerinden destekleyici çalışmalarının olduğu görüşünü belirtmiştir. Ayrıca bağımsız denetim firmalarından seminerler alındığı ve mesleki belge almak isteyenlerinde desteklendiği görüşü belirtilmiştir. D Katılımcısı davranış kuralları özelinde denetim, hukuk ve insan kaynakları birimlerinin webinarları ile rüşvet ve yolsuzlukla mücadele, çıkar çatışması konularına, insan ilişkileri, değer verme politikası gibi çeşitli bölümlerle ilgili 15 günde bir çalışanlara hatırlatma mailleri

atılması ve çalışanlar bilgisayar ekranları kilitletiğinde ekrana davranış kuralları hatırlatma bildirim, örneğin davranış kurallarının şu maddesine göre böyle bir durum olduğunda şu şekilde davranmanız gerekiyor, aksi takdirde şu bölümden bildirimde bulunabilirsiniz şeklinde bildirimler göndererek bildirim sayılarında da artış gözlemledikleri görüşünü belirtmiştir. E ve G Katılımcıları risk yönetimi ve iç denetim ile ilgili eğitim verilmediği görüşünü belirtmiştir. F Katılımcısı ise her denetimin başında yapılan risk değerlendirme çalışmalarının workshop niteliğinde yapılarak kurum kültüründe var olan farkındalığı yüzde yetmiş-seksen seviyesinde olduğu ve yeni giren kişilere de müdürleri tarafından bu bilgilendirmenin yapıldığı görüşünü belirtmiştir. H Katılımcısı denetim ekibinin çok genç olduğu için iç eğitim ve bilgilendirme ile desteklenmeleri gerektiği görüşünü belirtmiştir. I Katılımcısı ise iç denetim ile ilgili dışardan bir eğitim desteğinin alınmadığı katılımcının eğitim verdiği görüşünü belirtmiştir. J Katılımcısı uyum, etik ve risk yönetimi konularında periyodik eğitimlerin verildiği ve bunun yanı sıra işe yeni başlayan personellere şirket yapısı, rüşvet ve yolsuzluk gibi konularda oryantasyon verildiği görüşünü belirtmiştir. L Katılımcısı iç denetim ile ilgili eğitim verilmediği, iç denetimin sorumluluğunda olan uyum ve etik ilkeler ile ilgili eğitim ve oryantasyonların verildiği görüşünü belirtmiştir. M Katılımcısı ise iç denetim ve risk yönetimi ile ilgili yılda en az bir kere hatta yüksek riskli konularda ise altı ayda bir tekrar eden eğitimlerin verildiği görüşü belirtilmiştir.

3.5.3. İç Denetimin Hazırlık Aşamasına İlişkin Bulgular

İç denetime hazırlık aşamasında izlenen adımlar ve önceliklendirilen alanların neler olduğunu anlamak için yöneltilen soruda çoğu işletmede iç denetimin hazırlık aşamasında benzer adımlar izlendiği görüşüne ulaşılmıştır. Hazırlık aşamasında öncelikle risk matrisi değerlendirmesi yapılarak riskli alanlar tespit edilerek risk matrisleri oluşturulmaktadır. Böylece yapılan risk puanlamasına göre en riskli alanların denetim önceliğine alındığı tespit edilmiştir. Denetim planı

oluşturulurken geçmiş yıllarda yapılan denetim sonuçlarından elde edilen bilgiler değerlendirilerek ve bulguların kapatılıp kapatılmadığı, aksiyon planına sadık kalıp kalınmadığının kontrolü, bağımsız denetim raporları ve finansal tablolardan yararlanıldığı görüşü belirtilmiştir. İlgili fonksiyon en son ne zaman denetlenmiş, prosedürlere ve mevzuata uygunluk değerlendirmesi ve varsa gerekli güncellemelerin yapıldığı da belirtilmiştir. Denetim için tüm çalışmalar tamamlandığında bir denetim takviminin oluşturulduğu ve açılış toplantısı düzenlenerek üst yönetim veya denetim komitesinin onayıyla denetim takvimine uygun olacak şekilde denetim sürecine başladıkları görüşü tespit edilmiştir.

A Katılımcısı risk katsayılarına göre şirketin aktiflerine ve satışlarına etki eden, ciroasal anlamda büyük getiri sağlayan kalemlere odaklanılarak yüksek risk seviyesine sahip süreçlerin nasıl işlediği, kurumsal yapıya uygunluğu, belirlenen risklere karşı aksiyon alıp alınmadığı, düzeltici faaliyet alanlarının olup olmadığı, süreci yöneten kişilerin kontrol zafiyetlerinin olup olmadığı, usulsüzlüklerin olup olmadığı analar önceliklendirilerek denetim açılış toplantısı ile başlayarak, risk değerlendirmeleri ile süreçlere dair politikaların, talimatların, prosedürlerin, geçmiş dönem raporların incelenmesiyle ve onların risk değerlendirilmesinin alınmasıyla devam ettiğini, sonrasında denetim ekibinin denetim programı hazırlayarak, hangi işlem adımında hangi denetim testini uygulayacağını planlar ve denetim planlamasını yaparak denetime başladığı görüşünü belirtmiştir.

B Katılımcısı ilk önce denetlenecek alan belirlenerek hazırlık aşamasının oluşturulduğu görüşünü belirtmiştir. Örneğin, muhasebe birimi denetlenecek ise SAP sisteminden veriler alınarak, departmanın İK yönetimi, bütçeye uyumu, yatırımların fizibiliteye uyumu ve katma değeri gibi konulara ayrılarak, hangi alanlara odaklanılacağına dair konu başlıklarına göre gruplandırma yapılmaktadır. Yeni işlere, yeni yatırımlara ve yüksek hacimli alanlara odaklanılarak riskin verimlilik ve fayda taraflarına ilişkin farklı açılardan bakılmaya çalışılmaktadır.

Bunların dışında gelen ihbar olursa bu özel inceleme denetimi de öncelik sırasına alınarak çözüme ulaştırılmaktadır.

C Katılımcısı bir önceki denetimde ilgili süreçle ilgili açık bulgu var mı, bu bulguların kontrol eksikleri neler, açıkta kalan bulgular önceliklendirilerek, hem şirket faaliyetlerini hem de organizasyon yapısını anlamak adına bir önceki denetim raporunun okunması ile denetim hazırlıklarına başlandığı görüşünü belirtmiştir. Hangi noktalarda eksikliklerin olduğu tespit edilmektedir ve ilgili departman ile bir toplantı ayarlanmaktadır. Bu toplantıda denetimin amacı, kapsamı, hangi noktalara değinileceği, denetimin süresi gibi konularda bilgilendirme yapılmaktadır. Daha sonra şirketin yeni girdiği bir süreç var mı, varsa o alanlar denetim önceliğine alınarak analitik incelemeler yapılarak, cezai işlem olmaması için mevzuata uygunluk açısından mevzuat okumaları yapılmaktadır ve bu alanlar ile ilgili risk seviyeleri belirlenmektedir. Önemli risk seviyeleri belirlendikten sonra risk açıklamaları ve kontrol testleri belirlenerek denetim planı oluşturularak denetim süreci başlamaktadır.

D Katılımcısı öncelikle bütün departmanlar ile örneğin satış, tedarik zinciri, Ar-Ge ve üretim gibi birimler ile bir araya gelinerek öncelikle onların riskli gördükleri ve denetlenmesini istedikleri alanların olup olmadığı sorularak risk havuzunda değerlendirmeye alındığı görüşünü belirtmiştir. Daha sonra departmanlardan gelen önerilerin finansal etkileri de göz önünde bulundurularak önceliklendirme yapılarak bilgiler üst yönetime sunulmaktadır. Bu bilgiler dışında eğer üst yönetimden gelen bir istek olursa denetim ile ilgili yeterli kaynak oluşturularak (gerektiğinde dış kaynak temini ile) bütçelendirme yapılarak denetim komitesine sunulmaktadır. Denetim Komitesi'nin onayı ile denetim planı oluşturulmaktadır.

E Katılımcısı hazırlık aşamasında öncelikle şirketin kullanmış olduğu sistemden ilgili sürece ilişkin prosedürler, iş akışları, mevzuat vs. ile ilgili okumalarla ve süreç sahipleriyle görüşmeler yapıldığı görüşünü belirtmiştir. Bunlar

ıřığında çoęu riskli alan tespit edilerek risk kontrol matrisleri oluřturulmaktadır. Gncelleme gerekiyorsa gerekli gncellemeler yapılarak risk kontrol matrisi oluřturulduktan sonra saha alıřmasına bařlanmaktadır.

F Katılımcısı Uluslararası İ Denetim Standartları'na uygun risk bazlı bir planlamayla operasyonel srelerin iinde bulunan riskleri tanımlayarak bu risklerin kuvvetini lmleyen metodolojiyle hangi alanlara odaklanması gerektięinin ortaya ıktığı grřn belirtmiřtir. Bu noktalar yıllık iř gnlerine blmlenerek oluřturulmaktadır ve genel merkeze baęlı her lkenin uymak zorunda olduęu anahtar kontrollerle takip edilmesi gereken kontroller her yıl test edilmektedir.

G Katılımcısı hazırlık ařamasında ncelikle yılın bařında denetim takvimi oluřturulduęu grřn belirtmiřtir. Denetim takvimi oluřturulurken sre bazlı risk deęerlendirmesi yapılmaktadır. Hangi sre ne kadar riskli, bunun mali riski nedir, yasal riski nedir, uyum riski nedir, itibar riski nedir řeklinde bir puanlama yapılmaktadır. Puanlamaya gre denetim takvimi belirlendikten sonra sre plana gemektedir. rnek olarak, mesela muhasebe birimi denetlenecek, prosedr ve mevzuat incelemeleri yapılarak uygun mu deęil mi bununla ilgili n alıřma yapılmaktadır. Daha sonra denetim planı bu řekilde, řunlar řunlar denetlenecek, řunlara bakılacak, risk matrisinde bu alanlar riskli grlmekte gibi mdre sunum yapılmaktadır. O uygun bulunduęu takdirde denetim sreci bařlamaktadır, eęer uygun bulmazsa gerekli dzeltmeler yapıldıktan sonra denetim sreci bařlamaktadır.

H Katılımcısı hazırlık ařaması sre ve finansal denetimlerin altında oluřturulmuř kontrol listelerinin gncellenmesiyle bařlandıęı grřn belirtmiřtir. Buna gre bir sonraki yılın denetim planı oluřturulmaktadır. Buna gre ekibin zaman planlamaları yapılmaktadır. Hangi maęazalara kimler gidecek, hangi gnler gidilecek gibi byle bir denetim takvimi oluřturulmaktadır. Eęer Ynetim Kurulunun isteęi olursa ncelik o isteklere verildikten sonra normal rutin planlama yapılmaktadır. rnek olarak, haftalık veya aylık periyotta bir yapılan kasa

sayımları, banka talimatları ve masraflar gibi rutin kontroller vardır. Diğer bir hazırlık aşaması ise, nelerin önceliklendirileceği konusunda ekip ile istişare edilmektedir. Örneğin, ekibe bir arkadaş yeni katıldı, onunla oturup biz bundan sonra hangi denetimleri sürekli ele alalım gibi istişare edilmektedir. Yani süreç denetimleri finansı komple denetleyelim çıkalım şeklinde süreçle ilerlememektedir. Finansın önem derecesindeki veya suistimal içerebilecek hususları nelerse yani finansın bir kolu incelenmektedir. Yani denetim takvimine o konu alınmaktadır. Birinci öncelik yönetim kurulunun isteklerine verilmektedir ve ikinci öncelik risk içeren hususlar ve devam eden bulgulardır.

I Katılımcısı ise her sene risk haritalandırılması yapılmamaktadır. Bir kere yapılmıştır ve 700-800 satırlık sonuç çıktığı görüşünü belirtmiştir. Bu yüzden denetim planı yapılırken bütün iş birimleri ile “sizin en büyük riskleriniz neler?” şeklinde sorular yöneltilmektedir. Verilen cevaplara göre risk değerlendirmesi yapılmaktadır ve risk seviyesi belirlenmektedir. Riskler puanlanarak filtrelenerek ilk 100 risk değerlendirmeye alınmaktadır.

J Katılımcısı hazırlık aşamasında süreç denetimleri risk odaklı denetim planı oluşturulurken kurumsal risk yönetimi çalışmasının yapıldığı ve denetim evreninin ve önceliklerinin oluşturulduğu görüşünü belirtmiştir. Şirketin hedeflerine bağlı olarak oluşturulan bu riskler operasyonel, finansal, itibar, yasal olmak üzere kategorilere ayrılarak risk envanteri oluşturulmaktadır. Oluşturulan risk envanteri etki olasılık değerine göre puanlanmaktadır. En yüksek skoru alan risk en öncelikli risk olmaktadır ve denetim kaynağı o departman için ayrılmaktadır.

K Katılımcısı ise alt şirketleri olan 15 şirketin kendi iş süreçlerinin olduğu iş süreçlerine göre hukuksal, uyum ve regülasyon vs. gibi risk değerlendirmesine göre puanlama metodolojisinin olduğu görüşünü belirtmiştir. Süreç sahipleri ile görüşülerek değerlendirilen iç kontrol yapısı değerlendirilerek yapılan puanlama denetim ekibinin inisiyatifıyla bulgular ve denetim sonuçları nedeniyle puanlama değiştirilebilmektedir. Bunlar üzerinden belirli harmanlamalar yapılarak risk

değerlendirmesi oluşmaktadır. Risk değerlendirmesinde en son ne zaman denetime gidilmiş, denetim raporu ne olmuş, ne kadar bulgu vardı gibi durumlar göz önünde bulundurularak her birinin ayrı ağırlıklandırmasına ve risk değerlendirmesine göre önceliklendirme belirleniyor. Örneğin, çok uzun süre gidilmeyen ya da notu düşük olan rapor veya iç kontrol yapısı var ise operasyonel, finansal ve repütasyon gibi kavramlardan etkilenen notlandırmalar var ise bunlar en yukarıda olur ve eldeki kaynakla bu denetimlerin ne kadar sürede tamamlanabilir olduğu belirlenerek yapılacak denetimler sıralanıyor duruma ve risk derecesine göre aşağı sıralarda olan denetim ön sıraya alınmaktadır.

L Katılımcısı hazırlık aşamasında her sene Aralık ayında bir değerlendirme yapılarak hangi fonksiyonlara denetim yapıldığı belirlenerek aksiyon takip planları gözden geçirildiği görüşünü belirtmiştir. Standartlar çerçevesinde aksiyonların ne kadarı tamamlanmış, ne kadarı tamamlanmamış takip edilerek ve hiç denetlenmeyen fonksiyonlar belirlenerek bir sonraki yılın hafta hafta denetim planı oluşturulmaktadır. Eğer üst yönetimden risk algısına göre şu denetimi yapmayın, bu denetimi yapın şeklinde istek gelirse o denetim öncelik sırasına alınarak yıl başında hangi operasyonların denetleneceği belirlenerek denetim planı üst yönetimin ve denetim komitesinin onayıyla tamamlanmaktadır.

M Katılımcısı hazırlık planı ise hem lokal market riski hem de ilk 10 risk stratejisi olarak risk envanteri oluşturulduğu görüşünü belirtmiştir. Bu ilk 10 risk strateji riski, finansal risk ve regülasyon riski gibi riskleri de içermektedir. Örneğin, şirket yeni bir girişim yapacaksa şirket stratejisi, risk değerlendirmesi, yüksek risk politikası ve ilk on risk envanteri ile birlikte Genel Müdür ve Yardımcıları ile görüşülerek denetim planı oluşturulmaktadır. Oluşturulan denetim planı değişen regülasyon vs. ile risk seviyelerinin değişmesine yönelik çeyrek dönemlerde gözden geçirilerek güncellenmektedir.

3.5.4. Risklerin Önlenmesi ve Yönetilmesine İlişkin Bulgular

Risklerin önlenmesi ile ilgili A Katılımcısı risklerin tamamen önlenebileceğini ve bunun yönetsel bir karar da olabileceğinin yani stratejik hedefler doğrultusunda riskin kabul edilmesi, riskin reddedilmesi ya da üçüncü kişilerle riskin paylaşılması durumlarının olabileceği görüşünü belirtmiştir.

B, C, E, H, I Katılımcıları şirketlerinde ise risklerin önlenebileceği görüşünü belirtmişlerdir. Risklerin tespit edilmesi, değerlendirilmesi ve sonrasında alınacak aksiyonlar ile ilgili önerilerin sunulması iç denetimin meydana gelebilecek riskleri önlediği görüşünü savunmuşlardır.

D Katılımcısı riskleri önleyecek veya üstlenecek departmanın iç denetim olmadığı ve iç denetim biriminin risk konusunda bir yönetim fonksiyonu olduğu, iş birimlerinin riski önleme sorumluluğu olduğu görüşünü belirtmiştir.

J, K, L Katılımcıları işletmelerinde iç denetimin meydana gelebilecek riskleri önleyip önlemediğini ölçmenin mümkün olmadığı görüşünü belirtmiştir. Risk değerlendirmelerinin yapıldığı ama yine de risk belirsizlik olduğu ve belirsizliğin önlenmesinin kolay olmadığı görüşü belirtilmiştir. Ayrıca J Katılımcısı riskli alanların tespit edilip üst yönetime sunulması güvence verildiği görüşünü belirtmiştir.

Riskin yönetilmesi konusunda ise A, B, C, H, I, K, L ve M Katılımcıları işletmelerinde iç denetim birimlerinin görev ve sorumluluğunun bulunmadığını, sorumluluğun süreç sahiplerinde olduğunu belirtmiştir.

D Katılımcısı riskin yönetilmesi sürecinde iç denetim biriminin görev ve sorumluluğun olmadığı risk yönetim biriminin etkinliğini ölçmek, performansıyla ilgili görüş vermek ve yönetimde bir problem görüyorlarsa denetim komitesine ve yönetim kuruluna bilgilendirme sorumluluğu olduğunu belirtmiştir.

E Katılımcısı risk iştahına uygun kontrol tasarımı var mı, varsa yeterli mi, düzgün çalışıyor mu, bu konuda riskin yönetilmesi açısından temel görev ve sorumluluk olduğu görüşünü belirtmiştir.

F Katılımcısı ise iç denetime, regülasyonlara, şirket içi prosedürlere, etik yönetime uygunluk tarafında görev ve sorumluluğun olduğunu belirtmiştir.

G Katılımcısı riske karşı proaktif davranma sorumluluğunun olduğu görüşünü belirtmiştir.

3.5.5. Denetim Sonunda Elde Edilen Bulgulara Yaklaşım İlişkin Bulgular

Şirketlerin genelinde denetim sonunda elde edilen bulgulara iç denetçilerin yaklaşımının yapıcı ve çözüm odaklı olduğu tespit edilmiştir. Elde edilen bulguya ve bulgunun risk derecesine göre alınan aksiyon takip planlarının oluşturulduğu her bulgu için değişiklik gösteren bulgu kapanma tarihi belirlendiği görüşüne ulaşılmıştır. İç denetçiler ilgili fonksiyon ya da ilgili kişi ile görüşerek elde edilen bulgu ne dururumda, aksiyon alınmış mı, alındıysa hangi aksiyonlar alınmış, bulgu kapatılmış mı, kapatılmadıysa neden kapatılmamış, kapanması için ilgili fonksiyonun ne kadar süresi var gibi soruların cevaplarını kolaylıkla yönetebilmektedirler. Aksiyon alınmayan bulgular için önce ilgili birim yöneticisi ile görüşülerek bulgunun kapanması gerektiği iletiliyor ve Denetim Komitesi aracılığıyla üst yönetime ne kadar bulgu elde edilmiş ne kadar kapanmış ne kadarı kapanmamış şeklinde raporlama yapılıyor.

Yukarıdakilere ek olarak, A ve E Katılımcıları elde edilen bulgulara yaklaşım aksiyonların alınması ile ilgili kullandıkları program olduğunu ve program üzerinden süreç sahiplerine bulgunun belirlenen tarihe kadar kapanması ile ilgili e-mail ve zaman kısaldıkça hatırlatma maillerinin gönderildiği görüşünü belirtmişlerdir.

3.5.6. İç Denetimin Performansına İlişkin Bulgular

İşletmelerde iç denetimin performansının denetlenip denetlenmediği, denetleniyorsa nasıl denetlendiğini anlamaya yönelik sorulan soruda G, J, K ve M Katılımcıları işletmelerinde iç denetim faaliyetlerinin amacına uygun çalışıp çalışmadığını 5 yılda bir bağımsız denetim firmalarından kalite güvence hizmeti olarak iç denetimin etkinliğinin ve verimliliğinin ölçüldüğünü belirtmişlerdir. Raporlarda standartlara uygun denetimin yapıldığının yer alması için iç denetimin performans ölçüt kriteri 5 yılda bir bağımsız denetim firmaları tarafından denetimlerin yapılmasıdır. Bu işletmelerin dışındaki şirketlerin çoğunda performans ölçüt kriterleri kullanıldığı görüşüne varılmıştır. İnsan Kaynakları departmanının belirlemiş olduğu performans sistemi ile iç denetimin performansının ölçüldüğü tespit edilmiştir.

B Katılımcısı ise şirketinin iç denetim performansı bağlı olduğu holding tarafından denetlendiği görüşünü belirtmiştir.

C Katılımcısı yıl sonunda yazılan denetim raporu üzerinden denetim komitesi dolayısıyla yönetim kurulu tarafından hem iç denetimin hem de şirket performansının denetlendiği onun dışında herhangi bir performans değerlendirme ölçütünün olmadığı görüşünü belirtmiştir.

D Katılımcısı kendi kalite gözden geçirmelerinin yapıldığı ilerleyen zamanlarda ise bağımsız kalite gözlemden geçmeyi hedefledikleri görüşünü belirtmiştir.

E Katılımcısı şirket tüzüğünde iç denetimin performansından denetim komitesi sorumlu olduğu belirtilmiş ve bu nedenle denetim komitesi oluşturulan KPI'larla iç denetimin performansını değerlendirdiği görüşünü belirtmiştir. Katılımcının çalışma süresi boyunca 1,5-2 senedir dört büyüklerin yaptığı QR denetiminden geçemedikleri görüşü belirtilmiştir.

F Katılımcısı ise genel merkeze bağı bir şirket oldukları için iş planlarını her gün genel merkeze raporladıkları ve bu nedenle de performanslarının sıkı sıkıya takip edildiği görüşünü belirtmiştir.

H Katılımcısı denetimin performansının denetlenmediği fakat güzel işler çıkartıldığı görülmesi için performans değerlendirmesinin yapılması gerektiği görüşünü belirtmiştir.

I Katılımcısı kendi KPI sistemleri ile kontrol öz değerlendirmelerinin yapıldığı fakat bağımsız denetim kalite güvencesinden geçemediklerini ama kaliteli şirketlerin bu güvence hizmetini almaları gerektiği görüşünü belirtmiştir. Ayrıca kendi KPI hedefi olarak müşteri memnuniyet anketlerinin yapılması gerektiği ama güvenilir olmayacağı ve doğruyu yansıtmayacağı düşüncesiyle bunun yapılmasını doğru bulunmadığı görüşü belirtilmiştir.

L Katılımcısı ise genel müdür tarafından sene başında belirlenen hedeflerin yıl sonunda ne kadarının gerçekleştirildiği ölçülerek performans değerlendirilmesi yapıldığı görüşü belirtilmiştir.

3.5.7. İç Denetimin Faydasına İlişkin Bulgular

A, C ve H Katılımcıları tarafından iç denetçilerinin ortak görüşü olarak iç denetimin faydası risklerin tespit edilmesinde erken uyarı sinyali görevinin olduğu, tespit edilen risklerin ortadan kaldırılması ya da düzeltilebileceğine ilişkin yol haritasının belirlenmesi denetimin en büyük faydası olarak belirtilmiştir. İç denetimin sadece bir alana değil işletmedeki bütün alanlara ışık tutarak saygınlık yaratması da iç denetimin sağladığı faydalardan bir tanesi olduğu görüşünde bulunulmuştur.

B ve E Katılımcıları belli bir zaman sonra birimlerde yaşanan körlüğü ortadan kaldırması ve insanların denetlendiği hissine kapılarak daha temkinli davranmasını sağladığı görüşü savunulmuştur. Böylece daha kontrollü ve bilinçli

bir çalışma ortamının sağlandığı, finansal kaygının önlenebildiği ve operasyonların iyileştirilebildiği görüşünde bulunmuşlardır.

C, G ve J Katılımcıları iç denetimin yasa ve düzenlemelere uygunluğunu denetlemesiyle doğru ve güvenilir bilgiye ulaşmada öncü bir rol oynadığı ve böylece hata ve hilelerden kayıpların önlenildiği ve üst yönetime şeffaf bir şekilde raporlama yapıldığı görüşünde bulunmuşlardır.

Çoğu şirket iç denetimin faydası olarak genel yargısı iç denetimin şirketi güvenli alanda tutmak için katma değer sağlayan bir fonksiyon olduğu görüşünde bulunmuşlardır. Bu görüşe ek olarak I Katılımcısı *“İç denetim aslında değer katmaya çalışan bir yapıdır. İç denetim neden önemlidir? Sigortasız çalışan bir işçi düşünün, sigortası ödenmeyen bir kişi o şirkette çalışmak ister mi? İç denetim olmadan şirketler belki çok kısa bir süre giderler ama sonra bir yerde motor bozulduğu zaman bir yerde patlak verecekler. Mesela ceza yedikleri zaman iç denetim birimini tekrar kuralım derler. İç denetimin faydasını bu açıdan düşünün.”* şeklinde örnek vererek görüşünü belirtmiştir.

D Katılımcısı iç denetim biriminin paydaşlara güvence verdiği, eğer işlemeyen süreç ve kontrol mekanizmaları varsa bunları hatırlatan birim olduğu görüşünde bulunmuştur. Bu yargıya örnek olarak, şirket yapısı çeşitli kontrol mekanizmalarıyla güvence altına alınmış mı, bu mekanizma çalışıyor mu, bu şirket sürdürülebilir mi, bu şirketin karlılığı devam ettirilebilir mi gibi bu soruların güvencesini verdiği görüşünde bulunmuştur.

İç denetimin dışardan bir göz olarak işletmeye tepeden baktığı tümünden varım bakış açısıyla bütünsel bir yaklaşım sergilediği konusunda en büyük fayda sağlandığı B, F ve M Katılımcıları ortak görüşte bulunmuşlardır.

L Katılımcısı ise bu sorunun zor bir soru olduğu ve kurum için çok faydalı olduğu görüşünde bulunmuştur.

K Katılımcısı tarafından iç denetimin faydasının ölçümlenemeyeceği görüşünde bulunmuştur.

3.6. Araştırmanın Sonuçları

İç denetçi sayıları sektöre ve kurumun çalışan sayısına göre değişiklik göstermektedir. Sektör ve çalışan sayısı olarak değerlendirildiğinde iç denetçi sayılarının yetersiz olduğu tespit edilmiştir. İşletmelerde direk CEO'ya bağlı bir yapı bulunsa da genel olarak işletmeler üst yönetime bağlı olarak iç denetim faaliyetlerini sürdürmektedir. 1110 Kurum İçi Bağımsızlık başlıklı standardına göre iç denetim faaliyetlerinin yerine getirilmesine olanak sağlayan yönetim organına bağlı olmak zorundadır ve bağımsızlık işlevsel olarak yönetim kuruluna raporlama yapılmasıyla etkili bir şekilde sağlanmaktadır. Genellikle süreç bazlı denetimlerin gerçekleştirildiği, muhasebe, satın alma ve sektöre bağlı olarak üretim birimlerinin denetlenmesine öncelik verildiği görüşü tespit edilmiştir. İşletmelerin hepsinde denetim planı yıllık olarak risk odaklı oluşturulmaktadır. 2010 Planlama başlıklı standardına göre işletme hedeflerine uygun olarak İç Denetim Yönetici'si iç denetim faaliyetinin önceliklerinin belirlenerek risk esaslı denetim planı oluşturması sorunludur. Tespit edilen riskli alanlar denetim önceliğine alınmaktadır.

Denetime hazırlık aşamasında genellikle benzer adımlar izlense de fakat başvuru ve önceliklendirilen alanlar sektörlere göre değişiklik göstermektedir. 2200 Görev Planlaması başlıklı standardına göre her görev için amaç, kapsam, zaman, kaynak dağılımını, işletmenin hedeflerini, stratejilerini ve riskleri içeren bir plan hazırlanması ve yazılı hale getirilmesi zorunludur. İç denetim faaliyetinin işletmede meydana gelebilecek riskleri önlediği konusunda iki ayrı görüşe varılmıştır. İç denetçilerin çoğu iç denetim faaliyetinin işletmede meydana gelebilecek riskleri önemli ölçüde önlediğini savunurken bir kısım iç denetçi ise

riskin belirsizlik olduğu, belirsizliği dolayısıyla riskleri önlemenin derecesinin mümkün olmayacağı görüşünü savunmuştur. Riskin yönetilmesi aşamasında iç denetçilerin sorumluluğunun ortak olduğu alan aksiyon takip aşamasıdır. Bunun dışında bazı işletmelerde riskin yönetilmesi sorumluluğu iç denetim birimindeyken bazı işletmelerde riskin yönetilmesi sorumluluğunun süreç sahipleri olduğu tespit edilmiştir. 2120 Risk Yönetimi başlıklı standardına göre iç denetim risk yönetimi süreçlerinin değerlendirilmesi ve iyileştirilmesi aşamalarına katkı sağlamak zorundadır. İşletmelerin azınlığında personellere iç denetim ve risk yönetimi ile ilgili eğitimlerin verildiği görüşü saptanmıştır. İşletmelerde genellikle iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri ihtiyaca ve yapılan denetime göre değişiklik gösterse de uygulamada bütün test yöntemlerinin uygulandığı aşamasında benzerlikler olduğu görüşüne varılmıştır. İç denetçilerin elde edilen bulgulara yaklaşımı ise genellikle yapıcı ve çözüm odaklı olduğu anlaşılmıştır. Raporlama sıklığı olarak her denetimin sonunda olmak üzere genellikle bir ya da bir buçuk ayda bir denetim raporu yayınlanmaktadır. İç denetim biriminin performansının denetlenmesi konusunda üç ayrı kanıya varılmıştır. Bunlar, iç denetimin performansının ölçülmediği işletmenin var olduğu, iç denetim biriminin performansının üst yönetim ve insan kaynakları aracılığıyla ölçülen işletmelerin olduğu ve çok az sayıda işletmenin performans ölçme sisteminin dışında beş yılda bir bağımsız denetim firmalarından güvence hizmeti alınarak iç denetim fonksiyonunun performansının denetlendiği görüşüne ulaşılmıştır. 1300 Kalite Güvence ve Geliştirme başlıklı standardına göre iç denetimin etkinliğini ve verimliliğini ölçmek için iç denetim faaliyetlerinin bütün alanlarını kapsayan bir kalite güvence ve geliştirme programı hazırlamak ve sürdürmek zorundadır. Kalite güvence ve geliştirme programı ile hem iç hem de dış değerlendirmeleri içermelidir. Çünkü iç denetim biriminin Uluslararası İç Denetim Mesleki Uygulama Standartlarına uygun olduğu görüşünün belirtilmesi sadece Kalite Güvence ve Geliştirme Programı'nın değerlendirme sonuçlarına bağlıdır. İç denetimin sürekliliği konusunda ise iç denetçilerin ortak görüşü işletme içerisinde

sürekli denetimlerin yapıldığı kanısıdır. İç denetimin faydası konusunda farklı görüşler belirtilse de ortak kanı iç denetim fonksiyonu işletmeye katma değer katan, güvence ve danışmanlık hizmeti görevi üstlenen, işletmenin olmazsa olmaz bir parçası görüşüne varılmıştır.



SONUÇ VE ÖNERİLER

Geleneksel iç denetimden risk odaklı denetim anlayışı modeline geçiş ile birlikte geleceğe yönelik oluşturulan risk odaklı denetim anlayışıyla iç denetim faaliyetini yürüten kişilerden beklentiler artmış, sadece sorgulama yapmaları değil çözüm ve önerilerde bulunmaları beklenmektedir. Dolayısıyla danışmanlık ve güvence hizmeti veren iç denetim fonksiyonunun önemi artmıştır. Hesap verilebilirlik ve saydamlık ilkeleri doğrultusunda geçmişini analiz ederek geleceğe yönelik fırsatları ve tehditleri öngörebilen, süreç bazlı değerlendirmeler yapabilen, üst yönetimin taleplerinin doğru ve zamanında karşılayabilen, teknolojik gelişmeleri risk odaklı bakış açısıyla etkin bir şekilde kullanabilen, danışmanlık ve güvence hizmeti görevini yerine getiren iç denetçiler işletme başarısına arttırmakta hayati bir öneme sahiptir.

Risk odaklı iç denetim faaliyeti iç kontrol ve kurumsal risk yönetimi süreçleriyle eş zamanlı yürütülmektedir. İç kontrol ve kurumsal risk yönetimi uygulamalarının işleyişi ve tasarımı hakkında güvence ve danışmanlık hizmeti vermek iç denetimin üstlenmiş olduğu görevlerden biridir. Risk odaklı iç denetim işletme hedefleri ve stratejileri doğrultusunda gerekli yapıların oluşturulması ve riskli görülen alanlar ile ilgili üst yönetime iyileştirici ve katma değerli önerilerde bulunulması anlayışıdır. Risk odaklı iç denetimde risklerin yönetilmesi süreci iç denetçilerin değil işletme yönetiminin sorumluluğundadır bu nedenle etkin bir risk yönetimi için görev ve sorumlulukların açıkça belirlenmiş olması gereklidir.

Gelişen teknoloji ve küreselleşme ile birlikte meydana gelen hileli muhasebe kayıtlarının finansal raporlamaların güvenilir olup olmadığının sorgulanmasıyla iç denetim ve iç kontrol sistemlerinin etkin ve verimli bir şekilde yürütülmesi işletmeler için hayati bir öneme sahip olmuştur. İç denetimin şirkete katma değer sağlayarak etkin bir şekilde yürütülmesi için risk odaklı denetim planının oluşturulması, üst yönetim ile etkili iletişimde bulunulması, raporlama ve

takip sisteminin olmasına bağlıdır. İç denetim planı riskleri temel alarak oluşturulan denetim faaliyeti için gerekli olan insan kaynağını ve bütçesini içermeli, denetim komitesi ve üst yönetimin bilgi ve onayı alınarak denetim planı uygulamaya konulmalıdır. Uluslararası Standartların zorunlu kıldığı şirketin kalite ve güvence geliştirme programının olması iç denetim faaliyetinin sürekliliğini ve etkinliğini sağlama açısından önemli bir role sahiptir.

İç denetimin amacı işletme kaynaklarının etkin ve verimli bir şekilde kullanılıp kullanılmadığını, işletme varlıklarının korunup korunmadığını, işletme faaliyetlerinin prosedürlere uygun bir şekilde yürütülüp yürütülmediğini inceleyerek iç kontrollerin etkinliğini ve verimliliğini ölçmektir. Günümüzde iç denetimin temelini risklerin belirlenmesi oluşturmaktadır. Risk odaklı iç denetim sürecinde risklerin belirlenerek denetim kaynaklarını riskli alanlara yoğunlaştırmak denetimin etkinliğini ve verimliliğini üst seviyelere çıkarılması açısından önemli rol oynamaktadır. İşletme kaynakların etkin ve verimli kullanılması iç denetimin sağladığı katma değer bir parçasıdır. Risklerin belirlenmesi ve değerlendirilmesi aşamasında etkinlik ve verimlilik açısından değerlendirmeler yapılarak üst yönetime raporlanır ve böylece iç denetim işletmede meydana gelebilecek büyük zarara veya kayıplara yol açacak telafisi olmayan durumların tespiti ve önlenmesi konusunda üst yönetimin sorumluluklarını yerine getirmesine yardımcı olmaktadır. İç denetim işletmelerde geleneksel yaklaşım modelindeki polislik görevinden uzaklaşarak danışmanlık ve güvence hizmeti görevini üstlenmiştir. İç denetçilerin işletmelere sağladığı danışmanlık güvence hizmeti sayesinde iç denetim şirkete değer katan bir fonksiyon haline gelmiştir. İç denetçiler işletmenin maruz kalabileceği riskleri önceden tespit edebilecek ve gerekli risk değerlendirmelerini yapabilecek donanıma yetkinliğe sahip olmalıdır. İşletme içerisinde iç denetim faaliyetinin önemini vurgulamak için iç denetim ve risk yönetimi konularında eğitimler yaygınlaştırılmalıdır. Bağımsızlık ve tarafsızlık ilkelerine bağlı kalarak iç denetçiler şirkete nasıl değer katabileceği bilinciyle iç denetim faaliyetlerini yürütecek denetçiler yetiştirilmeli ve desteklenmelidir.

Özetle, iç denetim şirketlerin vazgeçilmez bir fonksiyonudur ve işletmelerin varlıklarını korumak ve işletmeye katma değer sağlamak amacıyla şirketin gelişmesi ve büyümesini destekleyen önemli bir fonksiyondur. İç denetim işletmede meydana gelebilecek risklerin erken tespit edilmesi, önlenmesi, meydana gelen risklerin yönetilmesi ve takibi açısından danışmanlık ve güvence hizmeti görevini başarıyla sürdürmektedir. İç denetim fonksiyonunun bağımsız ve tarafsızlık ilkelerini benimseyerek işletmeyi daha iyi seviyelere taşımak için faaliyetlerini sürdürdüğü unutulmamalıdır ve iç denetim birimine ve iç denetçilere gereken önem verilmelidir.

KAYNAKÇA

- Adilođlu, B. (2011). *İç Denetim Süreci ve Kontrol Prosedürleri*, İstanbul, Türkmen Kitapevi.
- Akkaya, G. (2011) “Risk Odaklı İç Denetim ve Risk Odaklı İç Denetim Planlamasında Risk Matrisinin Oluşturulmasına Yönelik Örnek Bir Uygulama”, *Yayımlanmamış Yüksek Lisans Tezi*, Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Enstitüsü
- Akpınar, M. (2012). Denetim Anlayış ve Metodolojisinde Deđişimin Adı: İç Denetim, *ZKÜ Sosyal Bilimler Dergisi*, 7(14), 285-305
- Akpınar, Y. (2010). 610 Nolu Uluslararası Denetim Standardı Hükümleri ile Türkiye Uygulamaları Çerçevesinde İç Denetim ve İç Denetim Çalışmaları, *Trakya Üniversitesi Sosyal Bilimler Dergisi*, 12(2),174-200
- Aksoy, T. (2018). Risk Odaklı İç Denetim Sürecinde Operasyonel Risklerin Belirlenip Ölçülmesine Yönelik Uygulamalı Bir 3x5 Risk Matrisi ve Risk Analiz Anket Formu Önerisi, *Mali Çözüm*, 28(147): 37-77
- Aktaş, E. (2015) “İç Denetim ve Risk Yönetimi İlişkisi”, *Yüksek Lisans Tezi*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü
- Akyel, R. (2010). Yönetimde İç Kontrol, İç Denetim ve Dış Denetim Fonksiyonlarının Birbirleri ile İlişkileri ve Türk Kamu Yönetiminde Uygulamalarının Deđerlendirilmesi, *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 19(3), 1-21
- Akyürek, B. (2006) “Bankacılık Sektöründe Risk Odaklı İç Denetim Sistemi, *Doktora Tezi*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

- Anadolu, Z. (2015) “Yeni Türk Ticaret Kanunu Kapsamında Risk Odaklı İç Denetim ve Meslek Mensupları Üzerine Bir Anket Çalışması”, *Yüksek Lisans Tezi*, Okan Üniversitesi Sosyal Bilimler Enstitüsü
- Atagan Çetin, A. (2016) “Kurumsal Sürdürülebilirliğin Sağlanmasında Risk Odaklı İç Denetim ve Bir Araştırma”, *Yayınlanmamış Doktora Tezi*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü
- Bakkal, H., Tunç, İ. ve Kasımoğlu, A. (2016) *İç Kontrol ve Kurumsal Risk Yönetimi*, İdeal Kültür Yayıncılık, İstanbul, 2016,
<https://0-web-s-ebsohost-com.opac.bilgi.edu.tr/ehost/ebookviewer/ebook?sid=86af8f42-7917-4a02-bb6d-f286b367dc28%40redis&vid=0&rid=1&format=EB>
- Baltacı, A. (2019). “Nitel Araştırma Süreci: Nitel Bir Araştırma Nasıl Yapılır?”, *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 5(2), 368-388
- Bektaş, U.C. (2019) “Uluslararası İç Denetim Standartları Çerçevesinde Risk Odaklı İç Denetim ve Uygulamaya Yönelik Bir Araştırma”, *Yüksek Lisans Tezi*, Ufuk Üniversitesi Sosyal Bilimler Enstitüsü
- Bozkurt, C. (2010). Risk, Kurumsal Risk Yönetimi ve İç Denetim, *Denetim*, (4), 17-30
- Teolupus, İç Denetim İle Bağımsız Denetim Arasındaki Farklar Nelerdir?, 2017, Çevrimiçi, 15 Aralık, 2019
<https://teolupus.com/teo/ic-denetim-ile-bagimsiz-denetim-arasindaki-farklar-nelerdir>
- Can, E.G. (2021) “Risk Odaklı İç Denetim: Risk Değerlendirmesi Üzerine Örnek Bir Uygulama”, *Yüksek Lisans Tezi*, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü

Celayir, D. (2021), *İç Denetim ve Risk Değerlendirme*, Hiperyayın, İstanbul, 2021

<https://0-eds-s-ebsohost-com.opac.bilgi.edu.tr/eds/ebookviewer/ebook?sid=23802d34-5bdf-49c4-81da-98403a832de5%40redis&vid=0&format=EB>

COSO, COSO Enterprise Risk Management, Integrating with Strategy and Performance, 2007, Çevrimiçi, 5 Mart, 2021

<https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf>

COSO, COSO Enterprise Risk Management, Applying Enterprise Risk Management to Environmental, Social and Governance-related Risks, 2007, Çevrimiçi, 5 Mart, 2021

<https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf>

COSO, COSO Releases Enterprise Risk Management-Integrated Framework, 2004, Çevrimiçi, 16 Şubat, 2019,

<https://www.coso.org/Documents/PR-09292004-ERM-Integrated-Framework.pdf>

COSO, Enterprise Risk Management -Integrated Framework, 2004, Çevrimiçi, 16 Şubat, 2019,

<https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf>

COSO, Internal Control – Integrated Framework Executive Summary, 2013, Çevrimiçi, 16 Şubat, 2019,

https://na.theiia.org/standards-guidance/topics/documents/executive_summary.pdf

Çağlayan, İzzet, *Kurumsal Risk Yönetimi-COSO 2017*, 21.05.2018, Çevrimiçi, 11 Ocak 2020

<https://www.slideshare.net/IzzetCAGLAYAN/kurumsal-rsk-ynetm-coso2017>

Çevikbaş, R. (2011). Türkiye’de İç Denetim Kurumu, *İdare Dergisi*, (427-472),47-67

Çidem, İ. (2021) “Katılım Sigortacılığı Şirketlerinde Risk Odaklı İç Denetim: Bir Vaka Çalışması”, *Doktora Tezi*, Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü

Deloitte, Uzun, A. K., Yeni Türk Ticaret Kanunu’nda İç Denetim Üzerine Düzenlemeler, 2012, Çevrimiçi, 15 Aralık ,2019

<https://www.verginet.net/dtt/1/yeni-ttk-ic-denetim.aspx>

Demirbaş, M. (2005). İç Kontrol ve İç Denetim Faaliyetlerinin Kapsamında Meydana Gelen Değişimler, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, (7), 167-188

Derici, O., Tüysüz, Z., & Sarı A. (2007) Kurumsal Risk Yönetimi ve Sayıştay Uygulaması, *Sayıştay Dergisi*, (65), 151-172

Doğan, Ö. (2011) “Kobilerde İç Kontrol Sisteminin Yeri ve Risk Odaklı İç Denetim: Denizli İli Uygulaması”, *Yüksek Lisans Tezi*, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü

Duran, E. (2013) Kamu İdarelerinde Kurumsal Risk Yönetimi Uygulamaları, T.C. Çevre ve Şehircilik Başkanlığı Mali Hizmetler Uzmanlığı Araştırma Raporu, Çevrimiçi, 25 Haziran, 2022,

[https://webdosya.csb.gov.tr/db/strateji/editordosya/ErdalDURAN-Kamu Idarelerinde Kurumsal Risk Yonetimi Uygulamalari\(4\).pdf](https://webdosya.csb.gov.tr/db/strateji/editordosya/ErdalDURAN-Kamu%20Idarelerinde%20Kurumsal%20Risk%20Yonetimi%20Uygulamalari(4).pdf)

Göğüş, S.E.H. (2012). *Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi*, İstanbul, Türkmen Kitapevi

Görener, Ö. (2010) “Risk Odaklı İç Denetim: Olasılık-Etki Analizi Çerçevesinde Bir Uygulama”, *Yüksek Lisans Tezi*, Yıldız Teknik Üniversitesi Sosyal Bilimler Enstitüsü

<https://icdenetim.ktb.gov.tr/yazdir?B2E057812BFE8E614E7D28626B5DBAE5>

Güler, A. ve Arkin, A.K., (2018) COSO 2017 Kurumsal Risk Yönetimi Çerçevesine Kontrol Öz Değerlendirme Yaklaşımıyla Bakış ve Bir Kurum Uygulaması-I, *Denetim Dergisi*, (18), 45-62

IIA, (t.y.), Çevrimiçi, 2 Ocak, 2019,

<https://global.theiia.org/about/about-the-iaa/Pages/About-The-Institute-of-Internal-Auditors.aspx>

IIA, The Institute of Internal Auditors, Standards & Guidance, Turkish Translations, (t.y.), Çevrimiçi, 1 Ocak, 2019,

<https://global.theiia.org/translations/Pages/Turkish-Translations.aspx>

İSMMMO, 2 Denetim Türleri, (t.y.), 35-42, Çevrimiçi, 21 Nisan, 2019,

<http://archive.ismmmo.org.tr/docs/yayinlar/kitaplar/130/2%20denetim%20turleri.pdf>

İSMMMO, İç Denetime Genel Bakış, 2015, Çevrimiçi, 27 Mart,2019,

http://archive.ismmmo.org.tr/docs/YAYINLAR/kitaplar/ic_denetim_2015.pdf

İSMMMO, “Küresel Riskler ve Denetim” Şirketlerde İç Kontrollerin Yeterliliğinde İç Denetimin Rolü, (t.y.), Çevrimiçi, 11 Ocak 2022

https://archive.ismmmo.org.tr/docs/SEMPOZYUMLAR/SEMPOZYUM_09/8%20paralel%20oturum%203/2%20ali%20kamil%20uzun.pdf

İstanbul Üniversitesi, İç Denetim Rehberi, 2013, Çevrimiçi, 21 Nisan, 2019

<http://cdn.istanbul.edu.tr/statics/icdenetim.istanbul.edu.tr/wp-content/uploads/2013/03/%C4%B0%C3%A7-Denetim-Rehberi.pdf>

Kamu Mali Yönetimi ve Kontrol Kanunu, 2003, Çevrimiçi, 21 Nisan, 2019

<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5018.pdf>

Karataş, Z. (2015). Sosyal Bilimlerde Nitel Araştırma Yöntemleri, "*Manevi Temelli Sosyal Hizmet Araştırmaları Dergisi*, 1(1) (2015), 62-80

Karlıdağ, G. Ö. (2020) "Risk Odaklı İç Denetim: Enerji Sektöründe Bir Uygulama", *Doktora Tezi*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü

Kaya, B. (2010) "Risk Odaklı İç Denetim ve Uygulaması", *Doktora Tezi*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü

Kızılboga, R., & Özşahin, F. (2013). Etkin Bir İç Kontrol Sisteminin İç Denetim Faaliyetine ve İç Denetçilere Katkısı, *Niğde Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 6(2), 220-236

Kışanlı, Y., Pehlivanlı, D. (2006). Risk Odaklı İç Denetim ve IMKB Uygulaması, *Muhasebe ve Finansman Dergisi*, (30), 75-87

Kurnaz, E. (2016) "Risk Odaklı İç Denetim Yaklaşımı: Türkiye'de Kamu Sektöründeki İç Denetçilere Yönelik Bir Araştırma", *Doktora Tezi*, Atatürk Üniversitesi Sosyal Bilimler Enstitüsü

Kurnaz, N. (2006) "Kurumsal Yönetim Ekseninde Risk Odaklı İç Denetim: Türkiye'nin 500 Büyük Sanayi İşletmesinde Risk Odaklı İç Denetim Uygulama Analizi", *Yayımlanmamış Doktora Tezi*, Dumlupınar Sosyal Bilimler Enstitüsü

Maliye Bakanlığı, Kamu İç Kontrol Rehberi, Risk Değerlendirme Standartları, Çevrimiçi, 25 Haziran, 2022, https://www.ktu.edu.tr/dosyalar/16_00_00_5d20f.pdf

Mandalas, M.D. (2019) “Kurumsal Risk Yönetimi Kapsamında Risk Odaklı İç Denetim Analizi; Marmara Bölgesindeki Devlet Üniversitelerine Yönelik Bir Araştırma”, *Yüksek Lisans Tezi*, İstanbul Aydın Üniversitesi Sosyal Bilimler Enstitüsü

Özbilgin, İ. G. (2010). Aracı Kurumların İç Kontrol Sistemi ve İlgili Düzenlemenin Değerlendirilmesi, *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 12(2), 219-242

Özbilgin, İ. G. (2012). Risk ve Risk Çeşitleri, *Bilişim Dergisi*, 7, 86-93

Özer, A. (2008). “Risk Odaklı İç Denetim ve Bir Uygulama”, *Doktora Tezi*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü

Pehlivanlı, D. (2008) “Kurumsal Risk Yönetimi Temelli İç Denetim ve Türkiye Uygulamaları”, *Doktora Tezi*, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü

Pehlivanlı, D. (2020). “Kurumsal Risk Yönetimi”, *MÜSİAD*, Çevrimiçi, 19 Şubat, 2022,

https://www.musiad.org.tr/uploads/yayinlar/yonetim-kitapligi/yonetim-kitapligi-pdf/kurumsal_risk_yonetimi.pdf

PRM Finans, Aracı Kurumlarda Uygulanacak İç Denetim Sistemine İlişkin Esaslar Hakkında Tebliğ, Seri V, No:68, 17 Temmuz 2003, Çevrimiçi, 19 Mart, 2019,

<https://www.prmfinans.com/seri-v-no-68-araci-kurum-ic-denetim>

Saruhan, B.K. (2017) “Risk-Based Internal Audit and Developing a Risk Matrix For Audit Planning of a Bank”, *Yüksek Lisans Tezi*, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü

Sevim, Ş., & Eliuz, A. (2007). Denetim Komitelerinin İç Denetimin Etkinliği Üzerindeki Roller ve İMKB’de Bir Araştırma, *Muhasebe ve Finansman Dergisi*, (36),60-70

T.C. Hazine ve Maliye Bakanlığı, İç Denetimin Faaliyet Alanı, (2006), Çevrimiçi, 21 Nisan, 2019,

<https://www.hmb.gov.tr/ic-kontrol-okuma-listesi>

T.C. Kültür ve Turizm Bakanlığı, Uluslararası Meslek Kuruluşları, (t.y.), Çevrimiçi, 22 Ocak, 2019

<https://icdenetim.ktb.gov.tr/yazdir?B2E057812BFE8E614E7D28626B5DBAE5>

Tanç, A. (2009) “Risk Odaklı İç Denetim Yaklaşımı ve Tekstil Sektöründe Bilgisayar Destekli Bir Uygulama”, *Doktora Tezi*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü

Taşar, M. (2019) “Yatırım ve Kalkınma Bankalarında Risk Odaklı İç Denetime Yönelik Uygulama Önerisi”, *Yüksek Lisans Tezi*, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Tıraş, Z. (2020) “KOBİ’lerde Risk Odaklı İç Denetim: Bir Uygulama”, *Yüksek Lisans Tezi*, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü

TİDE, (t.y.), Çevrimiçi, 18 Şubat, 2019,

<https://www.tide.org.tr/page/1/Hakkimizda>

TİDE, Etik Kuralları ve Etik Kurul Yönetmeliği, (t.y.), Çevrimiçi, 1 Ocak, 2019,

https://tide.org.tr/uploads/news/Tide_Etik_Kurul_Yonetmeliği_26032011.pdf

TİDE, IIA Uluslararası İç Denetim Standartları, Mesleki Uygulama Çerçevesi Kapsamında Uluslararası İç Denetim Standartları (Standartlar), 2017, Çevrimiçi, 7 Ocak 2022

<https://www.tide.org.tr/file/documents/pdf/UMUC-2017-updated.pdf>

TİDE, İç Denetim, İçgörü ve Nesnellik, (t.y.), Çevrimiçi, 1 Ocak, 2019,

https://www.tide.org.tr/file/documents/pdf/IIA_Ic_Denetimin_Paydaslar_Icin_Degeri_Detay.pdf

Tokkder, Risk Odaklı İç denetim Modellemesi, 2011, Çevrimiçi, 21 Nisan, 2019,

<https://tokkder.org/tokkder-dergi/1080>

Türedi, H., Zor, Ü. Ve Gürbüz, F. (2015). Risk Odaklı İç Denetim, *Muhasebe ve Finansman Dergisi*, 1-20

<https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6102.pdf>

Usul, H. Ve Mizrahi, R. (2016). *Risk Odaklı Denetim*, Ankara Detay Yayıncılık

Uygulamaları”, *Doktora Tezi*, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü

Uysal, M.C. (2017) “Kamu Kurumlarında Risk Yönetimi ve Risk Odaklı İç Denetim: Bir Model Önerisi”, *Doktora Tezi*, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü

Yahşi, Fahrettin (2014) “Katılım Bankalarında Risk Odaklı İç Denetim ve Bir Model Önerisi”, *Doktora Tezi*, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü

Yelken R. (2019) “Holdinglerde Risk Odaklı İç Denetim ve Bir Uygulama”, *Yüksek Lisans Tezi*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü

Yılmaz, G. (2018) “Otel İşletmelerinde Risk Odaklı İç Denetim ve Bir Uygulama”,
Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü



EKLER

Ek 1: A Katılımcısı Mülakatı

- Yaşınız: 35
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 12 yıl
- Kurumunuzda çalışma süreniz: 3,5 yıl
- Kurumunuzun sektörü: Lojistik, sigortacılık, depolama
- Kurumunuzun çalışan sayısı: 1.200-1500 arası

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Şu an iki kişi. Yakında üç kişi olacak.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Yönetim kuruluna, Yönetim Kurulu Başkanı ve Başkan Yardımcısı'nın olduğu bir Denetim Komitesi'ne bağlıyız.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Süreç bazlı denetimler yapıyoruz. İnsan Kaynakları süreci üzerinden örnek vereyim. İnsan Kaynakları bordro işlemleri, İnsan Kaynakları mutabakat süreçleri, personel işe giriş süreçleri ve kariyer planlama süreçleri gibi bizim böyle süreç ağacımızın altında bu süreçlere dair süreçlerdeki politikalara, talimatlara incek işlem adımlarına dair risk değerlendirmelerimiz var, risk öngörülerimiz var. Planımız da buradaki en yüksek odaklı en yüksek puana, kat sayıya bağlı, risklere odaklı denetim planı oluşturmak. Yani şöyle bir şey olabilir bizim planımızda, İnsan

Kaynakları işe alım denetimi. Eğer ki o alanda çok mevcut operasyonumuzda, işleyişimizde çok yüksek risk gördüysek İnsan Kaynakları herkesçe anlaşılabilir olduğu için İnsan Kaynakları üzerinden örnek veriyorum ama bizim operasyonlarımız zaten çok büyük. Asıl odağımız zaten operasyonel denetim. Ayrıca yayınladığımız raporların aksiyonlarını yönetim kurulunu da bilgilendirecek şekilde takip ederiz. Takip denetimleri yaparız çünkü aksiyon planında mutabık kalıyorsunuz denetim planlarında ve bunların bir 'deadline'ı oluyor. O 'deadline' geçtikten sonra da aksiyon alınıp alınmadığını da takip etmeniz gerekiyor denetim birimi olarak. Genel olarak denetim metodolojimiz bu ve tabii denetim sonrasında biz risk envanterimizde bir değişiklik söz konusuysa onların da güncellemesini yapıyoruz. Yani denetimden önce çok yüksek düzeyde öngördüğümüz bir riskin denetimde orta düzeyde olduğunu görme ihtimalimiz de varken denetimden önce orta düzey bir riski de denetledikten sonra çok yüksek dolaylarına da çıkarabiliyoruz. Oradaki işlem hacmini ve süreci denetimle birlikte daha net anladıktan sonra dolayısıyla böyle sürekli bir dirsek teması halinde olduğumuz risk odaklı bir denetim yapımız var.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Ortalama bir süreç için iki kişilik, üç kişilik bir denetim ekibi için 20-30 iş gününü kapsayan bir denetim programı hazırlıyoruz. Sonrasında bu bulgularımızı bir denetim raporu haline getirip süreç sahipleriyle müzakere ederiz. Nasıl çözeceğimize dair sadece denetleyip kenara çekilmektense nasıl çözüleceğine dair katma değerli öneriler geliştirmeye çalışarak raporumuzu tamamlar ve yönetim kuruluna sunarız. Sonrasında da yayınladığımız bu raporların aksiyonlarını Yönetim Kurulunu da bilgilendirecek şekilde takip ederiz.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Destek fonksiyonları da risk kat sayılarına göre planımıza dahil ediyoruz ama asıl alanımız tamamen işte 'saving' ve şirketin aktiflerine etki eden, satışlarına etki

eden, cirosal anlamda büyük getiri sağlayan alanlar, kalemler. Dolayısıyla işte operasyonlardan belli süreçler, yüksek risk düzeyine sahip süreçler seçerek bunların nasıl işlediğine dair, kurumsal talimatlara uygun ilerletilip ilerletilmediğine dair, o belirlediğimiz risklerde aksiyonların alınıp alınmadığına dair, düzeltici faaliyet alanları olup olmadığına dair ya da o süreçleri yönetenlerin bir kontrol zafiyetleri olup olmadığına dair, bir usulsüzlük ihtimali olup olmadığına dair gibi böyle belli denetim teknikleri ve standartlarını referans alarak her alana tabi kaynaklarımızın yeterli olduğu ölçüde, her sürece denetim gerçekleştirmeye çalışıyoruz. Metodolojik operasyonel ve finansal denetim sürecinin metodolojik olarak bir farkı yok eğer ki denetim açılış toplantısı ile başlar ve risk değerlendirmeleri ile o sürece dair politikaların, talimatların, prosedürlerin, geçmiş dönem raporların incelenmesiyle ve onların risk değerlendirilmesinin alınmasıyla devam ederse. Sonunda ekibimiz denetim programı hazırlayarak o hangi işlem adımında hangi denetim testini uygulayacağını planlar, denetim planlamasını yapar ve denetimine başlar.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Şöyle zaten en öncelikli gayemiz riskleri öngörebilmek bu risklerin çözümüne ilişkin düzeltici aksiyonlar geliştirebilmek bu düzeltici aksiyonlarda süreç sahipleriyle belli bir aksiyon planında mutabık kalarak onların hayata geçmesini sağlamak. Eğer ki bu başarıyı eksiksiz bir şekilde denetimlerinizde gösterirseniz yani bir düzeltici aksiyonların, mutabık kalınan düzeltici aksiyonların hayata geçirilmesi noktasında eğer ki bunları uygulatabilirsanız firmalardaki bu zor bir hadisedir, tamamen önleyebilirsiniz. Hatta orada risk yönetimlerin risk iştahı, risk alma yatkınlığı da belirleyicidir. Yani sizin için iç denetim departmanı için risk olan bir konu yönetimin stratejisi olabilir. Risk almak bir yönetsel strateji olabilir. Riski kabul de edebilir insanlar, ben bu riski alıyorum çünkü benim ciro hedefim var diyebilir ya da farklı hedeflerim var, stratejik hedeflerim var diyebilir ya da riski

paylaşmak isteyebilir. Başka fonksiyonlardan ya da üçüncü kişilerden alacağı işte atıyorum bir sigorta yaptırmak riski paylaşmaktır. Dolayısıyla o noktada risk yaklaşımı da önemli olmak üzere eğer riskten kaçınan bir şirkette, yönetim profilinde çalışıyorsanız yani riski kesinlikle kabul etmeyen ucunda bir ciro hedefi dahi olsa pazar hedefi dahil olsa risk kesinlikle almak istemeyen bir risk profili ile çalışıyorsanız ve aksiyon aldırma hızınızda aksiyon aldırma kabiliyetinizde iyiye biz çok yüksek olarak öngördüğümüz, çok riskli olarak öngördüğümüz birçok faaliyetin bu aksiyonları almaya başlamasıyla risk kat sayısının çok çok düştüğünü ve şirketinde bu öngördüğümüz risklere çok fazla maruz kalmadığını görüyoruz. Buradaki önemli olan kriter, toparlayayım, aksiyon aldırma kabiliyetiniz, hızınız, yetkinliğiniz, bir de yönetim risk yaklaşımı ve risk iştahıdır.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Risk yönetimi, riskin esas sorumlusu risklerin süreç sahipleri. Bu riskleri yönetecek öncelikli aksiyonları alacak takip edecek birincil sorumlu o süreçlerin sahipleri bunlar. Direktör seviyesi olabilir, Genel Müdür seviyesi olabilir, o şirketlerin yapılanmalarına göre değişir ama esas sorumlu o sürecin sahibi. Sonrasında biz o riskleri, ortaya döktüğümüz riskleri yönetebilip, yönetemediğine dair bir güvence veririz süreç sahiplerine. Dolayısıyla bizim sorumluluğumuz aslında ikincil sorumluluk. Yani riskleri çıkarırız, aksiyon planını, yolu gösteririz ki bu danışmanlık fonksiyonudur iç denetimin. O aksiyonları almak, yönetmek, o riskleri kabul etmek ve tabiri caizse alması gerekiyorsa almakta süreç sahibinin birincil sorumluluğudur. Bizim buradaki sorumluluğumuz ikincil ama yine de biz bu süreçlerde aktif bir şekilde rol alıyoruz. Aksiyonların alınması noktasında rol alıyoruz çok ikincil sorumluluk gibi davranmıyoruz aslında. Dolayısıyla direkt olarak sorumluyuz diyebilirim aslında bu şirket içinde cevap vermem gerekirse.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Tabii ki, ben aynı zamanda şirkette iç eğitmenim ve eğitim verdiğim alanlarda şirket içerisinde risk yönetimi ve iç denetim iki alanda periyodik olarak personellere pandemiye kadar fiziki giderek yapıyorduk bu eğitimi ama pandemiden sonra artık online eğitimler yapıyoruz periyodik olarak insanlara.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Gözlem, soruşturma, analitik prosedürler, döküman incelemesi, fiziki sayım, kayıtların kontrolü genel olarak bu yöntemleri kullanıyoruz. En fazla analitik prosedürlerimiz, süreçler eğer olgun bir süreç seviyesine sahip denetim gerçekleştiriyorsak işte döküman inceleme verileri, biraz böyle suistimale konu olan denetim varsa soruşturma, mülakat yapma, ifade, personellerden ifade alma, o ifadeleri karşılaştırma gibi tatsız noktalara da vardırabiliyoruz. Genel olarak bunları kullanıyoruz test olarak.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Yaklaşım şöyle, genellikle kabul edilir tabii ki buradaki denetim sonuçları. İçeride öyle bir kültür vardır, denetim kültürü vardır. Çünkü bu firma çok uluslu global ölçekteki müşterileri olan bir firma dolayısıyla bu ölçekte müşterilerle iş yaptığınızda belli kurumsal standartlara haiz olmanız gerekiyor. Belli o müşterilerin gerekliliklerini karşılıyor olmanız gerekiyor. Ve bu gerekliliklerin karşılanıp, karşılanmadığına ilişkin sürekli müşteriler tarafından denetlenen bir şirket burası. Dolayısıyla içeride denetim kültürü var, iç denetim kültürü bizimle birlikte oturmaya başlasa da dışarıdan denetime çok yabancı bir firma değil. Dolayısıyla denetime yaklaşım ve sonuçlarına yaklaşım tabii ki daha ılımlı ve olumlu sonuçları kabul etmek. Aksiyon planlarını öncelikle iş planlarına almak ve herhangi bir süreç

sahibiyle ve yönetim kuruluyla iletişim halinde olarak da bir problemimiz bulunmuyor. Biz denetim raporunu yayınlarız. Aksiyonu sahibine aksiyonları bir platform üzerinden yani artık biz dijital denetime geçtik, çok böyle word, excel üzerinden devam etmiyoruz. Bir tane program kullanıyoruz bunun için. O mutabık kaldığımız aksiyonları o programa girip süreç sahiplerine ‘deadline’ vererek atadığımızda zaten aksiyonların durumunu sorgulayan bir yapay zeka ile çalışan bir program bu. Sıkı bir şekilde takip ediyoruz. Dolayısıyla o noktada bir olgunluğa eriştirebildik insanları ama çok kolay değil, yeni bir iç denetim kurduğunuzda çok böyle iki üç sene içerisinde sonuç alabileceğiniz hadiseler değildir bunlar, aldık.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Aylık olarak rutin toplantılarımız olur. Onun dışında biz zaten her ay bir rapor yayınlıyoruz gibi denetim raporu yayınlıyoruz gibi bir takvimimiz var, aylık diyebiliriz.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Güzel soru, performans hedeflerimiz şöyle bir bağımsız denetim firması denetimin verimliliğini denetliyor olması beklenir, kitaplarda bu yazar ama ben üç senedir buradayım, bir bağımsız denetim firması burada iç denetim ne yapıyor diye gelip bizi denetlemedi. İçerideki etkinliğimizi ve verimliliğimizi bir performans yönetim sistemimizle takip ediyoruz. Yönetimin de vermiş olduğu belli bir performans hedeflerimiz var. Hem o hedefler üzerinden takip ediyoruz hem de biz denetimin etkinliğini ve verimliliğini her denetimin sonunda o denetlenenlere bir anket vererek ölçmeye çalışıyoruz. Yani siz kendinizi nasıl ölçüyorsunuz dersiniz bizi dışardan ölçmeleri en makulü ama biz de içeride hem ekibe hedef vererek hem departmana hedef vererek ve o hedeflerin belirli periyotlarda takip edilmesi şeklinde hem de her denetimin bir süreç sahiplerine denetime ilişkin etkinlik ve verimlilik anketi yaparak ölçmeye ve takip etmeye çalışıyoruz.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Tamamen şirketlerin denetime bakış açısıyla alakalı yani şirketin yönetiminin denetimden bu fonksiyondan ne beklediğiyle alakalı yani sizden bir şeyleri tespit eden ve işte icrai fonksiyonları kontrol altında tutan ve korkutan bir yapı olmanızı da bekleyebilirler ancak sizden onlarla daha iş birliği halinde ve verimlilik esasıyla çalışan bir danışmanlık rolü bekleyebilirler. Bu manada iç denetimin sürekliliği tamamen yönetimin bu fonksiyona bakış açısıyla alakalı. Polislik de yapmanızı isteyebilir, danışmanlık da yapmanızı isteyebilir. Süreklilik tabiki sağlanmalı ve dünyaya ayak uydurmalı iç denetim. Bu da geleneksel iç denetim anlayışıyla birkaç jenerasyon içerisinde yok olacaktır. Çünkü artık dijital denetimler başlıyor. Bu denetçinin tespit edebileceği şeyleri tespit eden yapay zeka teknolojileri geliştiriliyor. Bir kişi olarak belki de birine ihtiyaç olmayacağı bir dünyaya giderken sürekliliğin sağlanması için bu dünyaya ayak uydurulması gerekiyor.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Faydası şöyle bir kere artık denetim evrildi, biz ilk bu mesleğe başladığımızdaki yaklaşım yok artık denetimde ve bizden sonra da muhtemelen çevik denetim, uzaktan denetim gibi risklerin de değişmesi ile birlikte, çalışma modellerinin de değişmesiyle birlikte çok kısa süre içerisinde başka bir evrilme geçirecektir diye düşünüyorum. Bizim mesleğe başladığımızdaki gibi artık bir şeyleri denetle ve onların sonuçlarını yönetme ya da işte bağlı olduğunuz fonksiyonlara raporla sonra da kenara çekil değil artık denetimden beklenen. Ciddi manada, global ölçekte artık risklerin artmaya başladığı bir dünyada yaşıyoruz ve bu böyle bir dünyada da risklerin takip edilmesi, yönetilmesi ve seçilmesine ilişkin katma değerli öneriler ve aksiyonlar bekliyorlar artık yönetimler iç denetimden. Yani sadece tespit eden konumundan çıkarak, değer katan bir faaliyet haline gelmesi net olarak bekleniyor ve bu beklenti de riskler değiştikçe ve büyüdükçe de artık tespit eden değil de düzelter noktaya evrildi iç denetim. Biz de bu manada her zaman bu noktaya gelmeden iç denetim ben her zaman değer katmasını beklerim, bir şeyi tespit

etmenin çok da zor olmadığını, önemli olan onu ortadan kaldırmak olduğu yaklaşımıyla bu mesleği yıllardır icra ediyorum. Dolayısıyla iç denetimin en büyük faydası bence bir şeylerin röntgenini çekmek ya da ortaya dökmek değil, onların düzeltilebileceğine ilişkin yol haritası çizmek bu yetkinliklere sahip olmalı iç denetçi bence. Evet inceleme soruşturma denetleme ve bu metodolojiye hakim olmakla birlikte yol gösterici de olabilmeli ve tabiri caizse bir şeyi tespit ediyorsanız onun bir daha olamamasına ilişkin neler yapılabilir olacağını da bilmelisiniz. Bana en büyük faydası iç denetimin budur, yol göstericilik ve danışmanlık faaliyetidir. Çünkü insanlar yönetimler fonksiyonlar kendi yaptıkları işlerin farkında olmayabilirler. İç denetçiler her alana dokunarak, girerek her alandaki karanlık noktalara ışık tutarak insanları silkeleyebilir ve bu da saygınlık yaratır iç denetçiler için şirkette. En büyük faydası bu.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok. Hemen hemen her şeyi konuştuk. Hemen hemen tüm konuların üzerinden geçtik.

Ek 2: B Katılımcısı Mülakatı

- Yaşınız: 30
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 6 yıl
- Kurumunuzda çalışma süreniz: 6 yıl
- Kurumunuzun sektörü: Gaz
- Kurumunuzun çalışan sayısı: Beyaz yaka 700, tesis ve saha çalışanları ile birlikte yaklaşık 1.300 diyebilirim.

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Biz 3 kişilik bir ekibiz, Denetim Müdürü'müz var, 2 tane de çalışan olarak 3 kişilik bir ekiple çalışıyoruz. Şöyle bizim aslında direk denetim kadrosunda olmayan ama dışarıdan süreci, işleri geliştirmeye yönelik başka birimlerimiz de var. Bunun haricinde bağlı olduğumuz holdingin bir denetim ekibi var ve yılda bir kere ya da iki kere mutlaka holding denetim ekibi tarafından da şirketlerimiz denetleniyor. Dolayısıyla aslında kadro olarak 3 kişi işlere yetişebiliyoruz. Daha çok kişi olsa daha çok detaya bakılabilir mi, tabii ki bakılabilir. Ama şu anda da aksayan bir şey olan bir durum söz konusu değil, üç kişi yeterli.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Üst yönetime bağlı, Yönetim Kuruluna.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleştiriyor?

Şöyle bizim bir zorunlu demiyim de mecburen yaptığımız, yapmak zorunda olduğumuz denetimlerimiz var. Bir de bizim planladığımız denetimlerimiz oluyor. Yılın belli periyotlarında mutlaka muhasebe kayıtlarının üzerinden geçeriz. Muhasebe verileri üzerinden, hesap hareketleri hesaplar üzerinden denetim yaparız. Bunu iş yoğunluğumuza göre değiştirebiliyoruz. Onun haricinde bizim bir de planlı denetimlerimiz oluyor. Kendimize bunları hedef ediniyoruz ve şirketin hangi birimlerini denetleyeceğimizi yıl başında planlıyoruz. Yıl içerisinde de zaman buldukça bu denetimlerimizi gerçekleştiriyoruz. Süreç bazlı, departman bazlı diyebiliriz. İşletmemizin iştirak şirketleri var, iştirak şirketleri bazlı denetimler yapabiliyoruz. Geçtiğimiz yıl baktığımız şeylere bir daha bakmıyoruz. Bakmadığımız ya da yeni yatırımlar yapılan ya da büyük masraflar olduğunu düşündüğümüz, bildiğimiz toplantılarda ya bu konulara hiç bakılmadığını duyduğumuz konuların üzerine eğiliyoruz. Biz birimlerin bütün faaliyet

toplantılarına katılıyoruz dolayısıyla her birimin gündeminde ne var, bunun maliyet kalemlerini ne oluşturuyor, toplantılardan duyuyoruz. Bunlar da bize yol gösteriyor ve hangi birimi neye göre denetlememiz gerektiğini denetimin başında karar veriyoruz, yıl içinde o denetimleri yapıyoruz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Yıl başında biz hangi birimlere odaklanmamız gerektiğini belirliyoruz. Üç ayda bir yaptığımız oluyor, dört ayda bir yaptığımız, altı ayda bir yaptığımız oluyor ama yıl içinde mutlaka üç ya da dört kez mutlaka denetim yapıyoruz. Biz yıl başında plan belirlerken bağlı olduğumuz holdingin denetim takvimini öncelik alıyoruz. Onların denetime geldiği dönemlerde biz de onlara eşlik ediyoruz. Hem yardımcı oluyoruz, sorularını cevaplıyoruz, zaten hali hazırda baktığımız konulara onlar tekrar vakit kaybetmesinler diye hem de onların çok vakti olmuyor, bir ay kadar kalabiliyorlar, bazı konular çok uzun soluklu olabiliyor. Onların bir aşamaya getirdiği şeyi bizim sonuçlandırmamız gerekiyor. Dolayısıyla biz öncelikle bağlı olduğumuz holdingin denetim takvimine onların planına uyuyoruz.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

İlk olarak bir departmanı belirledik, bu departmanı denetleyeceğimize karar verdik. Bazı verileri, muhasebesel verileri direkt muhasebeden çalıştığımız kişilerden alabiliyoruz. Onun haricindeki verileri kendimiz çekiyoruz. Biraz daha objektif olsun diye, müdahale edilemesin diye SAP'den bu tarz verilerin eğitimlerini aldık, raporları öğrendik, sadece 'transaction' kodu girmemiz yeterli. Kendimiz önce verileri alıyoruz. Verileri aldıktan sonra verileri önce kendimiz inceliyoruz. Hangi alanlara, hangi masraflara odaklanmamız gerektiğini belirliyoruz ve konu başlıklarına ayırıyoruz. Departmanın İK yönetimi, departmanın bütçeye uyumu, yaptığı yatırımların fizibiliteye uyumu ya da bu yapılan yatırımın bize katma değeri

ya da bir ihale, bir satın alma gibi bir süreç varsa bunun gerçekten objektif ve doğru bir şekilde uygulanıp uygulanmadığı gibi böyle çeşitli kriterlere ayırıyoruz. Sonrasında konunun ilgilileriyle görüşmeye başlıyoruz. Elimizdeki veriler üzerinden de görüşebiliyoruz, yerinde ziyaret de yapabiliyoruz. Mesela satın alma birimimiz Gebze’de, fiili bir ürünü görmemiz gerekiyorsa ya da tesise yapılmış bir şeyse tesise gidip yerinde görüyoruz. Kıyaslıyoruz bu evrakta bu kadar diyor, gerçekten bu kadar mı? Bazılarını fotoğraflıyoruz, bazılarını dediğim gibi yerinde inceleyerek analiz ediyoruz. Sonrasında ilgili kişilerle, birimlerle yaptığımız kısa toplantılarla konuları neticelandiriyoruz. Sonrasında tespitlerimizi oluşturuyoruz. Bize göre birimle çatışabiliriz, aynı fikirde olabiliriz, fark etmez, tespitlerimizi bir rapor haline getiriyoruz ve bu raporu genel müdür ve genel müdür yardımcılılarıyla paylaşıyoruz. Sonrasında da hep birlikte bir değerlendirme toplantısı yapıyoruz. Ve o toplantıda birim de kendini ifade ediyor. Haklı oldukları yerleri, bize katılmadığı yerleri söylüyor, biz kendi eleştirilerimizi yapıyoruz. Sonrasında da Genel Müdür’le yaptığımız toplantıda alınan kararlara göre de bir aksiyon takip listesi oluşturuyoruz. Bu toplantıda şu kararlar alındı bu raporun sonucunda şu düzeltmeler yapılacak diye bir liste oluşturuyoruz ve yıl içerisinde o maddeleri birim yapmış mı, yapmamış mı diye kontrol ediyoruz. Ayrıca bağlı olduğumuz holding denetime geldiği dönemlerde biz de onlara eşlik ediyoruz, hem yardımcı oluyoruz sorularını cevaplıyoruz, zaten hali hazırda baktığımız konulara onlar tekrar vakit kaybetmesinler diye hem de onların çok vakti olmuyor, bir ay kadar kalabiliyorlar. Bazı konular çok uzun soluklu olabiliyor. Onların bir aşamaya getirdiği şeyi bizim sonuçlandırmamız gerekiyor. Onlar zaman zaman tesis ziyareti yapmak istiyor, onlara eşlik ediyoruz. Bunun haricinde dediğim gibi yılın belli dönemlerinde masraf denetimlerimizi yapıyoruz. Mizan, masraf, muavin bütün kayıtlarımızı alıyoruz, bir önceki yıllarla karşılaştırıyoruz. O çıkarımları yapıp tespitlerimizi ve analizlerimizi yapıyoruz ve o dönemi kapatıyoruz. Onun haricinde planlı denetimlerimizi aslında yaz dönemine denk getiriyoruz çünkü insanların yıllık izinde olduğu, bizden işin en az istendiği dönem yaz dönemi dolayısıyla kendi

işlerimize biraz daha vakit ayırabiliyoruz. Planlı denetimlerimizi Haziran-Eylül arasındaki döneme sıkıştırıyoruz. Eylül'den sonra biraz daha böyle bütçe, hedefler, hesaplar konuşulduğu bir dönem son üç ay. O dönemlere de biraz daha yıl içerisindeki eksik olduğunu düşündüğümüz şey varsa münferiden onlara bakıyoruz ya da Genel Müdür tarafından bize doğrudan atanan işler olabiliyor, spesifik bir şekilde şu konuya bakın, bu konu neymiş denebiliyor onlara bakıyoruz. Bütün bunların haricinde bize münferiden ihbar gelebiliyor, şikayet gelebiliyor, direkt bize gelebiliyor, Genel Müdür üzerinden gelebiliyor, holding üzerinden gelebiliyor. Bunlar hiçbir şekilde planlayamadığımız şeyler ve bunlar geldiğinde önceliklendirip, çözümlenemeyen gereken konular. Bunlar da aralara geldikçe bu planlı denetimlerimizin arasına da bu özel inceleme konularını yerleştiriyoruz ve denetimi neticelandiriyoruz. Bir yıllık akışımız bu şekilde oluyor. Denetim planı risk odaklı, daha çok yeni işlere odaklanıyoruz, yeni yatırımlara odaklanıyoruz, tutarı yüksek hacimli şeylere odaklanıyoruz. Riskin aslında bir güvenlik tarafı var; bir verimlilik tarafı, bir de fayda tarafı var. Bu ikisi eş mi, doğru mu, farklı açılardan bakmaya çalışıyoruz. Bir de bizim ekipte şöyle bir rol var. Benim mühendis olmam, ekipteki diğer arkadaşımızın da tamamen denetim kökenli olması, finans, banka denetimi yapmasıyla öyle bir tecrübeye alakalı, o biraz daha finans ve mali taraf kökenli, ben biraz daha süreç kökenli olduğum için birimiz mali taraftaki vergisel, hukuksal konuları incelemeye odaklı çalışıyor. Diğer tarafta süreç gerçekten verimli işliyor mu, burada verimsiz bir şey var mıyı anlamaya, tespit etmeye ya da büyük bir data varsa büyük bir veri varsa bunun için nasıl yorum yapabiliriz diye inceleleyen, analiz eden taraf oluyorum ben de. Aramızda böyle bir iş bölümü oluyor, buna göre belirliyoruz denetimde odaklanacağımız yerleri.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Şöyle bizim aslında kurumumuzun çok eski şirket olmasının etkisiyle çok temel konular zaten sistematik olarak kapatılmış kitlenmiş ve onay mekanizmalarına

bağlanmış durumda. Çoğu şey dökümanede edilmiş durumda yani siz aklınıza gelebilecek her türlü ekstrem bir örneği ‘qdms’ diye bir platformumuz var, orada süreçlerimizi tanımladığımız, prosedürlerini yazdığımız bir platform. Orada isim olarak arattığınızda karşınıza direkt döküman çıkabiliyor yani çoğu süreç riskli süreçler özellikle belli bir prosedüre belli bir onay mekanizmalarına bağlanmış, bazı alanlar kilitlenmiş. Bizim denetim yaparken fark ettiğimiz illaki konular oluyor.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Tabii ki, biz aslında tespit yapıp bırakan taraflar olmuyoruz, çözüm de getirmeye çalışıyoruz. Çözüm önerisi sunuyoruz ve yapılıp yapılmadığında gerekirse projeye liderlik yaparak takip ediyoruz. Bu risk ortadan kalktı mı, tekrarı oldu mu, geçmişe dönük bakıyoruz. Geçen yıl böyle bir tespit yapmıştık, bu yıl aynı durum yinelemiş mi, farklı bir şekilde önümüze gelmiş mi diye kontrollerimizi yapıyoruz ama dediğim gibi kurumumuzun çok eski bir şirket olmasının vermiş olduğu şekilde aslında süregelen bir denetim zaten var ve çoğu şey kapatılmış, çoğu şey standarda oturtulmuş durumda.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Bizim kalite biriminin altında iç denetçilerimiz var. Onlar aslında direk iç denetim gibi değil de tesislerin denetimi, bilgi güvenliği bazı evraksal konuların denetimine hazırlık olması amacıyla 30-40 kişilik bir ekipleri var. Çok farklı departmandan kişiler ve bunlar gönüllü olarak mevcut işlerinin yanında bu işi yapıyorlar ve yılda bir kez bizim dışardan mevzuatsal denetimlerimizin öncesinde onlar bir ay boyunca şirketin bütün birimlerini tek tek ziyaret edip denetliyorlar. Bilgi güvenliği konusunu biliyor muyuz, süreçlerimizin tamamı tanımlı ve sistemde güncel mi, sistemde olmayan bir süreç, tanımlanması gereken bir süreç var mı ya da sistemdeki süreçlere uyuluyor mu, riayet ediliyor mu, bu gerçek anlamda, fiili hayatta kullanılıyor mu yoksa 5 ay önce yazılmış ve orada kalmış bir şey mi, form varsa

formları nerede çıkartın bakalım şeklinde bir kontrolleri var. Doğrudan bizim olmasa bile böyle bir şirket içerisinde yapılanma var yılda en az bir kez mutlaka böyle bir denetim gerçekleşiyor.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Kullandığımız çok spesifik bir yöntem var diyemem ama biz büyük data'lara önem veriyoruz. Oradan da çok fazla tespitler yapıyoruz, kendimizi de bu alanda biraz daha geliştiriyoruz. Hani biraz daha şeyden ziyade konunun bizim önümüze gelmesinden ziyade biz bir şey çıkarmaya çalışıyoruz. Genellikle biz veriler üzerinden ilerliyoruz. Verileri kendimiz topluyoruz ve yansıtıyoruz, böyle dev ekranda inceliyoruz, analizlerimizi yapıyoruz sonrasında birime gidip soruyoruz. Aslında en başta birime gidip sen bu süreci nasıl yapıyorsun, nasıl yönetiyorsun gibi bir şey sormuyoruz. En başta biz inceliyoruz, kendimiz anlamaya çalışıyoruz sıfırdan. Çünkü biri anlattığında direkt onun bakış açısıyla bakıyormuş gibi oluyor. Biz kimseden bir şey duymadan, sıfırdan bir şekilde kendimiz anlamaya ve yorumlamaya çalışıyoruz. Gözümüze farklı gelen, absürt gelen şeyleri tespit ediyoruz. Birimle görüşmelerimizde de aslında direk somut bunların üzerinden ilerliyoruz. Böyle söylemiştin ama bak buradaki veride şöyle bir şey var diye. Bizim asıl güçlü olduğumuz yönümüz ya da kullandığımız teknik için bunu söyleyebilirim veri analizi sonrası birimlerle görüşmeler.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Şöyle bizim bir etik kurulumuz var bir de bunun yönetim kurulunda alınabilecek kararlarla ilgili belli maddelerin olduğu bir prosedürümüz var. Biz tespitimizi yaparız sonrasında İnsan Kaynakları müdürümüzün, hukuk müşavirinin, genel müdürün, ilgili birimin müdürü ve genel müdür yardımcısının olduğu bir toplantıda tespitimizi ortaya koyarız. Sonrasında biz kendi yorumumuzu da yaparız. Kişi kendi uyarı mı alması gerekiyor, sözlü uyarı mı, yazılı uyarı mı, iş akdi feshi mi, bu

konuda biz görüşümüzü bildiririz sebepleriyle birlikte. Sonra o etik kurul içerisinde bir değerlendirme yapılır ve herkes kendi görüşünü söyler ve ortak bir karar alınır ve bu karar uygulanır o toplantıdan çıkıldığı anda. Kişi ile ilgili de karar alınacaksa, tedarikçiyle ilgili birlikte çalıştığımız bir partnerle ilgili bir karar alınacaksa toplantı sonrası o etik kurulla birlikte alınan karar sonrası uygulanır.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Raporlama bizim bütün denetimlerimizde yapılır. Biz mutlaka hem geriye dönük kurumsal hafızayı tutmak için hem de hatırlamak için kendimiz geriye dönük bakmak için mutlaka raporu her sürecin sonunda yazıyoruz. Bu sadece tespit olmasa süreci özetleyen durum değerlendirmesi gibi bile olsa raporluyoruz. Ayda en az bir raporumuz çıkıyor.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Bizim denetim biriminin performansı direkt bir birim tarafından ya da genel müdür tarafından denetlenmiyor ama biz yaptığımız işlerin TL etkisini olabildiğince tutmaya ve çıkartmaya çalışıyoruz. Genel Müdür'le de hem hedef görüşmelerinde hem onun haricinde normal görüşmelerimizde kendisine söylüyoruz. Bu yaptığımız tespitler bunun karşılığında yıllık ya da önümüzdeki tüm yıllar için şu kadar TL'lik bir etkiyi biz aslında şirkete kazandırmış bulunuyoruz diye yani aslında dokunduğumuz birebir etki ettiğimiz şeyleri sunuyoruz genel müdüre ama direkt denetlenme denetimin etkinliğini denetleme gibi çok yok aslında. O biraz daha bağlı olduğumuz holdingin şeyi gibi oluyor bağlı olduğumuz holding şirketi denetlediğinde dolayısıyla bizi de denetlemiş oluyor.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Ben aslında buraya ilk geldiğimde 3 yıldan fazla çalışmam gibi düşünüyordum çünkü belli zaman sonra bir körlük olur ve bilgi gider bir süre sonra sürekliliğini kaybeder ve yeni bir yerde sıfırdan başlamak daha doğrudur diye düşünürdüm. Ama

şirket o kadar çok değişiyor, o kadar çok yeni iş geliyor ve bir önceki yılla bambaşka şeyler oluyor. Dolayısıyla aslında o sürekliliği hep korumamız gerekiyor çünkü hep bir hareket var hep yeni bir şey var aslında. Aynı şeyi tekrar tekrar her yıl denetlemiyoruz biz. Her yıl kendime yapacak yeni bir iş bulabiliyorum. Şirketinde aslında buna elverişli noktaları var, yeni yatırımları var, bununda etkisi olabilir ama illaki o sürekliliği korumamız gerektiğinin farkındayız çünkü her seferinde bilmediğimiz, aa buna hiç bakmamışız dediğimiz süreçler oluyor. O yüzden biz sürekliliği koruyoruz.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Birimlerin gerçekten belli bir zaman sonra belli bir körlükten sonra farkında olmadığı aslında bir bütçesi var, fiiliyatı var, onu çok dışardan baktıkça fark edemeyeceği şeyi küçük bir hatayı, bir faturadaki hatayı bu bir virgül hatası bile olabilir, bu o kadar çok böyle fatura giren ya da işlem yapan insanlar bunları fark edemeyebiliyor ama benim için sıfırdan dışardan baktığım için bunun bedeli bu kadar olamaz ya dediğim şeyler hep böyle o fatura hataları ya da tedarikçiden kaynaklı ürün hataları. Bunları tespit etmemize yarıyor. Hem dışardan bir göz olarak muhasebe kayıtlarının üzerinden geçmemiz insanların denetlendiği hissiyatını oluşturuyor ve insanlar bazı konularda daha temkinli davranmaya başlıyor. Çünkü denetlendiğini biliyor, bunun sorulacağını biliyor. En basiti girdiği bir fişin ona geri döneceğini biliyor bu yüzden daha kontrollü davranmaya başlıyor ve normalde bir insan birimde çalışan kendi birimiyle ilgili bilgi sahibi olabilir ama biz bütün birimleri denetlediğimiz için aslında böyle biraz daha yukardan bakma bakış açısıyla yaklaşabiliyoruz. Bir konuya çözüm getirmek ve yaptırabilmek günün sonunda gücümüz diğer birimlere göre daha fazla olabiliyor şirkete bu anlamda büyük katkıları olduğunu düşünüyorum. Genel birim için söylüyorum bunu çünkü farklı birimleri de bir araya getirebiliyorum. Farklı konulardaki parçaları da birleştirip biraz daha bütünsel bakışısıyla yaklaşabiliyorum. Bu anlamda faydası kesinlikle tartışılmaz diyebilirim yani.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Bilmiyorum sizin kariyer hedefiniz üniversitede mi devam edecek yoksa daha dışarıda reel hayatta bir çalışma hayatınız mı olacak, emin değilim ama ben denetimde çalıştığım için çok mutluyum, yaptığım işi de çok seviyorum. Dediğim gibi bundan sonra da kariyerimde denetim üzerinde olacak. Anlatırken de böyle bilmiyorum çok bir hazırlığım olmasa da böyle çok şey anlattığımı düşünüyorum, içimden geldiği gibi anlatmaya çalıştım, olduğu gibi anlattım, anlatmaya çalıştım, umarım teziniz için faydalı bilgiler vermişimdir.

Ek 3: C Katılıcısı Mülakatı

- Yaşınız: 29
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 5 yıl
- Kurumunuzda çalışma süreniz: 2 yıl
- Kurumunuzun sektörü: Spor
- Kurumunuzun çalışan sayısı: 1.900+

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

4 kişi, şöyle şöyleyim iç denetim faaliyeti ve bizim kurumumuz için yeterli. Çünkü aslında bizim şirketin altında 9 farklı şirket var. Biz bunun C1.Yönetim A.Ş. tarafındayız, mesela C2 Yönetim A.Ş. ayrı bir şirket aslında orada tamamen perakende, mağazacılık tüm bu AVM (alışveriş merkezi)'lerde gördüğün aklına gelebilecek mağazacılık sektöründeki devlerle yarışan bir şirket C2.Yönetim A.Ş.. Burada tamamen mağazacılık denetimi yapan ayrı bir iç denetim departmanı var. Bu şirket altında daha çok stokların sayılması, mağaza denetimleri gibi ya da lisans denetimleri gibi denetimler yapan ayrı bir departman var aslında orada. Diğer

tarafında bizim C1 Yönetim A.Ş.'den ayrı sana sayabileceğim şirketler arasında kolej var, eğitim ve öğretim açısından faaliyet gösteren, otelcilik faaliyeti gerçekleştirdiğimiz Düzce'de tesislerimiz var. Bizim ana merkez binada faaliyet gösteren C3 Yönetim A.Ş. olarak faaliyet gösteren yayın gurubu var. Bu saydıklarımın hepsi ayrı bir şirket hepsinin altında ayrı bir finans muhasebe gibi departmanları olan şirket yapısı düşün. C4 Yönetim A.Ş. var telekomünikasyon şirketinde tamamen Vodafone ve Türk Telekom gibi faaliyet gösteren apayrı bir şirket, apayrı bir sektör. Aktif gençlik var, basketbol müsabakalarının düzenlendiği ve onların faaliyetlerini takip eden C5 Yönetim A.Ş. olarak apayrı bir şirket ve bunun gibi yaklaşık 7-8 tane hepsi farklı sektörlerde, farklı faaliyetlerde bulunan şirketlerimiz var. Biz ne yapıyoruz burada, biz iç denetim departmanı olarak yıl sonunda bir denetim planlaması yapıyoruz. Önümüzdeki yıl biz hangi denetimleri yapacağız, süreç denetimleri olur, finansal denetimler, uyum denetimleri, mevzuat, arada özel incelemeler denk gelirse suistimal 'fraudla' alakalı denetimler. Bu faaliyetleri yöneten departman bizim aslında iç denetim birimi. Bu dediğim 4 kişi yaklaşık senede 13-14, özel incelemelerle birlikte 15-20, ortalama bir yılda çıkarttığımız rapor sayısı ve bunu da şimdilik 4 kişilik departmanla dediğim gibi yıllık yapmış olduğumuz planlama çerçevesinde gayet güzel bir şekilde yürütüyoruz. O açıdan 4 kişiyi yeterli buluyorum diyebilirim.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Yönetim kurulu ve Mehmet Yılmaz'a (isim paylaşamadığı için sembolik olarak farklı isim kullanılmıştır).

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleştiriyor?

İç denetim departmanı olarak yıl sonunda bir denetim planlaması yapıyoruz. Önümüzdeki yıl biz hangi denetimleri yapacağız, süreç denetimleri olur, finansal denetimler, uyum denetimleri, mevzuat, arada özel incelemeler denk gelirse suistimal 'fraud'la alakalı denetimler yapıyoruz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Yaklaşık senede 13-14, özel incelemelerle birlikte 15-20 ortalama bir yılda çıkarttığımız rapor sayısı.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Aslında biz şöyle yapıyoruz bir önceki seneye ya da ondan önceki sene aslında en son ne zaman denetime gidildiyse o işle ilgili önce eski bulgularımız açık mı, değil mi, bu bulgular kapatılmış mı, ilk olarak bunları denetliyoruz. Bir önceki denetimden açıkta kalan bulgu var mı, daha sonrasında buradaki kontrol noktası eksiklikleri, bulgu seviyeleri bunların bir önem seviyesi var. Yaptığımız daha önceki denetimlerde bulgular, eksiklikler, açıkta kalan tespitler giderilmediyse ilk olarak bunlar üzerinden başlıyoruz diyebilirim. Hem yeni gelen arkadaşlar ekibimizde çok yeni, biri yeni mezun, diğeri de yaklaşık bir ya da bir buçuk yıldır bizimle. Hem şirketimizin faaliyetlerini hem de içerideki organizasyonu anlamak adına bir önceki raporu okuyarak başlamak daha iyi oluyor yapıyı anlamak adına. Hangi noktalarda eksiklikler var hem de gerçekten bire bir o ilgili departman ya da hangi şirketse yaptığımız denetim biz bir toplantı 'set' ediyoruz. Bu toplantıda denetimimizin amacı ne olacak, denetimin kapsamı ne olacak, biz hangi noktalara değineceğiz, yaklaşık kaç hafta sürecektir bu denetim, bu konularda hem gideceğimiz yeri de bilgilendirerek hem de amaç ve kapsamı sınıflandırarak bir denetim planlaması başlatmış oluyoruz aslında orada. Daha sonrasında yapmış olduğumuz toplantılarda şirketin o yıl içerisinde geçmiş olduğu yeni bir süreç var mı bir önceki yıllardan farklı yeni bizim 'wording' açısından güncellememiz gereken bir sistem olabilir, yeni anlaşılan bir dijitalleşmeyle alakalı bir 'application' olabilir, yeni kullanılan bir sistem olabilir, SAP'ye geçiş süreci olabilir, bizim daha önce hiç kullanmadığımız, bu sene hayatımıza giren noktaları belirliyoruz. Doğal olarak o noktalar hiç denetlenmediği için o noktalar üzerinde yoğunlaşarak başlıyoruz. Daha sonrasında finansal analiz, varyans analizi bir önceki sene neydi bu sene ne oldu

gözüyle bu analitik inceleme diye geçiyor, burada mevzuatsal bir değişiklik var mı, onların tespitini yapıyoruz bu süreçte diyelim. En son iki yıl önce denetim yapmışız bu süreçte kanunsal ya da mevzuatsal bir risk teşkil eden bir durum olabilir mi, bunların tespitlerini yapıyoruz. Hangi mevzuatlara tabi o mevzuatları okuyoruz herhangi bir hukuki cezai yaptırımla karşı karşıya olabilir mi diye daha sonrasında da bu risk seviyelerini tespit ediyoruz. İlgili tüm güncellemeleri göz önüne koyduktan sonra en önemli riskli seviyelerden başlayarak risk açıklamaları ve bunlarla ilgili yapacağımız 'toc' dediğimiz 'test of control'leri belirliyoruz. Az önce de bahsettiğim gibi yeni sistem alındıysa bu sistemle alakalı yapmış olduğumuz atıyorum bir onay süreci ile ilgili gerçekten sistemi açtırıp, yanına oturup o sistemin efektif bir şekilde çalışıp, çalışmadığını ilgili süreci tarif eden kişiyle birlikte bizzat yerinde testlerimizi gerçekleştiriyoruz. En sonunda da tüm denetim 'work'leri tamamlanınca gerek 'hard copy' döküman olur, gerekse sistemsel ekran görüntülü olur, kanıtlarıyla birlikte 'audit' çalışmalarımızı tamamlayıp raporumuzu yazarak başkana teslim ediyoruz.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önlüyor?

Şöyle iç denetim riskleri ne derecede önlüyor? Yani burada iç denetim tabii ki bulgulara yaklaşımından ziyade bulgular daha ortaya çıkmadan aslında amacı tamamen bu bulguların daha tespit haline gelmeden ya da tespit edilen bulguların daha sonrasında alınacak aksiyonlar ve iç denetimin getirdiği önerilerle birlikte süreçlerin geliştirilmesi, tamamen iç denetimin aslında misyonu. Şirketin faaliyetlerine değer katmak ve bu faaliyetlerin geliştirilmesine, kontrol noktalarının artırılmasına, daha az hata yapılmasına, daha az ne denir daha risksiz bir şekilde ilerlenmesine, yönetimin faaliyetlerinin denetlenmesine, yönetim gerçekten ne kadar başarılı bu konuda güvenilir bilgi sağlama noktasında bir güven aşılmasına deyim ve risklerin önceden tespit edilmesi konusunda iç denetimin gerçekten bu süreçte çok önemli faaliyetleri oldu. Bizim burada yapmış olduğumuz yıl içerisinde

gerek suistimal denetimleri olsun bunlar gerçekten şirketin çok büyük bir ne deyim maliyet ya da gider olarak hiç aslında kardan zarar deyim yani hiç bilmediği, hiç tespit edemediği noktalarda iç denetim sayesinde o kanayan yaranın, o kanayan parmağın kesilmesi noktasında bir çok yardımı oldu aslında iç denetimin. Ayrıca dediğim gibi o sistemsiz iyileştirmelerin yapılması, gerekli mevzuatsal önlemlerin alınması ve riskin erken teşhisi komitesiyle iki ayda bir toplanarak gelecek yönünde herhangi bir risk varsa bununda önceden tespit edilerek giderilmesi konusunda iç denetimin rolü büyük diyebilirim.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Şöyle aslında bizim şirkette o sorumluluk tamamen iç denetimde. İlk olarak riskin erken teşhisi diye bir komite var, iki ayda bir toplanıyor bu komite. Bu arada gerçekten sektörel kurlarla alakalı olabilir, bu sektörünün içinde bulunduğu durumla ilgili olabilir, buradaki risklerin gerçekten önceden tespit edilip daha sonrasında şirketi zarara uğratabilecekken öncesinde bunun tespit edilmesi için kurulan bir komite aslında. Bu süreçte iç denetim önemli bir rol oynuyor, toplantılara bizzat katılıyor Denetim Komitesi. Bizim yapmış olduğumuz denetimler sonrasındaki bulgularımız ve bizim getirdiğimiz önerilerin bizzat komiteye sunulup, o komite kararlarına istinaden aksiyon alınması durumunda iç denetim çok önemli bir yer kaplıyor. Bir de şirkette herhangi bir mevzuatsal hukuki ya da örnek veriyorum KVKK diye bir süreç çıktı son dönemde. Çıkan bu mevzuattan dolayı kişisel verilerin korunması konusuyla alakalı bu süreci tamamen iç denetim üstlendi. Gerek dışardan 'outsorce' bir hukuk firması gerekse içerideki departmanların IT, İK gibi süreçleri yöneten aslında bir proje yöneticisi iç denetim ilgili departmanların toplantıların 'set' edilmesi, hangi departman hangi aşamada sorumlu olacak bu kişilerin belirlenerek bu süreci tamamen iç denetim yönetti. Dediğim gibi bu gibi konularda asıl odak noktası ve şef görevini gören aslında iç denetim diyebilirim.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Bu konuda şöyle İnsan Kaynakları yürütüyor eğitim süreçlerinin tamamını. Burada bağlı olduğumuz holdingle birlikte bir eğitim, online eğitim platformu üzerinden destekleyici bir çalışmaları oldu. Açıkçası tüm personellere bu pandemi sürecinde uzaktan eğitim adı altında şirket içerisinde veremese de şirket dışı eğitimlerle bir teşvik ve bütçe ayrıldı. Onun dışında ben şu anda SMMM stajyeri olduğumda SMMM ile ilgili tüm masrafların şirket tarafından karşılanması, pandemiden önceki döneme gidersek orda KPMG (Klynveld Peat Marwick Goerdeler)'de örnek veriyorum iç denetim risk yönetimi işte 'fraud investigation' ve işte ifade alma teknikleriyle alakalı bir seminer düzenleniyor burada hem destekleyici hem de bütçe açısından hiçbir sıkıntı yaratmayan diyebilirim. Eğitim talebiyle gelen tüm personellerine kapısını açan gerek CIA olsun, bu süreçte başlattığımız gerek yöneticimizin CEF olsun gerek SMMM olsun bu gibi tüm eğitim konusunda gerekli bütçe desteğini sağlayan personellerin eğitimi konusunda tam destek veren bir yapı var bizde. Bu açıdan eğitim veriliyor mu sorusuna evet diyorum.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Test yöntemleri olarak şöyle ilerliyoruz, öncelikle yaptığımız işte sistemsel mi yoksa manuel bir kontrol mü var, yoksa bir IT açısından bir sistem kontrolümü var, ilk önce bunların bir süreç içerisindeki mevcut yapısal durumlarına göre bu süreç değişiyor. Bir işlem testi dediğimiz müşterinin mesela belgelere ve defterlere tam ve doğru olarak kaydedilip kaydedilmediğinin denetimini yapıyoruz test olarak. Kontrol testi dediğimiz belge ve kayıtların incelenmesi süreci bir sözleşme varsa o sözleşmenin temin edilip, bizzat sözleşmenin okunup, riskli maddelerin ya da bir fatura testi yapıyorsanız o faturanın belgesinin temin edilerek ekteki dökümanlarının da birlikte incelenmesi dediğimiz kontrol testleri yapıyoruz.

Analitik testler dediğimiz veriler arasındaki ilişkileri test ettiğimiz bir önceki yıl neydi bu yıl ne oldu ya da ‘gross marjin’ analiz dediğimiz satışlar geçen yıl neydi bu yıl ne oldu, bunu ay ay karşılaştırıp bir önceki yılın Haziran ayına göre bu ay %11 pik yapmış, bunun sebebi ne? Bir kampanya mı olmuş yoksa hani daha çok o süreci de anlamaya yönelik analitik testler yapıyoruz. ‘Gros marjin’ ve varyans analizi diye adlandırabileceğim örneklerle bir de maddi doğruluk testleri var. Burada da mali unsurlarının genel muhasebe ilkelerine uygun bir şekilde tutulup tutulmadığıyla alakalı yapmış olduğumuz maddi kontrol testleri yapıyoruz. Aklıma gelen testler bu şekilde.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Elde edilen bulgular Denetim Komitesi’ne sunulup o komite kararlarına istinaden aksiyonların alınması durumunda iç denetim çok önemli bir yer kaplıyor. Kurum kültürünün her zaman iç denetimin arkasında olması lazım. İç denetçilerin sektörde en çok karşılaştıkları alan çıkar çatışmaları. Çıkar çatışmaları olabiliyor, çıkar çatışmalarından uzak durmaları gerekiyor bence, ilgili yönetim kurulu üyeleri olsun, ilgili departman müdürleri olsun, siz bir süreci denetlerken yapmış olduğunuz tespitlerden sonra o süreci sahiplenip böyle bir koruyucu, kendi departmanına kendi bulgusunu kapatmaya yönelik değil de şirketinin menfaatlerini düşünürcesine şirkete daha ileride getirebilecek zararları düşünürcesine bulguyu nasıl kapatabilirizi, nasıl bulgu daha sonra bizim başımızı ağrıtmaz gibi bizim de daha çok danışmanlık faaliyeti gibi öneri geliştirdiğimiz aşamada bizimle birlikte aslında o şirketin paydaşı olduğumuzu unutmamaları gerekiyor. Bu açıdan bence çok önemli bir nokta bu. Hem diğer departmanlar hem üst yönetim hem birim yöneticileri bunun farkında olarak davranırlarsa gerçekten bu şirkete katma değerde yaratır, iç denetim faaliyetinin performansını da artırır.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Ortalama ayda bir rapor gibi ilerliyoruz. Bu pandemiden önce birazcık daha yoğun ilerliyordu yani yılda 20 rapor ya da 20-21, 20'nin üzerinde olabiliyordu şu an pandemiyle birlikte daha 1 aya doğru yaydık açıkçası. Senede rutin bizim kendi planlamamız itibari ile 12 rapor gibi düşünebilirsin onun dışında özel inceleme ya da işte çok sık olmazsa da yılda bir ya da iki kere karşılaşılabileceğimiz daha önceki yıllardan hatırladığımız suistimal raporlarını da sayarsak yani bir 15, ortalama rakam vermem gerekirse 15 rapor üzerinden raporlama yapıyoruz.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Bizim performansımız biz Denetim Komitesi kapsamında yıl sonunda bir yıllık yapmış olduğumuz denetimin tüm bulgularıyla tüm yapılan denetimleriyle isimleriyle önemlilik seviyesine göre bir rapor şeklinde bir sunum hazırlıyoruz. Bunu da genellikle yıl sonuna doğru Aralık sonu Ocak başı gibi Denetim Komitesi'ndeki yaklaşık 4 ya da 5 yönetim kurulu üyesinin de 'schedule'larındaki uygun tarihlere göre bir toplantı 'set' edip burada hem bizimde performansımız hem de yıllık şirketimizdeki kendi performansların denetimi olarak karşılıklı bir 'feedback' süreci gibi oluyor. Ayrıca bizim bu yapmış olduğumuz denetimlerin sonunda bir de kapanış toplantılarımız var. Bu kapanış toplantılarında her bir yönetim kurulu üyesi belli bir şirketten ya da departmandan sorumlu, örnek veriyorum İnsan Kaynaklarından X isimli bir yönetim kurulu üyesi sorumluyken satın almadan Y isimli yönetim kurulu üyesi sorumlu bizde. Bu yüzden doğal olarak süreç tamamlanıp denetim raporu bittiğinde kapanış toplantısında bu yönetim kurulu üyeleriyle birlikte gerçekleştiriyoruz aslında. Orada da bazen başkan bazen yönetim kurulu üyeleri denetim sonrasında yapılan bu kapanış toplantılarında da bizim bu performanslarımızı değerlendirmiş oluyor ama ayrıca bunun için bir sistem olarak soruyorsan böyle bir sistem, 'feedback' sistemi gibi bizim yapmış olduğumuz iç denetim biriminin performansını denetleyecek ya da

bir prim usulü bu sene şu kadar rapor, bu kadar bulgu bulmuşsunuz karşılığında bu kadar, x çarpı maaş gibi prim sistemi yok ya da bir satış departmanı gibi ya da ne bileyim diğer kurumsal firmalarda görebileceğin performans bazlı bir prim sistemi yok. Denetimin performans süreci tamamen Yönetim Kurulları ile yapılan toplantı ve kapanış toplantıları itibariyle kalıyor.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Şöyle aslında bizde denetimin sürekliliği aslında birazcık C1 Yönetim A.Ş.'ye bağlı olduğumuz için SPK, SPK'da da iç denetim faaliyetinin sürekliliği mevzuatsal olarak bir zorunluluk. Bu süreçte sermaye piyasasında halka açık şirket konumunda olan C1.Yönetim A.Ş. de bu SPK mevzuatı aslında bu iç denetim faaliyetlerinin sürekliliğini zorunlu hale getirmiş bir vaziyette. Ayrıca bizim kendi iç yönelgesel açıdan baktığımız zaman kendi kurduğumuz iç denetim yönetmeliğimiz ve denetim komitemiz bu birlikte yapılan faaliyetlerin iç denetim faaliyetlerinin sürekliliğinin de aslında bir 'assurance' sağlıyor bir güvence sağlıyor bize o açıdan bunları sayabilirim.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Bence burada en büyük faydalarından biri bir kere yasak koyucunun, regülatörün koymuş olduğu yasa ve düzenlemelere uygunluğu denetliyorsunuz. En önemli risklerden biri bu şirketler üzerinde riski daha önceden bahsettiğim gibi riskin erken teşhisi komitesi olsun, iç denetim yönetmeliği olsun, bizim yapmış olduğumuz denetimlerde riski önceden tespit edebiliyorsunuz yani bir erken uyarı sinyali niteliğinde görevi görüyor şirketlerde aslında iç denetim. Güvenilir bilgi sağlamada aslında çok öncü bir rol oynuyor. Doğru ve güvenilir bilgiye ulaşmada yapmış olduğu gerek faaliyetler gerek mesleki yeterlilik belgeleri teknik anlamda da yeterli bir departman olduğu için genelde diğer departmanların başvurdukları nokta iç denetim bölümü oluyor. Herhangi bir raporlamada mutabakat sağlamak olsun bir verinin doğruluğu olsun burada güvenilir bilgi sağlama açısından önemli bir noktada. Üst yönetim tarafından belirlenen şirket içi saymış olduğum politikalara

uyumun denetlenmesi konusunda şirket kültürünün oluşumundaki o politikalara uyumu denetleme açısından çok önemli bir yere sahip ayrıca şirketin iç kontrol süreçlerinin sağlıklı bir şekilde sürdürülmesi açısından ya da hata ve hilelerden kaynaklanacak kayıpların önlenmesi konusunda bence iç denetimin yeri ve önemi gayet açık ve net diyebilirim.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok. Benim söyleyeceklerim bu kadar. Hemen hemen her konunun üzerinden geçtik zaten.

Ek 4: D Katılımcısı Mülakatı

- Yaşınız: 33
- Eğitim seviyeniz: Yüksek Lisans
- Toplam iş tecrübeniz: 9 yıl
- Kurumunuzda çalışma süreniz: 6 yıl
- Kurumunuzun sektörü: Sağlık, yapı ve tüketim malzemeleri
- Kurumunuzun çalışan sayısı: Yaklaşık 11.000

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Toplamda 15 kişi, yani kime sorsanız biriminde yeterli personel olduğunu söyler ama teknolojik yapıda yeri geldiğinde yetersiz 'outsorce' kaynaklarla belirli bir seviyeyi yakalamaya çalışıyoruz. Ama sorunuzun net cevabı daha fazla olsa elbette daha fazla yoğun denetimler yapılabilir. Ama personel sayınızı arttırdığınızda da bütçe kısıtları çeşitli kariyer hedeflerinin uyuşmaması dezavantaj olabiliyor. Herkesi aynı anda kariyer yolunda destekleyemeyebiliyorsun.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

İç denetim birimi Denetleme Kurulu çatısı altında görevini yerine getiriyor Denetleme Kurulu Başkanı Yönetim Kurulu Başkanı'na bağlı direkt olarak. Burada bir de Denetim Risk ve Yönetişim Komitesi var. Ben ona kısaca Denetim Komitesi diyorum ama o aslında üçlü bir komite.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Daha konvansiyonel şirketlerin satış, satın alma ve finans süreçlerine odaklanıyoruz. Satın alma biraz da bazen tedarik zinciri denetimine evrilebiliyor. Yani içerisinde lojistik denetimleri de olabiliyor. Aynı zamanda İnsan Kaynakları denetimleri de yapmaya başladık. Eski bir tarih ama en azından İnsan Kaynakları süreçlerinde de performans yönetimi süreçlerinde de denetimler gerçekleştiriyoruz. Bir de tabi ticari işletme olmayan bazı kuruluşlarımız var bunlarda da böyle sadece bir satın alma satış denetimi değil vergi risk çeşitli ticari riskler çeşitliliği ne durumda diye inceliyoruz böyle özetleyebilirim.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Yani Eylül, Ekim ayı gibi başlayan süreç yeni yılın başlamasıyla Ocak, Mart, Haziran ve Eylül olmak üzere 4 ayrı toplantıyla gözden geçirmeler ve durum bildirimleri de yapılarak denetim planı uygulanıyor. Varsa değişiklikte yapılıyor yıl içerisinde.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Denetim planı metodolojik olarak öncelikle ben tabi şirketlerden kuruluş diye bahsediyorum. Kuruluş dediğimde lütfen ticari şirketi söylediğimi düşünün. Kuruluşların genel müdürleri, CEO'ları, en üst düzeydeki yöneticileriyle denetim planı hakkında görüşmeden önce bütün birimleriyle yani satış, tedarik zinciri, varsa

AR-GE, üretim departmanlarıyla bir araya geliyoruz ve kendilerinin riskli gördükleri denetlenmesini istedikleri alanlar olup olmadığını onlara soruyoruz. Bu tünde yaklaşınca da topladığımız risk havuzunda daha sonra kendimiz bir değerlendirme yapıyoruz. Ve bunları üst yönetimle paylaşıyoruz. İlgili kuruluşun Genel Müdür'ü, CEO'su katılabilirse CEFO'su da yine katılıyor. Ve kuruluşların birimlerinden gelen önerileri finansal olarak etkilerini de göz önünde bulundurarak bir öncelik sıralamasıyla üst yönetime sunuyoruz. Üst yönetimde burada genellikle bu sıralamaya katılıyor bazı eklerde bulunmak istiyor, ya bizim şöyle de bir konumuz var bizim arkadaşlarımız iş birimi olarak bununla muhattap olmuyorlar ama bir satış anında yani şirketin satılması anında veya şirketin bir ortaklık kuracağı anda bizim şu şu risklerimizde var bunlara bakabilir misiniz diye talep topluyoruz. Ardından elimizdeki insan kaynağına bakıyoruz biz bunların ne kadarını tamamen iç kaynakla yapabiliriz, dış kaynak gereksinimimiz olacak mı, dış kaynak gereksinimimiz olacaksa bunu bütçeliyoruz ve denetim komitesine sunuyoruz. Oradan geçmesi halinde dış kaynak dahil olmak üzere denetim planını takvimlendiriyoruz. Tabi takdir edersiniz ki Covid ile birlikte bu denetim planına uyum dışında yeni taleplerde oluyor. Yani denetim planını dinamik gözden geçirmeniz gerekiyor bunun için çeyrek dönemlerde üst yönetimle biraya gelip sizinle bir yıl önce denetimlere başlamadan konuştuğumuz takvimle buradayız, şu şu aşamaları kaydettik şurada aşama kaydedemedik veyahut burada yeni bir ihtiyaç oldu, bunu da şu şekilde gerçekleştirdik ya da gerçekleştiriyoruz var mı sizin bir eklemeniz diye çeşitli toplantılar yapıyoruz.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önlüyor?

Yani şöyle bakmak lazım denetim biraz daha geçmişe hep bakar, bazı geçmiş dökümanları inceleyerek neyin olup bittiğini, bunların prosedüre veya mevzuata uygun olup olmadığını denetler. Bu biraz daha konvansiyonel klasik iç denetim yaklaşımı fakat ilerleyen teknolojiyle birlikte veri analitiği araçlarını daha etkin

kullanabilirseniz bunu öncelikle bir tasvir edici destekleyici analizler yapabilirsiniz yani bu normal denetimde bir oran analizi veya karşılaştırmalı finansal tablo okuma gibi düşünülebilir daha sonra buradan hareketle bütün datayı alıp belli modellerde 'predictive' analizlere de gidebilirsiniz. Burda iç denetimle iç kontrol veya 'monitoring' karışımı yani 'monitoring'le iç kontrol tamamen iç denetim biriminden ayrılacak bir şey değil analizlerinde 'deductive' olarak ya bakın datanız bu piyasadaki datalar bunlar, sizin şu satışlarımız şuralarda sıkıntıya düşebilir veya tüm tahsilatlarınız ileride problemlili olabilir diye önleyici bazı 'radflek'leri kaldırabilirsiniz ama riskleri önleyecek departman ya da alacak departman tek başına iç denetim değil sadece risk konusunda bir yönetim fonksiyonu var risk yönetimi bazında bazı süreçler etkin işliyor mu, işlemiyor mu, bunları söyleyebilir ama riski alırız veya önleriz diyemeyiz iç denetim olarak. İş birimleri riskleri alır riski önlemeye çalışır.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Riskin yönetilmesi için bir görev ve sorumluluğumuz yok sadece risk yönetimi biriminin etkinliğini ölçmek performansıyla ilgili görüş vermek gibi sorumluluğumuz var risk yönetiminde bir problem görüyorsak onu denetim komitesine aktarmak üst yönetimi yönetim kurulunu bilgilendirmekle sorumluyuz.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Şöyle davranış kuralları özelinde denetim, hukuk ve İnsan Kaynakları birimlerinin 'webinar'ları oluyor. Davranış kuralları zaten halka açık bir şekilde ulaşabileceğiniz şirketin websitesinde sayfanın en altından ulaşılacak yaklaşık 70 sayfalık bir döküman. Bu döküman içerisinde çeşitli bölümler var. Rüşvet ve yolsuzlukla mücadelen tutun, çıkar çatışması konularına, insan ilişkileri, değer verme politikası gibi çeşitli bölümleri var. Bu bölümleri özellikle 15 günde bir 'mailing'ler ile tüm çalışanlara hatırlatmalar yapıyoruz. Yani nedir, rüşvet ve

yolsuzlukla mücadele politikamız olduğunu biliyor muydunuz diyerek bir sabah maille karşılaşabiliyorsunuz. Yine İnsan Kaynakları birimiyle kafa yorup biraz daha etkinliğini arttırmak için çalışanlar ekranlarını kilitlediklerinde şirketimizin davranış kurallarının şu maddesine göre böyle bir durum olduğunda şu şekilde davranmanız gerekiyor aksi takdirde şu kısımdan bildirimde bulunabilirsiniz gibi özellikle o bir çay, kahve molasından döndüğünüzde de çalışanlar bu davranış kurallarını görüp, hatırlayıp, tepki verebiliyorlar. Bu uygulamadan sonra da bildirim sayılarında artışlar gözlemledik.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Kurgularken bağımsız denetimden yola çıktık detay testler, analitik tetstler, prosedürler akabinde çeşitli ‘high level’ kontrol değerlendirmeleri. Biz öncelikle kuruluşumuzda bir risk kontrol matrisi var ise buradaki risk matrisini alıp kontroller neler, bu kontroller etkin mi, değil mi, güncel durumları nedir onu görmek istiyoruz veya iç kontrollerin etkin olduğuna dökümanlarıyla beraber, kanıtlarıyla beraber kanaat getiriyorsak orada çok fazla detay test yapmıyoruz ama şüphelendiğimiz bir konu var veya geçmişinde yaşanan maddi kayıpla sonuçlanan bir durum varsa oralarda kontroller yeterli de olsa detay testlerimizi yoğunlaştırabiliyoruz. Yani detay testlerden de kastım bir süreci baştan sona bir ‘walkthrough’ olarak işini anlayıp kontrol noktalarını veya veri girdisi olan kısımların dökümanlarını toplamak bu dökümanlarda veri girişi olan yerlerde bütünlük sağlıyor mu, herhangi bir dış müdahale geliştirilebilir bir veri kaynağı var mı, yok mu onu kontrol ediyoruz. Genel olarak böyle özetleyebilirim.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Denetim birimi olarak bulgulara önem sırasına göre topluluğa katkı sağlayacak riskleri ön plana çıkarabilecek bulguları parlatıp öne çıkarıp biraz daha düşük seviyede düşük risk seviyesinde olanları daha geride tutuyoruz bizim bulgulara

yaklaşımımız biraz daha o ve bulgulara karşı tarafın cevabını veya önerilerini beklerken de genelde bir sistem yatırımı gerektirip gerektirmediği bizim kritik sorduğumuz soru çünkü bütçe gereksinimi olabilir kuruluşlarda rapor tamamlanmadan önce raporun tespit yani bulgu kısmını riskleri ve önerileriyle birlikte gördükleri için genelde kapanışta herhangi bir itiraz olmuyor. İtiraz olursa risk kabul yapma şansları var yani risk kabulden kastım şu, ben bu riski kabul ediyorum, bu riski alıyorum, sizin bulgunuzda tespit ettiğiniz, ortaya koyduğunuz, riskli olduğunu düşündüğünüz konu hakkında aksiyon almayacaksa ben buna bir beyanda bulunmuyorum diyebiliyor burada Denetleme Kurulu olarak eğer hakikaten burada bir risk görüyorsak şirketi veya topluluğu çeşitli yönlerden olumsuz etkileyeceğini düşünüyorsak bunu yönetim kuruluna tabi kanıtlayabilme yetkimiz var. Şu ana kadar böyle bir durumla karşılaşmadık ama üst yönetime ve yönetim kuruluna çeşitli konuları öncelikli olarak aktardığımız oldu. Bunlar aktarılmayan konular değildi ama aksiyonun hızlanması için yine üst yönetimle paylaştık. Yönetim Kurulu ile paylaştık.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

İç denetim birimi Denetleme Kurulu çatısı altında görevini yerine getiriyor. Denetleme Kurulu Başkanı, Yönetim Kurulu Başkanı'na bağlı direkt olarak. Burada bir de Denetim Risk ve Yönetişim Komitesi var ben ona kısaca Denetim Komitesi diyorum ama o aslında üçlü bir komite. Denetim Komitesi'nde de yine Denetleme Kurulu Başkanı, Yönetim Kurulu Genel Sekreteri de yine İç Denetim Direktörümüz bu iki katılımcıyla oralardaki yönetim kurulları çeyrek dönemlerde yapılırken öncesinde Denetim Komitesi de gerçekleştiriyor periyodik raporlama bu şekilde. Yılda iki sefer Yönetim Kurulu Başkanı'na direkt aslında sunum gerçekleştiriliyor. Bu sunumlarda da gerçekleşen denetimlerin ön uç bildirimlerini paylaşıyoruz. Raporlarımız ise denetimler sonlandıkça ilgili üst yönetim ile önem sırasına alınanlar önceliklendiriliyor, kapanış toplantısı yapılıyor.

**Kurumunuzda iç denetim biriminin performansı denetleniyor mu?
Denetleniyorsa nasıl?**

Biz öncelikle kendi kalite gözden geçirmemizi yapıyoruz. Standartlar belki biliyorsunuzdur ben de yeni öğrendim, beş yıl içerisinde dış kalite gözden geçirmeden geçtiğiniz taktirde uluslararası standartlara uygun denetim yapıyorum ifadesini raporlarınızda kullanabileceğiniz şekilde bir şart getiriyor. Bizim hedefimizde bu bağımsız kalite gözden geçirmeden geçmek yani ‘big four’ dan bir denetim şirketine iç denetim fonksiyonunu denetletmek. Şu an itibari ile kendi içimizde buna hazırlık yapmak amacıyla kendi gözden geçirmemizde kısmen uyumlu ve genellikle uyumlu olarak adlandırılabilir şekilde değerlendirmeleri gerçekleştirdik ama tabii gelişime bir sürü açık alan var zamanla daha da iyi olacaktır.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

İç denetimin sürekliliğini sağlayabilmek adına büyük organizasyonlarda holding çatısı altında örgütlenen iç denetim departmanları ‘turnover’da yüksek çıkınca problem yaşayabiliyor. O yüzden biz 2018 Haziran ayından itibaren kuruluşlarda iç denetçi görevlendirmeye başladık. Be demek bu? İşte holdingde belli denetçiler var, iç denetim departmanında ama şirketimizin iş alanlarından yapı grubu yani banyo seramik malzemeleri ve karo malzemeleri şirketlerinde birer denetçi, doğal kaynaklar şirketinde birer denetçi, tüketim ürünleri üretimini yapan şirketlerde birer denetçi olmak üzere oraya denetçiler atadık. Onlar şirketin günlük işleyişi içerisinde yeni çıkan konulara da hakim olarak denetim planlarını revize ediyorlar, denetimlerini gerçekleştiriyorlar. Yeri geldiğinde destek ihtiyacı olduğunda holdingden onlara destek sunuyoruz. Birlikte gerçekleştirdiğimiz projeler oluyor matris olarak da orada sürdürülebilirliği sağlayabilmek orada CEFO’nun CEO’nun baskısı altında ezilmemesi için matris olarak da Denetleme Kurulu’na bağlılar. Yani sürdürülebilirliği sağlamak için iç denetim anlamında böyle bir yaklaşım

gerçekleştirdik. İlerleyen dönemde belki gözden geçirilmesi revize edilmesi gerekebilir şimdilik işlediğini düşünüyoruz.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Yani iç denetim işlemeyen süreçleriniz varsa işlemeyen kontrol mekanizmalarınız varsa bunları size hatırlatır ve bazı felaketleri yaşamadan bunlara önlem alabilirsiniz. Bu felaketlerden kastım eğer bir CEFO'nuz tahsil edemediği alacaklarıyla baş edemez durumdaysa ve kendi KPI'ları sebebiyle de bunları gündeme getirip çözüme ulaştıramıyorsa iç denetim departmanı bunu bir ana konu olarak ortaya koyup çözüm önerilerini de paylaşıp gündeme getirilmesini sağlayabilir şirketi. Belki de o tahsil edemeyeceği alacaklarla ilgili planlama yaparak bazı alacakların daha hızlı alınmasını sağlayabilir. Şirketle ilgili çok verimli sonuçlar ortaya çıkartabildiğini düşünüyorum. Denetçiler biraz daha derinlemesine inceleme yapmaktan keyif duyan, konuyu kanıtlarıyla birlikte değerlendirip sunabilen ekipler, o açıdan disiplinler arası çalışmalarda da çok ciddi katkılar sunduk devamı da geldiğinde bunları danışmanlık projeleri olarak kendi içimizde değerlendiriyoruz. Özetle, iç denetim paydaşlara güvence verir. Şirketlerin yapısı çeşitli kontrol mekanizmalarıyla güvence altına alınmış mı, bu mekanizma çalışıyor mu, bu şirket sürdürülebilir mi, bu şirketin karlılığı devam ettirilebilir mi bunların aslında güvencesini verir. Şirket beklentilerini anlayarak denetim yaparsanız da yani bazı kuruluşların tek önceliği kar olmayabilir, tek önceliği ciro olmayabilir, başka ilke hedefleri de olabilir buna göre denetim her zaman o paydaşın hedefine ulaşması yolundaki güvenceyi sağlar, içinin rahatlamasını sağlar, halka açıksanız daha stabil bir hisse senedi olmasını da sağlayabilir o kurumsal öğrenmeyle birlikte.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok, benim söyleyeceklerim bu kadar.

Ek 5: E Katılımcısı Mülakatı

- Yaşınız: 34
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 10 yıl
- Kurumunuzda çalışma süreniz: 1,5 yıl
- Kurumunuzun sektörü: Enerji
- Kurumunuzun çalışan sayısı: 10.000-11.000 arası

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Denetim Direktörümüz var, direktöre bağlı 3 tane Denetim Müdürü var, 3 Denetim Müdürü'nün altında etik ve soruşturma tarafı da olduğu için 2 oradan, 4 biz, 2 de IT, toplamda 12 kişi. Sayı açıkçası bence yeterli olmuyor. Yeterli değil çünkü şirket süreçleri de çok karmaşık dolayısıyla bence yani en azından süreç denetimi ekibine bir ya da iki kişi daha ek takviye olursa çok daha iyi olur ama bizde bir yandan şey de yapmaya başlıyoruz, denetimde dijitalleşme, veri analitiği vs. projelerimiz var ve böylece işte bu az sayıda olan denetim kaynağını öyle kompanse edebilelim amacımız o.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Denetim Komitesi altında üst yönetime bağlı çalışılıyor.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Kurumumuzda üç farklı denetim ekibi var. Bir süreç denetim ekibi ben süreç denetim ekibi tarafındayım, bir IT 'audit' var, bir de etik-soruşturma tarafı var. Bu hani üç ekip çok aslında iç içe çalışmıyor, konuları bakımından ayrıştırıyor ama zaman zaman da şeyler olabiliyor, birbiriyle kesiştiği noktalar olabiliyor. Mesela

işte soruşturma tarafından belirlenen çok önemli şeyler varsa onalar süreç denetimine paslıyor, bunu denetim planına ekleyebilir miyiz gibi daha geniş incele gerektiriyor, süreç incelemesi gerektiriyor vs. gibi şeylerde olabiliyor. Ya da biz mesela 'IT audit'ten destek isteyebiliyoruz. İşte şu kontroller doğru mudur vs. gibi ama hani genel olarak şey herkes kendi sınırları çerçevesinde kendi işinden sorumlu diyebilirim.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Biliyorsunuz öncelikle bir denetim planı yapmamız gerekiyor, denetim planını yapmak içinde belirli kaynakların olması gerekiyor öncelikle denetim evreninin belirlenmiş olması gerekiyor. Şöyle yapıyoruz kurumumuzda denetim evrenini her yıl gözden geçiriyoruz. Çünkü çok hareketli bir yapıya sahip bir kurum hem satış tarafı için hem de dağıtım tarafı için bir de tepe çatısı şirketimiz var hem de onun süreçlerini gözden geçiriyoruz ve denetim evrenini güncelliyoruz. Denetim evreninin güncellenmesinin akabinde bir başka kaynaktan da risk envanteri, şirketin risk bölümünün hazırladığı periyodik olarak takibini yaptığı bir risk envanteri var. O risk envanterini alıyoruz ve denetim ekibinin daha önceki yıllarda gerçekleştirdiği denetimlerin sonuçlarını yine hani alıyoruz bu üç ana veri oluyor. Bu üç ana veriyi bir araya getirip işte bir sonraki yılın denetim planını oluşturuyoruz. Aynı zamanda Denetim Direktörümüz üst yönetimle de bir araya geliyor. Hem CEO seviyesinde hem de diğer direktör veya müdür seviyesinde kişilerle bir araya gelip onların gündemindeki konular neler, riskli konular neler, onları belirleyerek denetim planını oluşturuyoruz.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Denetim planının oluşturulmasının akabinde öncelikle bir hazırlık aşamamız oluyor tabi ki bu hazırlık aşamasında da 'qdm's' diye bir sistem kullanıyoruz oradaki ilgili sürece ilişkin işte prosedürler, iş akışları vs. onları indiriyoruz, okumaya başlıyoruz. Sonrasında enerji sektörü çok regüle bir sektör olduğu için işte 'epdk'nın vs.

mevzuatların ilgili sürece ilişkin mevzuatları indiriyoruz, onları okuyoruz ve hani biraz böyle bu okumaları yaparken de ilgili süreç sahipleriyle bir ön görüşme yapıyoruz. Hani bize bir süreci anlatsınlar diye. Prosedür üzerinden gidiyoruz genelde veyahutta onların eklemek istedikleri konular prosedürde yer alamayan şeyler varsa biraz eskiyse prosedür böyle görüşmeler yapıyoruz. Orada aslında görüşmelerde zaten riskli alanları belirliyoruz biraz biraz, sonrasında bu hazırlık aşaması genelde böyle bir hafta gibi sürüyor. Hazırlık aşamasının ardından bir resmi açılış toplantısı düzenleniyor bu resmi açılış toplantısında da denetlenen bölümün direktörü katılıyor, sorumlu müdür katılıyor, Denetim Direktörü katılıyor, Denetim Müdürü katılıyor ve denetim ekibi katılıyor. Bu açılış toplantısının akabinde de saha çalışmasına başlıyoruz. Tabi şimdi buradaki kritik nokta saha çalışmasına başlarken biz bu hazırlık aşamasında yaptığımız okumalar, prosedür okumaları, iş akışlarının incelenmesi, ondan sonra işte mevzuat okumaları gibi bunlardan çıkan sonuçları bir risk kontrol matrisine koyuyoruz. Eğer o süreç daha önce denetlendiyse atıyorum satın alma denetimi belirli periyotlarda denetliyoruz. Üç yılda bir denetleniyor satın alma bölümü daha önce bununla ilgili bir risk kontrol matrisi vardı zaten eğer bir güncelleme gerekiyorsa o güncellemeyi yapıyoruz. Ama hiç denetlenmeyen bir bölümse kendimiz en baştan bu risk kontrol matrislerini oluşturuyoruz ve saha çalışmasına başlıyoruz. Şimdi saha çalışmasında sürecin büyüklüğüne göre karmaşıklığına göre süre olarak değişkenlik gösteriyor. Bu arada her bir denetimde bir kişi, bir denetçi olacak şekilde dizayn ediyoruz. Denetimleri tabi ki müdür yönlendiriyor ama hani sadece bir denetçi oluyor denetimde dolayısıyla süreyi de ona göre ayarlıyoruz. Genelde 4 hafta ya da 5 hafta saha çalışması oluyor. Saha çalışmasının bitiminde bir mutabakat toplantıları düzenliyoruz. O mutabakat toplantılarının ardından ilgili departmanın müdürüyle bir ön kapanış toplantısı yapıyoruz. Ön kapanış toplantısının ardından da nihai kapanış toplantısı yapıyoruz. Rapor yazılıyor saha çalışmasının ardından. Mutabakat yaparken aslında rapor böyle biraz daha hani oluşmuş oluyor. Mutabakatın ardından da artık ön kapanış toplantısında da raporu göstererek raporun üzerinden geçiyoruz müdüre herhangi bir şey olmasın diye, anlaşmazlık

olmasın, nihai kapanış toplantısında hiçbir pürüz çıkmaması adına. Sonrasında nihai kapanış toplantısında da ilgili bölümün direktörüne direk sunumumuzu yapıyoruz. Tarihler konusunda bazen aksiyon alma tarihlerinde biraz sorun olabiliyor, hani biz biraz daha tabi sıkı tutuyoruz. Atıyorum altı aylık ya da dokuz aylık tamamlama süreleri veriyoruz. Ama işte denetlenen birim biraz daha süre isteyebiliyor hani biraz daha o tarafta anlaşmazlık yaşayabiliyoruz. Onun haricinde mutabakatın ardından da kapanış ön kapanış, nihai kapanış derken aradan iki hafta geçiyor yani bir denetimi toplamda iki aylık bir sürede tamamlamış oluyoruz. Süreç de genel olarak böyle.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önlüyor?

Şöyle şimdi meydana gelebilecek riskleri yüzde elli, yüzde elli diyebiliriz. Yani olan şeyleri tespit ediyoruz, bunu yüzde elli diyebiliriz. Olabilecek şeyleri de tespit ediyoruz yani bunda belki olan şeyler yüzde altmış olabilir. Bazen işte olabileceklerin oranı daha düşük olabilir ama hani bu seviyelerde yüzde elli yüzde elli ya da yüzde altmış yüzde kırk gibi. Çünkü biraz daha şeye önem veriyoruz bu 'audit tool'larını kullandığımız için oda sürekli denetime bizi 'control audit'e yönlendiriyor. Oradan da aslında şeyler çok çıkıyor yani riskli olabilecek alanlar çok çıkabiliyor. Ama bu daha böyle yeni yeni olanda bir şey yavaş yavaş o yüzden oranına birazcık yüzde kırk diyebiliriz olabilecek riskler için bir de şöyle mevzuat o açıdan kurumumuz çok iyi bir örnek oluyor, çok mevzuat olduğu için işte bahsettiğim gibi enerji sektöründe şimdi mevzuatın büyük oranını zaten kontrol edebiliyorlar. Ama hani bazen gözden kaçan şeyler oluyor ya da çok önemsemeyebiliyor süreç sahibi o noktayı. Ama biz diyoruz ki bu mevzuatta yazdığı için şu ana kadar 'epdk' denetimlerinde çıkmamış olabilir, konu etmemiş olabilirler ama bu konu edilmeyecek anlamına gelmez. Olabilecek bir risk bu diyoruz. Hani o yüzden bu değerlendirmelerimizde de fazlaca çıkıyor yani aslında dolayısıyla regüle bir sektör bu konuda çok daha uygun oluyor.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Şöyle biz zaten iç denetim olarak şeyden sorumluyuz iç denetim ve risk departmanı değil departmanımız, ayrı bir departman. Bizim riske karşı olan sorumluluğumuz da şu, şirket tarafından belirlenen riskler ve onlara ilişkin kontroller yani şirketin risk iştahına uyumlu bir şekilde kontrol dizaynı oluşturulmuş mu, oluşturulan o kontrol dizaynı yeterli mi bunları kontrol ediyoruz. Aslında bir de belirlenmeyen riskler var mı şimdi denetimde mesela o risk envanterinde belirlenmeyen riskler olabilir. Denetim sonucunda da ekstra riskler gelebilir, konular gelebilir o konuların o risk envanterine adaptasyonu ile ilgili görüşmelerimiz oluyor. Ama hani temel olarak bu böyle sık olan bir şey değil çünkü risk envanteri gerçekten hani kapsamlı ama temel olarak şey kontrol dizaynı yeterli mi, o riske ilişkin yani kontrol var mı ve kontrol dizaynı yeterli mi, düzgün çalışıyor mu onu kontrol ediyoruz ve temel olarak ondan sorumluyuz.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Yani risk yönetimi ile ilgili bilemiyorum risk departmanı bir eğitim düzenliyor mu ama şu yeni sistem kullanılmaya başlarken sanırım bir eğitim düzenlendi ama çok emin değilim. Denetim tarafında da ben girdiğimden beri 1,5 yıl oluyor bir eğitim verilmedi. Ama yani şey ne bileyim zaten bilinen bir şey olduğu için o kültür yerleştiği için çok ihtiyaç duyulmuyor şu anda ama risk tarafında var mı öyle bir eğitim emin değilim.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Şöyle bir kere örneklem metodunu uyguluyoruz, şimdi örneklem metodunu da artık biraz geliştirdik bu veri analitiği ‘tool’larıyla birlikte ‘sas’ kullanıyoruz. Oradan hani direk sorumlu olan şeyleri tespit ediyoruz. O sorumluların içerisinde

örneklem seçip bunlar gerçekten sorumlu mu yani bir kümül data çıkıyor karşımıza. Sorumlu olarak teyit etmek amacıyla belge kontrolü yapmak amacıyla onların arasından örneklem seçiyoruz bu birinci yöntem. İkinci yöntem direk örneklem seçmek hiç data analitiğini kullanmadan, onun dışında ne yapıyoruz süreç sahibiyle yan yana oturup açar mısın ekranını işte bu süreci nasıl işletiyorsun diye birlikte yan yana kontrol ediyoruz. Atıyorum işte faturayı aratma, fatura girişi, bu fatura girişini nasıl yapıyorsun gösterir misiniz diye birlikte test yapıyoruz oradan. Onun dışında neler yapıyoruz galiba bu kadar diyebilirim.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Kurumumuzda olgunlaşmış bir denetim kültürü olduğu için biz aylık olarak şey yapıyoruz denetim takip sistemi üzerinden hatta iki hafta ve bir aylık periyotlarda bilgilendirme yapıyoruz süreç sahiplerine işte aksiyonun tamamlanması için son iki hafta kaldı, bir hafta kaldı diye bir uyarı mailleri gönderiliyor. Bir de ‘overdue’ olduktan sonra yani süresi geçtikten sonra gönderilen mailler var ve aynı zamanda da bu denetim komiteleri toplantısı öncesi yönetim kurulları toplantısı öncesinde denetim komitesi raporlarında da bin tane unsur şey tamamlanmamış aksiyonlar diye bir başlığımız var. Orada kaç adet bulgu var, kaç adet aksiyon var, bunlardan kaç tane tamamlanmamış, ‘overdue’ olmuş, kaç gün geçmiş aksiyon tamamlanma tarihinden gibi bilgileri içeren bir sayfamız var ve hani orada hem denetim komitesine hem de Yönetim Kuruluna sunuluyor ve yani şirketin üst yönetimde bunu önemseydiği için tam bu komite toplantılarından önce özellikle bir böyle telaşlanıyor, kapatmaya çalışıyor bulgularını, aksiyonlarını, işte aksiyonları tamamlamaya çalışıyorlar o yüzden aslında şey üst yönetimden inen kültürle birlikte aksiyon sahipleri biraz daha şeyler sıkı tutuyorlar bu şeyi denetim konularının kapanmasını kapatılmasıyla ilgili aksiyonların alınmasını.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Şöyle aynı anda dört denetim sürdürülüyor, süreç denetimi, hani öyle olunca işte iki ayda iki buçuk ayda dört tane denetim raporu çıkıyor diyebiliriz. Denetim raporu çıkarken resmi yapılan Denetim Müdürü 'tool'da oluyor, mail gönderilen esas o oluyor ama cc. de zaten raporda da gözüktüyor, şirketin Genel Müdürü, kurumumuzun genel müdürü, dağıtım şirketinin genel müdürü, satış şirketinin genel müdürü var bir de tepede kurumumuzun CEO'su var CFO'yu da muhakkak koyuyoruz. Bunlara mail atılıyor ama raporun üzerinde de yazıyor bu kişilerin ismi raporun 'tool'unda kimler var, sorunlu kişiler, cc. de kimler olacak, onlarda yazıyor. O şekilde mail atılıyor, sonrasında da bunlar üç ayda bir yapılan denetim komitesi ve şeyde yönetim kurulunun toplantılarında konuşuluyor. E tabi bütün konular konuşulmuyor orada kritik yüksek ve daha böyle önemli olabilecek orta seviyedeki bulgular aktarılıyor.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Normalde bizim bu şey tüzüğümüzde Denetim Komitesi sorumludur diyor. Dolayısıyla denetim komitesi bir değerlendirme yapıyor. E bizim zaten her bir ünvan için KPI'larımız belli, denetim bölümü olarak da KPI'larımız belirli, onlara uyum konusunda nasılız diye denetim komitesi zaten bilgilendiriliyor ama şu an öyle yapılmadı henüz iç denetim standartlarına uygun denetim gerçekleştiriliyor mu diye bu dört büyüklerin yaptığı 'qr' denetiminden geçmedik ama en son ne zaman geçmişti bilemiyorum onu ama şu son dönemde 1,5-2 yılda 'qr' dan geçmedi henüz.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Şöyle bizim iç denetim prosedürümüzde yazan 3 yılda bir denetlenecek diyor. Bir süreç için yani hani ama atıyorum çok riskli bir şey vardır, bölüm vardır, süreç vardır hani onun yılda bir denetlenmesi gerekebilir. Atıyorum bunlar zaten

prosedürde yazıyor. Biz denetim planını da yaparken zaten dediğim gibi önceki yılların denetim sonuçlarını alıp onları da dikkate alarak bir analiz gerçekleştiriyoruz. Yani o tamamen sürecin riskliliğine bağlı olarak ya da atıyorum yepyeni bir bölüm doğmuştur, ortaya çıkmıştır o bölümün muhakkak görülmesi denetlenmesi gerekiyordu gibi tamamen duruma göre değişkenlik gösterir ama hani şu prosedürde yazan 3 yılda bir denetlenir her bir süreç uygun olması durumunda. Yılda bir de denetlenebilen süreçler olabilir diyor o da tamamen risk analizine bağlı olarak değişiyor.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Körlüğü engelliyor, yani ben mesleğimi çok seviyorum çünkü yani bazen tabi çok zorlanıyorum da nihayetinde hala önyargılı süreç sahipleri olabiliyor hala ama şöyle tamamen taptaze bir bakış açısı geliyor o süreci baştan aşağı hani o kültürü öğreniyor ve oradaki yanlış giden şeyleri tespit edebiliyor başka tecrübeleri olmuş oluyor. Çünkü başka departmanlarda gördüğü iyi uygulamaları işte o departmana entegre edebiliyor vs. ya da hiç aklına gelemeyecek olan riskler olabiliyor işte körlük dediğim o. Yani bunu böyle direk gösteriyor, ne kadar güzel dışardan birisi geliyor sana sen şunu daha iyi yapabilirsin diyor. O açıdan ben çok önemsiyorum yani finansal kaygı engelleyebiliyor, operasyonu iyileştirebiliyor, zaman ve insan kaynağı olarak da düşünmek lazım, sadece finansal kaynak değil, hani bunların optimize edilmesini sağlıyor. O yüzden bence şey çok önemli bir destek fonksiyonu denetim.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok. Hemen her şeyi konuştuk, anlattım, üzerinden geçtik konuların.

Ek 6: F Katılımcısı Mülakatı

- Yaşınız: 38
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 16 yıl
- Kurumunuzda çalışma süreniz: 1 yıl
- Kurumunuzun sektörü: Alkollü içecek
- Kurumunuzun çalışan sayısı: 1.000+

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

İki kişi, Türkiye’de iki kişi, şu an Türkiye ofisin ihtiyaçları için yeterli.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

İç denetim birimi finansın altında CFO’ya direk raporlama yapıyor aynı zamanda ‘head quarter’da genel merkezde bağlı olunan ekibe iç denetim grubuna raporlama yapıyor.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

‘Head quarter’ yani genel merkezin programında var olan ya da programda var olan SOX denetimleri var. Bunun dışında yıllık plan dahilinde bizim risk bazlı iç denetim planımız var, süreç denetimi daha çok operasyonel süreçler üzerinde fabrikalarımız var ülkede 9 tane onların denetimini yapıyoruz. Aslında bakacak olursanız risk bazlı SOX denetimi çünkü şirket borsaya kote ve de bununla beraberde lokal bazda risk bazlı operasyonel süreç denetimi.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Denetim planı yıllık bazlı oluşturuluyor ve her 'quarter' da revize ediliyor, gözden geçiriliyor. Önce tabii 'top' konularda olabilir çünkü aynı zamanda etik ve uygunluk departmanımız ve dolayısıyla hani öncelikli 'top' konular ortaya çıkabilir üst yönetimin ya da işte risk komitesinin öngördüğü. Bunlar için de üçer aylık dönemlerde bir değerlendirme yapılıyor. Üçer aylık dönemlerde risk komitesinde denetim planı hakkında bilgi veriliyor.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Denetim planımız uluslararası iç denetim standardına uygun modellerle ilerliyor. Risk bazlı bir planlama söz konusu. Kurumun sahip olduğu tüm operasyonel süreçlerin içerisinde bulunan riskleri tanımlayarak bu risklerin kuvvetini ölçümleyen bir metodolojiyle hangi alanlara odaklanmamız gerektiği ortaya çıkıyor. Bu alanları da yıllık periyod yıllık iş günlerine bölümleyerek oluşturuyoruz. Bunun dışında zaten dediğim gibi genel merkeze bağlı bir ekibiz biz her ülkenin zorunlu kendi kontrolleri var. Dediğim gibi borsaya kote olduğu için Sarbanes Oxley yasalarına uygun denetim çalışmaları yapılmak zorunda ve o kontrollerinde etkin ve verimli bir şekilde işlediğini her market yani her birimin kendisi raporlamak zorunda genel merkeze biz de bunları yapıyoruz. Yani zorunlu olduğumuz kontrol listesinde zorunlu olduğumuz anahtar kontroller ve takip etmemiz gereken kontrolleri her yıl test ediyoruz.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Şöyle zaten üçer her 'quarter'ın sonunda şirketin idari takımı olarak adlandırılan genel müdür ve direktörlerle bir arada bulununca bizim de içinde bulunduğumuz risk komitesi toplantısı yapılıyor. Burada şirketin 'top risk', 'top 10 riski', 'top 4' uygunluk riski mutlaka ölçümleniyor ve konuşuluyor. Geçen süre içerisinde hem

operasyonel süreçleri hem de denetim sonuçlarında ne gibi bulgularla karşılaşıldı bunu hukuk ve regülasyon bölümüyle beraber değerlendiriyoruz.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Tabi tabi, iç denetim ve iç denetime uygunluk tarafında bunu kabul ediyor yani uygunluk 'compliance' tarafı hem regülasyonlara uygunluk hem de şirket içi prosedürlerinde etik yönetime uygunluğu aslında.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Tabi, çalışanlara her sene başında biz bu senenin kapsamımıza girecek kontrolleri belirlemeden önce 'risk assesment' dediğimiz risk değerlendirme çalışmaları yapıyoruz. Bu risk değerlendirme çalışmalarında 'workshop' niteliğinde yapıyoruz ve kurum kültüründe de var olduğu için bu yaklaşım ve bakış açısı zaten genel olarak kurumun farkındalığı yüzde yetmiş seksen seviyesindedir ve kuruma yeni dahil olan her bir birey de bunun farkındalığı yani kendi müdürlerinden başlayarak bunun farkındalığıyla ve bilgilendirmesiyle işi yapar. Dediğim gibi bunun yaptıkları işin içine girmiş olduğu için kontroller bu onların kaçınılmaz bir durumu oluyor.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Gene burada da şey yapıyoruz uluslararası iç denetim standartları metodolojisinin uygulandığı sıklık kontrolün uygulama sıklığını baz alarak oluşan örneklem sayısından belli oranlar çıkaran metotlar var bu 'head quarter'ın, genel merkezin her sene başında 'instruction'larla iletildiği bir metodoloji ve bu metodoloji sürece uygun olarak bahsi geçen kontrolün sıklığına bağlı olarak örneklem sayısını belirliyoruz ve biz bir yıllık süre içerisindeki denetimlerimizi üç faza ayırıyoruz. Üç faz dahilinde yıllık testleri bitiriyoruz yani şöyle söyleyim sana bu senenin denetimini işte yıl Haziran'da kapanıyor diyelim Mayıs'ta yapıp bitirmiyoruz bunu

Haziran'dan sonraki Haziran'a kadar üç ayrı dönemde bölüm bölüm test örneklemi olarak seneye yayıyoruz.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Bu çok ciddiyle takip edilen bir şey çünkü bahsi geçen bulgular tamamıyla SOX sistemlerine uygun olarak aynı zamanda bağımsız denetim firması tarafından da raporlanan bulgular. Bu sizin borsaya beyan etmek durumunda olduğunuz bulgular. Dolayısıyla bir bulgu tespit ettiyseniz bundan emin olup doğru şekilde raporlamak ve 'as soon as possible' diyoruz, hemen bu bulguyu kapatmak bulguyu yok edici faaliyetlerde bulunmak üzere aksiyonlar aldığımız durumundayız. Dolayısıyla sıkı sıkıya takip edilir, çok canlıdır öyle deyim.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Biraz önce bahsettiğim gibi yıl içerisinde bir takvim var bu da genel olarak üçer aylık dönemlere denk geliyor. Her üç aylık dönemin sonunda bir bildirim yapıyoruz. O dönem içerisinde yaptığımız testlerde bulgularla karşılaştı mı risk çevresinde herhangi bir değişim var mı, bulunduğu ülkede herhangi bir değişim var mı, 'hard topic' çıktı mı, 'quarter'da bir raporlama oluşuyor ama yıl sonunda bir 'sign off', yıl sonunda bir raporlama yapıyoruz final bu yılı bu şekilde kapattık dememiz gerekiyor Genel Müdürlük tarafından onaylı bir şekilde.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Tabi, dediğim gibi genel merkeze bağlı ekibiz biz şöyle düşünün dünyada var olduğu ülkelerde ilgili birimler var ve bu birimler genel merkezdeki ana merkeze bağlıyız ve denetim sonuçlarımızı iş planımızı onlara da raporluyoruz. İş planımızı her gün raporluyoruz dolayısıyla performansımız sıkı sıkıya takip ediliyor.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Günlük operasyonların içerisine girmiş diyebilirim çünkü her bir operasyonel birim muhatap olduğu zorunlu kontrollerin her sene başında bizler tarafından farkındalığında oluyorlar. Kontroller tüm operasyonel birimlere dağıtılıyor. Bizim yıl içerisindeki kapsamımıza dahil ettiğimiz kontrol testinin yanı sıra biz kapsama dahil etmeyiz ama onlar uymak zorunda olduğu kontrollerin işlerliğinden sorumlular ve bunu da dökümantasyonunu sık sık arayla yapıyorlar yani günlük operasyonun değişmez bir parçası.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

İç denetim aslında şirketin tümünden varım en tepeden baktığı şirketin tüm iç müşteri sisteminin yani biliyorsunuz tüm operasyonlar ve süreçler birbirlerinin iç müşterisidir ve veriyi ve bilgiyi bir yerden girer ve bir yerden çıkar dolayısıyla böyle olduğunda kuş bakışı seyredebilen çok kıymetli bir fonksiyon. Bunun en önemli noktası da bunu şirketin üst yönetimi tarafından sahiplenilmesi şayet sahiplenilip yapılan çalışmalar sonrasında hedef aksiyonlar ve bunlar üzerinde tüm birimlerin hedeflerine performanslarına KPI'larına konulursa müthiş katma değeri olan müthiş faydalı sonuçlar üreten bir fonksiyon eğer sahiplenilmezse havada kalan bir fonksiyon. Yönetimin en çok dikkat etmesi gereken şey bu aslında.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok.

Ek 7: G Katılımcısı Mülakatı

- Yaşınız: 33
- Eğitim seviyeniz: Yüksek Lisans
- Toplam iş tecrübeniz: 8 yıl

- Kurumunuzda çalışma süreniz: 4 yıl
- Kurumunuzun sektörü: Sigorta
- Kurumunuzun çalışan sayısı: 260

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Dört kişi, iki tane iç denetçi, bir tane de IT denetçisi var, toplamda dört kişiyiz. Bir kişiye daha ihtiyacımız var.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Direk Yönetim Kuruluna, zaten sigorta şirketleri ve bankalarda iç sistemler yönetmeliği var. Bu iç sistemler yönetmeliğinde iç denetim birimleri öncelikle yönetim kuruluna bağlı olarak çalışır, bağımsızdır. Diğer herhangi bir ilgili genel müdür veya diğer birimlere bağlı olarak çalışmaz diye orada bir madde var. Bundan dolayı sigorta şirketleri ve bankalardaki denetim birimleri direk Yönetim Kuruluna bağlı olur ve oraya raporlama yapar.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleştiriyor?

Bizde yaklaşık mesela örneğin, örnek üzerinden gidersek 2020 yılında 27 tane denetim yaptık, denetim raporu hazırladık öyle bir durum var bir tane denetim başkanı var bizde. Söylemiştim daha önce iki tane iç denetçi, bir tane de IT denetçisi var, toplamda dört kişiyiz. İç Denetim Başkanı, müdür de diyebiliriz başkanlık yapıyor, ünvanı başkan. Bu sorunuz değil ama genel olarak cevap vereceğim kurumu anlamanız için, sonra sorunuzun cevabına geleceğim zaten akışında ilerleyecek durum. Biz de iki iç denetçi var, bir tane IT denetçisi var, bir tane de iç denetim başkanı var, IT denetçisi sadece IT ile ilgili denetimleri yapıyor, şirketin IT denetimlerini yapıyor, bilgi sistemleri denetimi. Ama diğer arkadaşım ve ben, biz şirketin mali süreç denetimlerini yapıyoruz. Öncelikle ben sayayım mesela denetimleri neler yapıyoruz, mali denetimler dedim, muhasebe mali işler birimi

denetimi, hasar birimi denetimi, bizde hasar birimi var, teknik birim var, teknik birim denetimi yapıyoruz 'resuarance' birimi var, 'resuarance'ın denetimi yapıyoruz, acenteler denetimi yapıyoruz, sonra bizim kanunen zorunlu kılınan bir denetim yapmamız gereken katastrofiks size yabancı gelebilir bu tabirler belki sigortacılık dışında yani sigortacılık farklı bankacılıktan da farklı. Katastrofiksler var, her üç ayda bir yapıyoruz bu denetimi. Oradaki katastrofiksler oluşumu, orada tarifeler var, o tarifelere uyulmuş mu, uyulmamış mı, bir de deprem riski var ülkemizde, onunla ilgili bazı hesaplamalar var, onların denetimini yapıyoruz. Tahsilat denetimi yapıyoruz, iç kontrol risk yönetimi ve uyum birimi denetimi yapıyoruz, teknik servis, teknik birim denetimi yapıyoruz, katastrofiks yapıyoruz. Kurumsal yönetim raporu, bu katastrofiks raporu kanunen zorunlu. Bunu yapıyoruz. MASAK'la ilgili kanunen zorunlu MASAK denetimi yapıyoruz, tahsilat dedik, hasar birimi dedik, hukuk servisi denetimi yapıyoruz, IT dedik, rücu dedik, hasar ve lojistik birimi, idari işler, insan kaynakları denetimi, pazarlama denetimi, mali işler denetimi evet bu şekilde işliyor bizim süreçlerimiz. Biz sigortacılıkta sürekli çalışıyoruz yani sürekli farklı denetimler var. Sürekli kendimizi geliştirmemiz gerekiyor, bir tane değil hepsini yapıyoruz. Bizim mali tablo da bilmemiz gerekiyor, hukuğu da bilmemiz gerekiyor, hasarı da bilmemiz gerekiyor, sigortacılığı da bilmemiz gerekiyor, hepsini bilmemiz gerekiyor. Alan bizde geniş belki diğer şirketlerde mesela bir holding şirketinde iç denetimdeki kişi mali işler denetimi yapar genellikle, çoğunlukla tahsilat ve tedarikçilerin denetimini yapar, 3-4 tane rapor yazar senede, iş biter. Ama bizde öyle olmuyor. Bizde bunlar biraz kanunen zorunlu. Çünkü diyor ki iç sistemler yönetmeliğinde sigorta şirketindeki tüm birimlerin denetimleri yılda bir kez yapılır. Böyle olduğu için bizde hepsini denetlemek zorundayız. Ama muhtemelen değişecek bu biraz süreç denetimine dönecek, yeni bir yönetmelik taslağı var. Ondan sonra aslında süreç denetimi olduğu zaman bizim işimiz biraz daha rahatlayacak, daha özgür bir yapı olacak. Belki daha özgün raporlar ortaya çıkacak çünkü şimdi biraz daha yoğun bir şey oluyor belki gerektiği kadar bir konunun üzerine değinmiyoruz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Yılda bir kez yapılıyor. Ocak ile Mart arasında en geç bitmiş oluyor çünkü yönetim kurulu toplanıyor. Aslında Ocak ayında yapıyoruz ama yönetim kurulu en geç Mart ayında bunu onaylıyor. Biz o takvime göre raporlara başlamış oluyoruz. Önceki yıldan kalan raporlarda olabiliyor çünkü devam eden raporlar olabiliyor. 2022 denetimine Mart ayı itibari ile başlamış oluyoruz çünkü o arada bir, iki aylık süre önceki yıldan sarkan, devam eden işler ve süreçler oluyor. Çünkü biz bir rapor yazıyoruz, bir bilgi soruyoruz, bir ay sonra cevap geliyor. Yani o da rapor bitmemiş oluyor o zaman, süreç böyle uzuyor.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Öncelikle yılın başında denetim takvimini oluşturuyoruz. Denetim takvimi oluşturulurken risk değerlendirmeleri yapıyoruz. Bir risk değerlendirme, süreç bazlı risk değerlendirme tablomuz var. Hangi süreçler ne kadar riskli? İşte bunun mali riski nedir, yasal riski nedir, uyum riski, itibar riski bunlar nedir? Onların bir puanlamasını yapıyoruz biz. Puanlamasına göre takvim belirliyoruz. Takvim belirdikten sonra süreç plana geçiyor. Bu planlama aşamasında öncelikle biz o takvimde belirtilen örnek vereyim, bir örnek üzerinden gidersek daha iyi olur. Mesela bir muhasebe birimini denetleyeceğiz, muhasebe biriminin yaptığı işleri denetleyeceğiz, bununla ilgili bir ön çalışma yapıyoruz. Diyoruz ki işte bunlar hangi alanlar, prosedürlerini inceliyoruz tekrardan çünkü değişebiliyor, prosedürlerine bakıyoruz. Bu prosedürlere uygun mu, uygun değil mi, öncelikle bununla ilgili, sonra müdürümüze sunuyoruz. Diyoruz ki bizim planlamamız bu şekilde, şunları şunları denetleyeceğiz, şunlara bakacağız, bunları riskli görüyoruz. Bizim risk matrisimizde de bunlar riskli alanlar. Siz bunu uygun görüyor musunuz? O da diyor ki ben bunu uygun görüyorum ya da şunları düzeltin, bunları yapın, daha sonra rapor yazılma aşamasında iken, ben süreci biraz daha anlatayım, böyle soru cevap gidince şey olmuyor. Biz şimdi ön çalışmayı yaptık, müdürümüze sunduk.

Müdürümüz bu ön çalışmayı onayladı, bundan sonra ilgili birime mail gönderiyoruz. Diyoruz ki biz muhasebe biriminizi denetleyeceğiz, bununla ilgili size soracağımız sorular var. İlk önce onlara soracağımız soruları soruyoruz. İstedğimiz evrak varsa istiyoruz. Evrakla ilgili bir işlem varsa şu evrakları bize getirir misiniz ya da gönderir misiniz? Ama şey var onu unuttum, atladım, mevzuat taramamız var o plana geçmeden önce müdürümüze sunmadan önce mevzuat taramasını da yapıyoruz. Güncel mevzuatta değişiklik var mı? Ondan sonra dediğim gibi o ilgili birimle görüşüyoruz, ilgili birim bize bu cevapları verdikten sonra ya da o aşamada çünkü uzun sürebiliyor yani bazı evrakların gelmesi. Biz saha çalışmasına geçiyoruz. Saha çalışmasında aslında o kontrol noktalarımızı belirliyoruz. Belirlediğimiz o kontrol denetim noktalarımızı prosedürlere mevzuata uygun mu değil mi diye biz inceleme yapıyoruz. Bu incelemede daha sonra biz raporlarımızı word veya diğer programlar üzerinden yazmıyoruz. Bizim 2017 yılında Türkiye'de belki sigorta şirketleri içerisinde birkaç tane şirkette vardır, biz dijitalleştik. O tarafta bir program aldık 'workrunner' diye. O program üzerinden - o programı da aslında biz geliştirdik, şuan başka şirketler de kullanıyor - biz bu süreçlerin hepsini, anlattığım şeylerin hepsini, birkaç mail hariç hepsini oradan yapıyoruz. Mesela biz oraya oradaki süreçleri giriş yapıyoruz. Raporla ilgili giriş yapıyoruz. Oradaki inceleyeceğimiz kontrol noktalarını tek tek başlık olarak yazıyoruz altlarını. Daha sonra incelediğimiz konulara göre dolduruyoruz ve bu rapor öncesi bir döküman, bir taslak rapor oluşuyor. Bu taslak raporu oluşturduktan sonra ilgili birimlerden de cevap aldıktan sonra konu ile ilgili veya bu raporu yazarken de başka sorular sorabiliyoruz mail yoluyla. Daha sonra bir taslak raporu oluşturuyoruz. Bu taslak raporu oluşturduktan sonra müdürümüze sunuyoruz. Yine bir online, o süreç online devam ediyor rapor. Müdürümüz bu raporda düzeltmeler yapıyor veyahut onaylıyor. O aşamada biz şey yapıyoruz, o taslak halini daha onaylanmadığı süreci düşünün, siz müdürümüzün kendi onayı var. O esnadan sonra biz ilgili birimle mutabakat kısmına geçiyoruz. Yani bu rapordaki yazdıklarımızda

mutabık mıyız? Bunlar zaruri olarak yaptığımız şeyler. Yani yapmamız gereken şeyler. Çünkü mutabakat yapılmazsa o Yönetim Kuruluna sunuluyor geri dönüşü biraz zor. Çünkü hatta atlayabiliyoruz bazen bazı şeyleri veya o raporu yazarken ilgili işlem düzeltiliyor, onu raporda ifade etmemiz gerekiyor. Mutabakat yapıyoruz, bu mutabakatı genellikle şu dönemde online yapıyoruz veya yüz yüze de yapabiliyoruz. Şirkete bir veya iki kere geliyoruz. Şirketin büyük bir çoğunluğu evden çalışıyor yüzde 75-80'i. Daha sonra bu mutabakat aşamasını geçtikten sonra eğer bulgu varsa, burada bir bulgu varsa diyoruz ki ilgili birime gönderiyoruz bu raporu yine online olarak. Onlar yine bulguyu online olarak sisteme giriyor diyor ki bu bulguda şöyledir, biz aksiyon alacağız ya da almayacağız. Şu tarihte yapacağız ya da yapmayacağız bu işlemi veya reddediyor. Diyor ki yani ben bunu hiç yapmak istemiyorum. Bundan sonra müdürümüze gidiyor rapor tekrardan o verilen cevaplardan sonra. Bir kapanış toplantısı yapıyoruz müdürümüzle beraber iç denetim birimi raporu yazanlar. Kapanış toplantısı yapıldıktan sonra rapor bitmiş oluyor ve süreç oradan sonra performans değerlendirmeye giriyor, denetim performansı, müdürümüz bizim bu rapordaki göstermiş olduğumuz performansı yine online olarak değerlendiriyor program içerisinde. Bu da bizim yıllık performansımızı oluşturuyor aslında baktığımızda totalde. Çünkü orada şey var işte bu raporu ne kadar sürede yaptı, işte özgün işler yaptı mı, başarılı oldu mu, oradaki performansı 4-5 tane soru var, bu soruları cevaplıyor ve bir puan oluşuyor. Buradan sonraki aşamada ilerlersek raporun şey işlemleri var bu online raporu çıktı alıyoruz. Bunu ciltliyoruz ve bunu yaptıktan sonra yönetici özeti hazırlıyoruz. Yani bunu üst yönetime sunulması için Yönetim Kuruluna bir özet hazırlıyoruz, bu raporu iletiyoruz onlara. Onun haricinde özet rapor sunuyoruz çünkü hepsi 30 sayfa rapor olabiliyor. Özet istiyorlar. Ondan dolayı özet raporumuzu sunuyoruz. Bunun devamında yönetim kurulunun toplanmış olduğu toplantılarda, her ay toplanıyor bizde artık, eskiden üç ayda bir idi şimdi her ay toplanıyor. Bu raporumuzu orada müdürümüz sunuyor. Eğer bulgu ve aksiyonlar varsa, aksiyon alınacaksa bir

konuyla ilgili yönetim kurulunun verdiği direktifler doğrultusunda orada bir aksiyon alınıyor. Aksiyon takibini de yapıyoruz. Aksiyon takibini de ayrıca o program üzerinde aksiyonları takip ediyoruz. Yani aksiyon takipten kasıt şu bir tespit var, bu bulguyu diyor ki Haziran 30'da yapacağım ben. Biz bunu Haziran'a gelene kadar aralıklarla kontrol ediyoruz, yapılmış mı yapılmamış mı diye süreç bu aşamada böyle.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Bunu ölçümlendirmek zor. Olağan durumun dışında bazı riskli alanlar ortaya çıkabiliyor anlık olarak. Mesela kovid, bununla ilgili bir rapor yazıyoruz. Bunun önlenmesi için de yönetim kuruluna sunuyoruz, diyoruz ki bu önlemlerin alınması lazım şirket anlık proaktif davranıyoruz.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Mesela riskli gördüğümüz bir alan var, bu alanı incelemeye alıyoruz çünkü biz o takvime illa uyacağız diye bir kural yok. Mesela Anayasa Mahkemesi'nin bir kararı var sigortacılıkla ilgili çok derinlemesine girmiyorum sizin ilgi alanınızın dışında o kararı verdi, dedi ki ben genel şartları iptal ediyorum trafik sigortası genel şartlarını dedi. İş karıştı bu 2020 içerisinde bundan dolayı hesaplamalar değişti. Şirketin bununla ilgili ayırması gereken karşılıklar farklılaştı. Bununla ilgili iki kere rapor yazdık anlık çünkü büyük bir riskti şirket için. Böyle aksiyon alabiliyoruz yani böyle şeyimiz var bununla ilgili risklere karşı proaktif davranma ve rapor yazma.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Şirket personeline iç denetim ve riskle ilgili herhangi bir eğitim vermiyoruz. Bu zamana kadar verilemedi, farklı eğitimler var ama iç denetim ve riskle ilgili bir eğitim yok.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Bununla ilgili şey var, örneklem denetim metodolojisi diye bir şeyimiz var bizim. O konuyla ilgili denetim metodolojisi. Denetim metodolojisi çalışma yöntemimiz şu şekilde örneğin, işlem kontrolü, günlük işlemlerde asgari kontrol sınırı 10. Yani her gün yapılan bir işlemde 10 gün, 10 tane mesela dosya inceliyoruz, hata tespit. Eğer bir hata var ise mesela 20 tane bakıyoruz, 3 hata varsa 20 tanede 40 tane bakıyoruz. Böyle bir metodolojimiz var, test örnekleme var aylık işlemlerde mesela bir işlem aylık yapılıyorsa bunun kontrolü ile ilgili 5 tane bakıyoruz yine bir hata varsa 10 tane bakıyoruz. O 10 tane içerisinde 3 tane hata çıkarsa 20 tane bakıyoruz, 20 tanede 7 tane hata varsa bu örneklem veya metodu duruma göre değerlendiriyoruz. Yıllık işlemlerde de asgari sınırimız 3 tane ya bu asgari bu, bunun üstünde yapabiliriz asgari mesela yıllık bir işlem var 3 tane bakıyoruz. Hata çıkarsa 6 tane bakıyoruz mesela örnek 6 tanede 3 tane çıkarsa 12 tane bakıyoruz. Böyle bir örneklem denetim metodolojimiz var.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Şimdi bulguya bakış açımız şöyle bizde mesela bulgunun işte seviyesi var. Uluslararası Denetim Standartlarında tespit edilen, uygunluk sağlayan risk derecemiz var. Bu risk derecemizi önemsiz, düşük, orta, yüksek ve çok yüksek olarak beş duruma ayırıyoruz. Bulgu önemsizse veya düşükse zaten yönetim kuruluna bunu ifade ediyoruz raporda ama yönetim kurulu bunu çok dikkate almıyor. Önemsiz ve düşük bulgularsa yine de yazıyoruz biz raporlara çünkü bazen sizin düşük dediğiniz bulgu şu an düşüktür ama bir yıl sonra orta veya yüksek boyuta ulaşabilir bu yüzden raporlarda ifade ediyoruz. Fakat yönetici özetinde onları ifade etmiyoruz. Orta, yüksek ve çok yüksek olarak Yönetim Kuruluna, İç Sistemler Komitesi var oraya sunuyoruz. Onlar oradaki yüksek ve çok yüksek özellikli durumlarda direk ilgili birimlere, Genel Müdür'e, bir sonraki gün Yönetim

Kurulu toplantısı yapıyor orada ifade ediyor bu durumu düzeltin diye acil ve hızlı bir şekilde diğer türlü onların girmediği durumlarda ise zaten biz o bulguları dediğim sistem üzerinden bulgu takiplerini yapıyoruz. Bizim o bulgulara karşı tepkilerimiz şöyle o usulsüzlük ve dolandırıcılıksa durum değişir ama yasal bir şeyi varsa ceza durumunuz varsa veya mali tutar veya bütçe büyüklüğü ile ilgili itibar kaybı dediğimiz durum varsa o zaman durum değişir ama usulsüzlük veya dolandırıcılık ve bu tarz problemler varsa o zaman bizim bakış açımız direk Disiplin Kurulu var oraya ilgili kişinin oraya sevk edilmesi başlıyor, tutanak tutuluyor bununla ilgili süreç devam ediyor ama bizim şirketimizde şuana kadar ben çalıştığımndan bu yana bizim yazdığımız raporlarda usulsüzlük ve dolandırıcılıkla ilgili herhangi bir konu olmadı. Bazı şikayetler olabilir ama büyük bir derecede olmadı bizim şirketimiz biraz hassas bir şirket.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Raporlama biz bütün birimleri örneğin denetliyoruz şirkette aşağı yukarı yirmi tane birim var yılda 20-30 civarı rapor yazıyoruz. Bir birim için bir kere ihtiyaç olursa, bir birim için iki kere olabilir, üç kere de olabilir en az bir.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Yönetim Kurulu ihtiyaç duydu, sizin performansınızı ölçelim diye. KPMG bizim performansımızı ölçtü. Bundan %90-95 oranında başarılı çıktık. Yapmamız gereken bazı konular vardı, onları da yapmış olduk şu anda Uluslararası İç Denetim Standartları'na göre çalışıyoruz yüzde yüz diyebilirim yani.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Biz sürekli denetim yapıyoruz sürekli denetim yaptığımız için yanlış anlaşılmasın birimler yılda bir kez denetleniyor. Biz şirketi her an denetliyoruz bütün birimleri çünkü şey gibi değil örneğin ne şirketi diyelim X gıda şirketi, bizim müdürümüz de orada çalışmış o yüzden oradan örnek vereyim, orada ne var stok yönetimi var.

Mesela orada nedir maliyetler ile ilgili maliyet denetimi vardır, nedir orada pazarlama, suistimal, tedarikçi vardır. 5 tane konusu vardır, onu sürekli yaparlar zaten onların ekipleri 30-40 kişidir ama bizde 3 kişiyle. Biz 1 tane müdürü şey yaparsak müdür rapor yazmadığı için biz 3 kişiyle tüm şirketin birimlerini denetliyoruz. Bu da ben mali işleri her zaman denetleyemem zaten bu öyle bir şey değil. Diğer birimleri denetlemem gerekiyor ondan dolayı sürekli denetim halindeyiz aslında ama ilgili birimi sürekli denetim halindeyiz ama genel olarak denetliyoruz öyle diyebilirim.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

İç denetimin faydası şu kişilerin mevzuata süreçlere prosedürlere uygunluğunun aslında bir kontrolü ve kendilerinin ya da ilgili birimlerinin eksiklerini varsa onların tespiti yoksa onların geliştirilmesine faydalı olan yönetim kuruluna şeffaf bir şekilde şirketin durumunu aktaran bir birim olarak görüyorum ben. Ve Türkiye'deki mesela banka ve sigorta şirketlerinden sermaye piyasası ve şu anda yeni çıkan kanunla şirketlerde zorunlu hale geldi. Bunlar da zorunlu iç denetim, iç kontrol Türkiye'de hepsinde olması gerekiyor, tüm şirketlerde olması gerekiyor aslında böyle bir iç denetim mekanizması olması gerekiyor. En azından 1 kişi çalışması gerekiyor şirketteki, iyi görünsün. Şirketin aslında çalışanlarının yapmış olduğu hataların, eksikliklerin bir göz tarafından kontrol edilmesi ve bunun rapor haline dökülmesi aslında iç denetimin önemli olan noktası burası.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok., bayağı bir konuştuk anlattım süreci. Benim anlatacaklarım bu kadar.

Ek 8: H Katılımcısı Mülakatı

- Yaşınız: 38
- Eğitim seviyeniz: Yüksek Lisans

- Toplam iş tecrübeniz:12 yıl
- Kurumunuzda çalışma süreniz: 2 yıl
- Kurumunuzun sektörü: Perakende
- Kurumunuzun çalışan sayısı: 1.200

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Normalde tam kadromuz 1 müdür, totalde 9 kişi ama şu anda hali hazırda işe alımlar mevcut olarak devam etmekte. Hali hazırda 7 kişi diyebilirim, alınacak arkadaşlarla beraber özellikle saha tarafına 7 kişi. Yeterli buluyor muyum? Tabi her departman yöneticisinin aslında risk problemidir bu. Yeterli bulmuyorum aslında benim bununla alakalı bir denetçi olarak bir görüşüm var, sebeplerimde var yeterli olmamasına. Şimdi perakende de aslında bizler birçok perakende denetiminde hemşerilere alışmaya başladık. Bu da nedir bizler denetimi ikiye ayırıyoruz genel olarak en azından benim kendi denetimlerim boyunca perakende denetimini ikiye ayırdık. Biraz buna iç kontrolde diyebiliriz aslında ama ben yine de iç denetim demeyi tercih ediyorum her ne kadar farklarını bilsem de. Saha tarafını denetleyen ekibimiz var, bir de merkezi tarafı denetleyen ekibimiz var şu anda. Ancak benim hedefim bunu önümüzdeki yıl hibrit bir modele çevirmek. Hibritten de kastım aslında şu hem sahayı denetleyecek ekip arkadaşlarım hem de merkezdeki süreçleri denetliyor olacaklar. Ancak buna bağlı bir iç denetçi arkadaşımız var aslında o tamamen merkez odaklı bir süreç denetimi gerçekleştiriyor ve gerçekleştiriyor da olacak. Neden yetmiyor? Çünkü hızla büyüyen bir firmayız çok ciddi anlamda hem yurtiçi hem yurtdışında atılımlarımız mevcut, mağaza sayılarımız artıyor, denetlenecek alanlar artıyor. Bu sebeple aslında kadromuzda bir noktada şu an hali hazırda yetirebiliyoruz ama hedeflediğimiz planlar çerçevesinde onlar maalesef yetmiyor özellikle. Örnek veriyorum, mağaza denetimi gerçekleştirecek bir ekip arkadaşım olması şu an için tabi pandeminin araya girmesi sonucunda bunu bilmiyorum soracak mısınız ama pandeminin maalesef hayatımıza girmesiyle beraber süreçlerimizde ciddi aksamalar oldu. Bütün iş dünyası gibi bizlere hem

şirketim olarak hem denetim ekibim adına ciddi aksamalara sebep oldu, buna kadro eksikliği dahil.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Yönetim Kuruluna bağlı çalışıyoruz bizler. Yönetim Kurulunun da talebi doğrultusunda aslında isteği doğrultusunda diyebiliriz.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Aslında ben denetimi ikiye ayırıyorum. Birisi operasyonel denetimler bir de diğerleri, yani diğerleri dediğim aslında süreç denetimlerimiz ve finansal denetimler diyebiliriz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Yönetim Kurulunun da talebi doğrultusunda aslında isteği doğrultusunda senede ortalama üç tur çıkarmaya çalışıyoruz. Üç turdan da kastım şu 250 mağazanın yılda 3 kere denetlenmesi gibi işte buna göre yıllık bir takvim oluşturuluyor.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Aslında biraz önce bahsettiğim gibi ben denetimi ikiye ayırıyorum. Birisi operasyonel denetimler bir de süreç denetimlerimiz ve finansal denetimler diyebiliriz. Şimdi biz bu denetimleri aslında nasıl önceliklendiriyoruz ve planlıyoruz diyecek olursanız, ilk hedefimiz yine operasyondan bahsedelim. Belirli bir mağaza sayımız mevcut ve bunların da yerinde denetimi gerekli. Bir 'check-list'imiz var ve her yıl güncel dediğimiz yani güncellemekten kastım sürekli planların değiştiği değil ama içerisinde oynamaların da olduğu veya çıkartılan ya da eklenen bir 'check-list'inde olduğu, her yıl yıl sonunda 'check-list'imizi güncelliyoruz ve ona göre önümüzdeki yılın 'root'unu planlıyoruz. O 'root'tan kastım şu; Yönetim Kuruluna bağlı çalışıyoruz bizler. Yönetim Kurulunun da talebi

doğrultusunda aslında isteği doğrultusunda diyebiliriz, senede ortalama üç tur çıkarmaya çalışıyoruz. Üç turdan da kastım şu, 250 mağazanın yılda 3 kere denetlenmesi gibi işte buna göre yıllık bir takvim oluşturuluyor. Bu takvimde de ekip arkadaşlarımıza zamanları planlıyoruz. Hangi mağazalara kimler gidecek, hangi günler gidilecek gibi böyle bir takvim oluşuyor. Bu dediğim gibi normal hayatımızdan bahsediyorum. Bu arada pandemiyle alakalı hiçbir şey belirtmicem bu sürede, bu operasyon ayağı bu şekilde ilerliyor. Yılda ortalama 750 civarı bir denetim yapmaya çalışıyoruz. 250 çarpı 3 gibi yurt içine yapıyoruz. Yurt dışına da böyle gideceğiz, denetimler başlayacak ama ben şu an hala hazırda olanı anlatıyorum size. Diğer tarafta süreç denetimleri aslında nasıl yapılıyor? Orada da bana bağlı olarak çalışan ekip arkadaşımız var ki daha önceden de ekip arkadaşlarımız vardı merkezi süreçleri denetleyen. Burada aslında ayırımımız birazcık da Yönetim Kurulu Başkanı'mızın yani aslında şirket kurucumuz, onun istekleri doğrultusunda biraz ilerleyip, önceliğimizi aslında onun isteklerine ayırıp daha sonra da bizler normal bir rutini planlıyoruz. Şu anda yine maalesef pandeminin araya girmesiyle bu planlarımızda aksamalar oldu ama normal hayatta nasıl işliyordu peki, normal hayat şu şekilde işliyor. Bizim örnek, haftalık veya aylık periyotta bir yaptığımız aslında rutin kontroller var. Bunlar neler; kasa sayımları, banka talimatları, masraflar gibi düzenli olarak yaptığımız bunlar var. Bir diğeri de bu konuda ekip arkadaşlarımla çalışmayı severim neleri önceliklendirelim? Örnek olarak bir ekip arkadaşım var, aramıza yeni katıldı, onunla da oturduk aslında istişare yaptık. Biz bundan sonra hangi denetimleri sürekli ele alalım gibi. Çünkü burada süreç denetimlerini şu şekilde ele almalıyım lütfen. Yani biz bağımsız denetimlere girelim, finansı komple denetleyelim, çıkalım şeklinde süreçle ilerlemiyoruz veya biz girelim insan kaynaklarını komple denetleyelim değil işte burada sizin sormuş olduğunuz noktaya geliyor. Finansın önem derecesindeki veya suistimal içerebilecek hususları nelerse yani finansın bir kolunu inceliyoruz gibi düşünün. Yani takvimimize onu alıyoruz veya insan kaynakları işte bordro tarafı diyelim. İnsan Kaynaklarına baktığın zaman çok geniş bir kapsamı içeriyor. Bunun içerisinde ama bizler bunun risk derecelendirmesi gibi

düşünün, bordroyu alıyoruz gibi düşünün bu şekilde aslında ilerliyor. Evet yani 2022’de asıl gerçek hayatımıza normal rutinimize dönüyor olabileceğiz. Sebebi de şu orada önceliklendirdiğimiz ne olacak Yönetim Kurulu Başkanı’nın ilk planı isteği doğrultusunda bunlar ele alınıyor olacak. Ama onun haricine yıllık periyotta denetimimize risk içeren birimlerin veya işlemlerin hususları takvimimize alıyoruz. Onun haricinde de yine örnek olarak tedarik departmanının bütün süreçlerini denetlemeye girmek gibi aslında genel denetimler, genel süreçleri de gerçekleştiriyor olacağız burada. Şu anda net olarak şunu sizlerle paylaşamam yani paylaşamam deyip paylaşmayacağım gibi algılanmasın. Net olmayacağı için aslında paylaşmıyorum. Sebebi de şu ben size diyebilirim ki bir senede üç tur sürekli denetim yaparak sonra süreç denetimi yaparız diye ama tamamen sizi kandırmak olur çünkü bu konuda netliğimiz olmayabilir. O sebeple aslında size burada rakam vermiyorum ama şunu vurgulamak isterim ki her zaman önceliğimiz, birinci hedefimiz burası, Türkiye şirket kurucumuzun, Yönetim Kurulu Başkanı’mızın istekleri bir bu, ikincisi risk içeren hususlar. Sürekli takvimimize aldığımız ve aslında devam ettiğimiz hususlar dediğim gibi bunlara kasa, banka talimatları aynı zamanda masraflar gibi bunları düşünün. Onların haricinde de yıl içerisinde belirli birimlerin denetimi biz bir yıl içerisinde bu arada belirtmek isterim her departmanı denetlemiyoruz. Yani denetim departmanı olarak ben bu arada kendi departmanım adına konuşuyorum bunu da tekrardan vurgulamak isterim, her departmanı denetlemiyoruz. Belirli departmanları, örnek olarak bu sene finansla, insan kaynakları dediğim gibi spesifik noktaları haricinde tedarik departmanını denetledik, görsel departmanı denetledik gibi genel denetimden bahsediyorum. Önümüzdeki sene IT’yi alıyoruz, pazarlamayı alıyoruz gibi düşünün çünkü şu anda da kısıtlı bir ekibimiz olduğu için yani merkezde kısıtlı bir ekibimiz olduğu için şu anda genel olarak İç Denetim Yöneticisi arkadaşımız işin ağır kısmını yürütmekte ve tabii haliyle bir departmanın denetimi baktığımızda uzun sürebiliyor. Bu sebeple de aslında 2022 de hibrit modele dönüyorum. Sahadaki bulunan denetçi arkadaşlarımızı süreçlere de dahil edip onlara aslında bu işi mesleki olarak öğretip, hem bu süreçte bizim merkezdeki yükümüzü de hafifletip denetim sayımızı

arttırmak, bir taraftan operasyonun devam etmesi bir taraftan denetimin devam etmesi olacak.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Biz hali hazırda aslında departman olarak iç kontrol yapıyoruz da diyebiliriz. Yani olay sadece bizim iç denetim gerçekleştiriyor olmamız değil. Aslında mesleki olarak burada iç kontrol de gerçekleştiriyoruz. Ne gibi faaliyetlerle aslında bunu yerine getiriyoruz diyebiliriz? Şimdi örnek, her birimin altındaki alt süreçleri denetlerken aslında oradaki açık kalan hususlar, risk olabilecek noktaları aslında keşfediyorsunuz. Örnek olarak, bir departmanı denetlemeden önce bir açılış toplantısı gerçekleştiriyorsunuz, açılış toplantısıyla beraber aslında o birimdeki insanların ne işler yaptığını, sistemselsel olarak ne işler yaptığını, sorumluluklarını, onların yetkilerini öğreniyorsunuz ve burada da aslında süreçlerde o kişinin sorumluluklarını gerçekten yerine getirip getirmediği veya fazla sorumluluk aldığı, fazla yetki aldığı gibi sistemselde bir arada geçerli sadece fiziki değil aslında bunları gözlemlene imkanı oluyor. Bu gözlemlenmeyle birlikte aslında çapraz kontrollerin yapılıp yapılmadığı, üst yönetim onaylarının yapılıp yapılmadığı, buna dair aslında riskleri görebiliyorsunuz. Aslında tek bir kişinin her şeye yetkisinin olduğu riskler, hususlar varsa bunları tespit edebiliyorsunuz. Bunu önlemek için aslında önerilerde bulunup, bunları ‘follow-up’ denetimleriyle beraber ne derece uygulandığını görüyorsunuz. Denetim bu açıdan hepimiz yani departmanımız adına birçok noktada aslında doğru nokta atışlarıyla ilerliyor diyebilirim. Burada da aslında gördüğümüz yegane şeylerden biri denetim neyi sağlıyor, her zaman biliyorsunuz denetçiler şirket prosedürlerini çok severler. Neden severler? Oradan soru çalarız, onlar çerçevesinde aslında işlemlerin uygulanıp uygulanmadığını kontrol ederiz. Burada da işte sizin söylediğiniz noktaya en büyük yardımcı husus bu prosedürler bir kere ilgili departmanların ilgili süreçlerin prosedürleri var mı, şimdi en önemli hususlardan biri bu, bunları inceleriz var mı, yok mu. Yoksa yazılı olmalı, önerilerde bulunup bu konuda departman olarak da destek sağlıyoruz. Yani

danışmanlık faaliyeti anlamında. İkincisi varsa güncel mi, yani güncelliğini yitirmiş mi, var, güncel uygulanıyor mu, doğru uygulanıyor mu, bunların kontrollerini sağlıyoruz. Çünkü hepimiz ister istemez bu süreçlere denetçiler olarak hakim olmak zorunda olduğumuzda ilk olarak aslında bu noktayı incelediğimizde açık risk içerebilecek hususlar varsa zaten ilk tespitleriniz buradan itibaren gelmeye başlıyor. Daha sonra sistemsel yetkileri kontrol ediyorsun. Sistemsel giriş yetkileri, değiştirme yetkileri veya silme yetkileri diyelim, departmanlarda bunlar kimlere ait veya gereksiz yetkiler var mı, görme yetkisi bile dahil buna bırakın değiştirme, silme gibi süreçleri, görme yetkisi de var mı gibi bunların kontrollerini aslında yerine getiriyoruz. Riski önleyici birtakım faaliyetlerde bulunuyoruz. Bizim şirketimizde şöyle bir noktada var, parasal hususları yani finansal hususları içeren noktalarda çok ciddi bir mekanizma var. Şirketin en üst Yönetim Kurulu Başkanı'na kadar ilerleyen bir mekanizma var. O mekanizmadan da kastım şu; şu anda bizde birçok aslında uluslararası ya da global firmaların yaptığı şey üzerinden ilerlemiyoruz. İmza yetkileri dahilinde örnek veriyorum, şu kadara kadar bu kişi, bu kadara kadar bu kişi, bu kadara kadar bunlar bunlar gibi ilerlemiyoruz. Bizde onlar hemen hemen finansın Genel Müdürü'nün ve Yönetim Kurulu Başkanı'nın bilgileri ve onayları dahilinde ilerleyen bir süreç var şu anda. O yüzden oradan çok fazla bir şeyin çıkabilme ihtimali kolay kolay doğmuyor. Bunun haricinde biz tabii ki yine söylüyorum banka talimatlarından tutun da finansal riskleri içerebilecek hususlara, sistemsel kontrollerle yani tutarsal önceliklendirme veya örneklem yollarıyla, derecelendirme yollarıyla aslında kontrollerini sağlayıp buna göre risk içerebilecek hususları da ilgili departmanlarla paylaşıp o şekilde ilerliyoruz.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Şöyle denetim olarak ben her zaman şunu savunuyorum aslında. Bir nevi de kural gibi ama bizler tespit eden tespitiyle beraber onları da 'follow-up'ını yerine getiren bir departmanız, önlem alan bir departmanız, yani danışmanlık yapan bir

departmanınız. Ama eğer sorunuza yanlış algılamadıysam biz bir icra mekanizması değiliz. Biz sadece o tespitlerin yapılıp yapılmadığının kontrolünü yapan tarafız. Ama icra mekanizmasına hali hazırda ona dokunan bir departman değiliz ama şu da var aslında söylemiştim gerçekten bizler bir taraftan da ihtiyaç olması dahilinde, talep olması dahilinde prosedürler olabilir, çeşitli bilgi alışverişi olabilir, onu destekleriz ama karar asla vermeyiz.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Ekibim aslında çok genç, yaş ortalaması şu andaki sahadaki arkadaşların yaş ortalaması nereden baksanız 25-26 civarı, çok genç. O yüzden onlar çok yatırım yapılabilir, geliştirilebilir süreçler. Bu sebeple de aslında burada objektif olarak değerlendirmek lazım, saha tarafında yaşlar genç olduğu için o denetim mekanizmasının sürekli üzerinde olup, sürekli bir kontrol etmem gereken bir husus olabiliyor. Burada bir takip noktamızda aslında yani operasyonun 'follow-up'ında biraz aksamalarımız oluyor. Onu da tabii ki iç eğitimle veya çeşitli bilgilendirmelerle geliştirmeye çalışıyoruz.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Genel olarak örneklem diyebilirim. Örneklemeler üzerinden gidiyoruz. Burada risk içeren yani örneklemelerden de kastım aslında o bir. İkincisi tutarsal olarak önceliklendirme diyelim biz ona. Yani önceliklendirmeden de kastım şu; vurguluyorum olay sadece yüksek tutarlara odaklanmak değil, küçük küçük olup, düzenlilik arz edenlerden de bahsediyorum. Genel olarak bizim kontrol ettiğimiz miktarsal ve tutarsal olarak buradaki bir oran analizi, aynı zamanda da diğer tarafta örneklem yoluyla ilerliyoruz.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Aslında hepimizin alışkın olduğu şekilde diyebiliriz. Tabii ki düşünün şahsi olarak da düşünmek lazım. Birileri size sorular sormaya başlarken de ister istemez bir huzursuzluk doğabiliyor, suçsuz da olsanız ve herhangi bir sıkıntınız olmasa bile ister istemez bir rahatsızlık doğabiliyor. Bir de bunu denetimle beraber ilgili departmanların eksik hususlarını, davranışlarını düzeltmesi gereken noktaları dile getirdiğinizde yani işi yapana işi öğretmek istediğinizdeki burada yanlış anlaşılmasın bu arada öğretmekten kastım asla bakın bunu çözmeliyiz, öğretmekten kastım bu yani parmakla işaret etmekten bahsetmiyorum. Yani o eski müfettiş yapısından bahsetmiyorum. Aslında daha güncel bu yönetim tarzından bahsediyorum. Böyle davrandığınızda ister istemez defansif bir algı size karşı bakışlarda o olumsuz bakışları fark edebiliyorsunuz. Oluyor, olmuyor değil. Yani bunu kim aksini iddia etse aslında ben bunun doğruluğuna inanmam. Çünkü bugüne kadar meslek hayatımda bunu aa ne kadar güzel yani bizim bu sorunlarımız varmış, süper, bunları tespit ettiniz, elinize sağlık diye neşeli hal ile davranan kimseyi ben görmedim. Tabii ki şu da var, aslında şunu vurgulamaya çalışıyoruz bizler denetim ekibi olarak, şunu yapmıyoruz; bakın bunlar sizin hatalarınız, bunları yanlış yapıyorsunuz, bunları düzelteceksiniz gibi bir şey değil. Şu her zaman vurgulanıyor bizde, biz her zaman ekip arkadaşız, biz bu şirket altında toplandık ve bu çatı altında beraber çalışıyoruz. Eğer yanlışlarımız veya aksayan taraflarımız varsa bizler bunu düzeltmek için varız, burada yol göstericilik için varız aslında her zaman vurguluyoruz. Ama tabii yine başa dönecek olursak bizler bırakın suistimali normal yapılan hatalar ve aksayan taraflar veya yapılmayan noktaları da departmanlara aktardığımızda ister istemez biraz orada algıda olumsuz bir algıyla karşılaşabiliyorsunuz.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Şöyle aslında raporlamamız biz yine benim yönetim sürecimle alakalı bir hususta olabilir bu. Yani standartlardan bahsetmicem size tamamen subjektif olarak buradaki ilerleyişten bahsedeceğim, yine söylüyorum bizim iki yapımız olduğu için hem merkez hem saha burada değişkenlik gösterebiliyor aslında. Şimdi bizler saha tarafında da bu güncel süreçleri daha aplikasyon üzerinden denetimler gerçekleştirerek orada bir raporlama mekanizması kurduk. Yani telefonlarımızda yüklü bir aplikasyon var. İçerisinde 'check-in', 'check-out'un yapıldığı, 'check-list'in bulunduğu, fotoğrafların eklendiği, çeşitli departmanların işaret edildiği bir aplikasyon var, bir 'check-list' var. Buradan düzenli olarak mağazalara gidildiğinde, denetim yapıldığında, puanlaması da puantajı da çıkıyor. Raporlar ilgili birimlere gidiyor gibi düşünün, burada düzenli bir raporlama var ve bu raporlamada haftada bir Yönetim Kurulu Başkanı'mıza benim tarafımdan yapılıyor. Yani hangi mağazalara gidildi, kaç puan alındı, riskler neler gibi bunlar yapılıyor. Bir de diğer tarafta yine merkeze dönelim, merkezde tamamen o işin bitmesiyle odaklı raporlama yapılıyor. O sürecin denetiminin bitmesiyle odaklı. Bunun haricinde genel bir raporlama gibi bir sürecimiz yok. Yine saha tarafında her periyod bittiğinde dönem bittiğinde bir bilgilendirme raporlaması oluyor. Karşılaştırma raporları oluyor ama diğer tarafta tamamen işin 'term'inin bitimiyle beraber bir raporlama sistemimiz mevcut.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu?

Denetleniyorsa nasıl?

Direkt olarak söyleyeceğim hayır. Yani bu konuda çok netim. Şöyle tabii ki denetimin denetlenmesi, denetimin performansı bu konuda çok önemli mi? Evet, kesinlikle önemli. Ancak şirketimizde daha o denetimi denetleyecek veya denetimin performansını ölçeklendirebilecek bir yapıda maalesef değiliz, keşke olsa. Çünkü aslında bakarsanız burada olmasını da şu sebeple isterim, hem ekibimle beraber çok güzel işler çıkartıyoruz ama sonuç itibari ile o performans ölçütümüz

olmadığı için ki bu noktada aslında şirket yönetimine de gerekli bilgilendirmeler yaptım, ölçeklendirme neye göre alalım, gerekli 'term'lerinden tutunda biz kendi 'KPI'larımızı belirleyelim. Bu konuda gerekli bilgilendirmeleri yaptım. Tabii ki çok isterim çünkü denetiminde bir şekilde bizler bu arada çoğu departman gibi aslında biz de buradayız, bakın biz bunları yapıyoruz sürekli aslında noktası da olmuyor değil çünkü biz de buradayız, biz de bu işleri yapıyoruz, sürekli bu işleri yapıyoruz diye genel bir raporlama yapıyoruz ama bizim ettiğimiz cümle herhangi bir denetlenmemiz veya performansımızın ölçütlenmesi gibi bir durum şu an için yok.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Bu aslında finansal olarak risklerin ortaya çıkmasıyla beraber aslında Türkiye'de de iç denetimin önemi ortaya çıktı ve özellikle halka açık firmalarda iç denetim departmanlarının kurulma zorunluluğu bunu diğer şirketlerde aslında neredeyse biraz zorunlu hale getirdi. Bu sebeple de aslında denetimin önemi bütün ülke açısından, bütün şirket demeyelim ama Türkiye'deki çoğu firma, yerel firma açısından da aslında ortaya çıktı ve bunun bu devamı denetimin sürekliliği hiçbir zaman kişi bazlı değil tamamen departman bazlı sürekliliğin de önemi ortaya çıktı ve bu açıdan da şirketler bana soracak olursanız bu önemi anladıklarından dolayı da her zaman denetim departmanının devamlılığının ve sürekliliğinin devam etmesini istiyorlar. Bu yolda da aslında önlerinde bir taş varsa Yönetim Kurulları özellikle bu taşları kaldırmaya da çalışıyorlar.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Şirketlere tabii ki fayda sağlıyor muyuz, ciddi anlamda faydalar sağlıyoruz. Aslında bu bir nevi konuşmuştuk sizinle konuşmanın ortasında ama denetim departmanı bu şirketteki riskleri ortaya çıkartarak, bu mali riskler de olabilir, normal süreç riskleri de olabilir, bu riskleri ortaya çıkartıp aslında bu riskleri önlemeye çalıştığı için ve önleyici önerilerde bulunduğu için bir şekilde ne kadar önemli olduğunu da anlıyoruz. Olaya sadece şey gözüyle bakmamak lazım, suistimal gözüyle

bakmamak lazım, tabii ki suistimal önemli. Bunun büyüğü, küçüğü hiçbir zaman olmaz, şirketlere zarar verir. Ama normal insanların yapmış olduğu rutinde de denetim sayesinde tespit edilen hatalar ve eksiklikler giderilebilir. Bu da dip toplamda aslında baktığınızda şirkete çok büyük bir katma değer sağlayabilir. Bu sebeple de dışarıdan, içte olmasına rağmen dışardan bir göz olarak denetim departmanlarının firmaya vermiş olduğu katkı, katma değer gerçekten çok yüksek.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok.

Ek 9: I Katılımcısı Mülakatı

- Yaşınız: 45
- Eğitim seviyeniz: Yüksek Lisans
- Toplam iş tecrübeniz: 22 yıl
- Kurumunuzda çalışma süreniz: 3 yıl
- Kurumunuzun sektörü: Kuruyemiş
- Kurumunuzun çalışan sayısı: 1.000

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

I Yönetim A.Ş'de 3 kişilik bir ekibiz genelde. Bankalar Denetim Kurumu var BDDK-Bankalar Düzenleme ve Denetleme Kurumu der ki; her 200 kişiye, 200 çalışana 1 tane denetçi önerir. Aynı zamanda yurt dışında farklı şirketler var, bunun analitiğini yapmış şirketler, bu şirketlerde yaklaşık 200-250 arasında çalışana bir denetçi düşün der. Uluslararası firmalar bunlar, danışmanlık firmaları. Ama Türkiye'de de BDDK teftiş kurumu dediğimiz bankalara bu şeyi vermiştir, 200 kişiye 1 denetçi düşün. Biz de zaten 650 kişiyiz standartlara uygun bir şekilde 3

kişiyiz aslında. Belki 3, 5-4 kişilik ekipler de kurulabilir. Buçuk kavramı şudur denetimde, siz aslında bir denetim değil bir buçuk denetim yaparsınız. Yani siz bir denetimi tamamlarsınız, süre içerisinde yarım denetimi de, denetimin yarısını da, başka ne bileyim satın alma ya da bilgi güvenliği denetimleri yaparak pas geçersiniz, bir tane denetimde finanstan denetim yaparsınız, bir buçuk denetim yapmış olursunuz ya da bir buçuk dediğimiz o insan gücüyle çalışırsınız. Bu sizin tamamen kurduğunuz ekiple alakalı bir şey. Ekibiniz güçlüyse siz de güçlüsünüz. Ekip güçsüzse siz de güçsüzsünüz. Yani yeniden sıfırdan öğrenen bir ekibiniz varsa siz güçsüz bir ekipsiniz diyebiliriz aslında. Ama biraz tecrübeli bir ekibiniz varsa siz daha hazır bir ekipsiniz diyebilirsiniz. Yani bu işler denetim camiasında böyle. Yani biz tabi eski şirketimde denetçi yardımcısından başlayarak işe alımları yapardık, orada yetiştirirdik elemanları, daha öncesinde yani 2016 öncesinde denetçi yardımcısı da almazdık, direk denetçi alırdık. Daha hazır adamlar getirirdik. Ondan sonraki süreçte, 2016'dan sonraki süreçte denetçi yardımcısına giderek aslında biz orayı okul haline getirmeye çalıştık. Burada bir okullaşma durumumuz olmuyor maalesef. Çünkü kurumsal bir şirketteyiz daha çok parasal etkiyi hesaplamamızı isteyen yapıdayız. Fon şirketi I Yönetim A.Ş.. Dolayısıyla bizden daha çok süreç düzeltme ve aynı zamanda parasal etki hesaplayarak şirketlerin kendi şirketleri içerisinde ne diyelim gelir arttırıcı gider azaltıcı faaliyetlerine odaklanmamızı isteyen bir yer. Ama genelde denetçiden beklenen budur. Yani geliri arttırmanızı gideri azaltmanızı beklerler patronlar ama bunu her zaman yapamazsınız. Aman zaman zaman siz geliri de azaltırsınız, gideri de arttırırsınız.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Buradaki yapımızda iç denetim Yönetim Kurulu'na bağlı. Yönetim Kurulu'nun onayıyla istediğimiz herkese raporlama yapabiliyoruz. Bizim Yönetim Kurulu'muz bir süreliğine kendisine raporlama yapmamızı istedi. Yaklaşık 1 yıldan fazla 1,5 yıldır da doğrudan CEO'ya raporlama yapıyoruz. Yönetim Kurulu sadece yılda iki kere raporları okuyor ve varsa yorumlarını yapıyor. Yani 'conflict' oluşmuyor. Raporları okumasa ve yorum yapmasa 'conflict' oluşur. Direk CEO'ya bağlı olmak

dođru deđil çünkü sizde tahmin etmişsinizdir ama yorum bizde toplantılarda yaptığı için burada biz bir ‘conflict’ görmüyoruz. Yönetim Kurulu madem doğrudan CEO’ya bađlı çalışmamızı istedi, doğrudan raporlamamızı istiyor, bizde bu çerçevede Yönetim Kurulu’nun kararına saygı duyuyoruz. Ama olması gereken yapı aslında bir bađımsız bir birim tarafından iç denetimin yönetilmesi. Yönetim Kuruluna bađlı olarak Denetim Komitelerinin olmasıdır. Ama şirketimiz yapı olarak küçük olduđu için böyle bir komite kurulmadı. Doğrudan Yönetim Kuruluna bađlı olarak çalışma esaslarında çalışıyor ama fiiliyatta doğrudan CEO’ya bađlı oluyor şu an.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Deđiştiriyor ihtiyaçlar doğrultusunda. Gidiyoruz önce finans denetimleriyle başlıyoruz, bilgi güvenliği dediğimiz bilgi işlem denetimlerine geçtik, daha sonra satış birimlerini denetledik, satın alma birimlerini denetledik, şimdi tekrar satış birimlerinde distribütörleri denetliyoruz. Bu kendi planı oluyor, o senenin risklerini deđerlendirip, risk deđerlendirmesi yapıp dolayısıyla riskler üzerinde konsantre olduktan sonra ne tür riskler var ve bunları nasıl ‘intigate’ ederiz yani nasıl azaltırız hangi aksiyonları vermek gerekir bunun üzerine şirketi tabiri caizse zorluyoruz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Denetim planları normal koşullarda geleneksel denetim yapan birimlerde yılda bir kez oluşturulur bütçesi de Eylül, Ekim gibi yapılır. Yeni yıl planlanır. Eylül, Ekim, Kasım risk deđerlendirmesi yapılır. Risk deđerlendirmesinden bir sıcaklık haritası çıkartılır. Sıcaklık haritasının sonunda bunlar denetim evrenine gider. Denetim evreni ortaya çıkar. Yani hangi sıcaklıkta yerler var yani o kırmızı olan yerler bizim için buradan seçelim, biz bir denetim evreni oluşturalım. Bu galaksiden şu yıldızı alalım, bu galaksiden şu şu gezegeni alalım, şu kuyruklu yıldızı alalım gibi kırmızı bir harita oluşur. Denetim evreninden de denetim planı çıkar. Denetim evreni dediğimiz şey belki bin satırlık bir şey. Denetim evreni çıkar o bin satırdan. Siz

bunlara sahip, yıllara sair, belki sadece 100 tanesini seçerseniz, o 100 tane denetim içerisinde de yıllara sair bitirmek, 100 denetimi bitirmek, belki sizin 10 yılınızı alır anlatabiliyor muyum? Belki siz yapmayacaksınız o denetimi, denetim planının da bir yandan revize edilmesi gerekir çünkü bu mantık geleneksel mantık buraya kadar. Bir de modern teknikler var şimdi geleneksel mantıkta her şey kitabi bir şekilde çok güzel geldi değil mi size? Yani aslında çok sorunlu bir yapı bu neden? Siz çünkü Eylül'den Eylül'e, Ekim'den Ekim'e hiçbir şey yapmadan, tek bir denetim planıyla gittiğiniz zaman çevikliği kaybediyorsunuz. Aslında hiçbir denetim planı yoktur ki bir gün önce vermiş olduğun karar, bir kelam değil. Yani bunu siz değiştirmekle mükellefsiniz denetçi olarak. Bir gün önce artık geçti ve yeni bir şeyler söylemek lazım diye bir şey varya aslında her gün yeni şeyler söylememiz lazım. Dolayısıyla sizin aslında geçmişi çok iyi okuyup, yoğurmanız lazım. Geçmişi iyi okuyunca geleceği de aslında bir şekilde yönetmeyi en azından beceremeseniz bile bir şekilde cesaretiniz artıyor. Dolayısıyla siz planı yapacaksınız ama o plana yeri geliyor uymayacaksınız. Bu hani o şeyi anlatabiliyor muyum orada bir direniş göstermekten bahsetmiyorum, plana uymamak. Plana uymak çünkü tembellik. Plana uymamak esas meziyet, fark yaratmak buradan geliyor. Biz şu anda çevik sistemi uyguluyoruz. Çevik sistem benim yurtdışında da Türkiye'de de anlatmaya çalıştığım, hani genç arkadaşlara da iletmeye çalıştığım, hiç böyle bir şey duymamıştım diyorlar. Duymamıştın zaten ben söylüyorum diyorum bende. Orada insanlar hani diyoruz ya mutlak değer yöntemini işte biraz önce söyledim ya gelir arttırıcı gider azaltıcı, hayır gelir azaltıcı gider arttırıcı etkisi de sizin denetim planına uymamanız gerektiği gerçeğini insanlara anlatıyorum. Bu da tabi gerçekten çok verimli çok hoş sohbetlere kalıyor bende bunu söylemekten keyif alıyorum açıkçası genç arkadaşlara sizler gibi. Öyle bir yapı. Ee ne oldu peki orayı da açıklayayım. Şöyle yapı içerisinde nasıl deyim size çevik olmaktan bahsettik. Oradaki şeylerinizde değişken yapıyla sizin aslında yönetimin ihtiyacı olan denetimleri hemen uyguluyor olmanız gerekir.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Şöyle ben I Yönetim A.Ş.'ye 2018 de katıldım. Risk haritalandırmasını öyle her sene yapmadım açıkçası söylemek gerekirse. Bir kere yaptım ve 700-800 satırlık bir şey çıktı. Ama eski şirketimde 10.000 satırdı bu risk haritası. Risk haritası kolay bir şey değil. Gerçekten üzerinde durmanız gereken riskler var. 10.000 tane risk çıkıyor düşünseniz, 1.000 tane de bu şirketimde çıktı. Böyle böcek çıkma riski, cam çıkma riski, taş çıkma riski çünkü çekirdek yiyorsunuz içerisinden bir dış malzeme çıkmasını istemez müşteri değil mi ve bundan denetçi olarak yine sorumlusunuz. Denetçi olarak değil de firma olarak sorumlusunuz. Denetçi de tabi buradaki yapılanların kontrol edildiğini, gerçekten burada güvenli bir şekilde üretim hattının işlediğinden emin olmak ve buna güvence vermek ister. Biz denetim planını yaparken oturuyoruz bütün iş birimleriyle konuşuyoruz. Diyoruz ki sizin en büyük riskleriniz neler? Üretim Müdürü'ne yani Fabrika Müdürü'ne, Operasyon Direktörü'ne, Hukuk Müdürü'ne, Pazarlama Müdürü'ne, Satın alma-Satış Müdürü'ne, İhracat Direktörlüğü'ne, Satış Direktörü'ne, hepsine tek tek gidiyoruz. Burada kendilerine tabi ki sorular soruyoruz. Kendilerine birazcık yön veriyoruz. Çünkü onlarda bilmiyorlar ne olduğunu. Risk nedir? Nasıl anlatılır? Hiç bilmiyorlar. 5'li dediğimiz uluslararası sistemde kabul edilmiş bir skala sistemi, risk değerlendirmesi yapıyoruz. Bu skala sistemini girerek riskleri belirledikten sonra bu riskleri aritmetik olarak 'antifiy' ediyoruz. Yani bir risk seviyesi belirlersiniz. Risk 10 üzerinden çok riskliyse ne verirsiniz siz bir riske? Çok riskli bir durum, 10 üzerinden kaç verirsiniz? Çok, çok riskli ama 10 verirsiniz. Bizim skala sisteminde de 5'li bir yapı var. 5 üzerinden 5 veriyoruz çok yüksek katastrofobik bir şeyse. Biraz azsa, yüksek riskliyse 4 veriyoruz. Orta riskliye 3 veriyoruz. Düşük riskliyse 2 veriyoruz. Çok düşük riskliyse 1 veriyoruz. Yani gidip 10'lu sistem kullanmıyoruz. 10'lu skala kullanmıyoruz. Bunu yapıyoruz, önce riskleri belirledik, riskleri belirledikten sonra rakamsallaştırdık. Buraya kadar sorun var mı? (Yok) Şimdi bir de rakamsallaştırdık da neyi rakamsallaştırdık? Neyi

rakamsallaştırdığımız sorusunun cevabı da etkiyle olasılık. Etki risk dediğimiz varlık. Etkiyle olasılık varlığının çarpımından oluşuyor. Şimdi ben dedim ya beşli skala kullanıyoruz diye. 5 kere beş 25, etki beşse riskte yan olasılıkta beşse zaten maksimum verebileceğiniz risk 25. Yani aslında 25’li bir yapıdan bahsediyoruz. En yüksek katastrofik riskimiz 25. 25 alanlar, 20 alanlar, 15 alanlar, iniyor aşağı doğru 10 alanlar, 5 alanlar, 0 alanlar diye. Böyle bir yapı içerisinde siz haritalandırmaya başlıyorsunuz, adresliyorsunuz, risklerinizi puanlıyorsunuz ve filtreliyorsunuz. Bu riskler arasında en yüksek alanlardan belki ilk 100’üne bakıyorsunuz. Anlatabiliyor muyum? Bunları da yaparken iş birimlerine tek tek soruyorsunuz. İnanmak zorundasınız çünkü onlarla beraber aynı gemidesiniz. Artık iç denetçisiniz de bu sizin orada bir şeyi ispatlamanız beklenmiyor. Artık riskleri konuşurken sohbet ediyorsunuz ama belki güvence anlamında belki ufak tefek kanıtlar isteyebilirsiniz. Ama orada hemen kanıt istenmesi gerektiğini düşünmüyorum. Riskleri konuşuyorsunuz, o adam risklerini eğer yanlış anlatıyorsa ve bu arada suistimal yapıyorsa, yakalanacaktır zaten orada mutlaka. Bu çekirge misali bir şekilde ne diyelim o havuza düşecektir.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önlüyor?

Derecesini bilemem, derece dediğiniz kavram çok geniş bir kavram. O yüzden çok uzaklaşmayayım iç denetim aslında şirketlerin bir sigortasıdır. Sigorta şirketleri ne derecede aslında sigortayı karşılarsa iç denetimde oranın aslında o derecede risklerinin önceden karşılanması amacıyla bir sigorta işlemi görür. Risk ortaya çıktıktan sonra denetçi bunu yazmamışsa zaten denetim riski de buna denir. Denetimin de kaçırma riski var yani hem. Yani şey değil para kaçırma değil, bulguyu kaçırma riski var, hata yapma riski var ya da hata da demeyelim, testlerde o ‘material statement’ dediğimiz ciddi seviyede seçim yapmamasından kaynaklı. O ‘sample’ı seçmemesinden kaynaklı tercih riski var. Yani tercih edilmemesinden kaynaklı bir denetim problemi çıkma riski her zaman var. O yüzden zaten denetim

hiçbir zaman bir sonuca tam güvence vermez, mutlak güvence vermez. Her zaman için makul güvence verir.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Sorumluluk iç denetim birimi almaz. Sorumluluk almaktan kaçmaz iç denetçi. İç denetçinin şöyle düşünün iç denetçi bir fotoğrafçı aslında. Fotoğrafi çekmekte ve onu doğru bir şekilde 'top' etmekten sorumlu. Bağımsızdır iç denetçi. Yönetime pürüzsüz bir şekilde o resmi vermekle mükellef. Dolayısıyla aslında denetçi değil burada sorumlu olan üst yönetim. Cevap doğrudan bu yani denetçi sadece bir araç orada, bir fotoğraf makinası aslında denetçi ya da orada 'top' edilecek bir film. Denetçi bu kadar 'pure' yani ama o resme bakıp o resmin gerçekten siyah beyaz olduğunu, bu resmin gerçekten aa bu resmi çekmişsin ama arkada gemi olması gerekirdi, 'gemi nerede?' sorusunu sorması gereken evet denetçi, yardımcı olur ama fotoğrafını denetçi çekiyor ama orada düzeltmesi gereken gemi ile ilgili düzeltme biraz doğru olmadı ama orada gerekli 'adjustment'ları yapması gereken birim üst yönetim. Daha doğrusu iş birimleri diyelim, üst yönetim demeyelim.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Bu şirket açısından soruyorsanız eğitimi ben kendim vermeye çalışıyorum arkadaşlara nazikane. Dışardan bir eğitim almıyoruz sadece şirket içerisinde satış veya satın alma birimlerinin ya da IT biriminin vermiş olduğu eğitimler oluyor. O eğitimlere katılım oluyor. Bunun dışında iç denetim için özel eğitim almıyoruz. Ben arkadaşlara eğitim vermeye çalışıyorum ilgili dökümanları göndermeye çalışıyorum varsa elimde bir döküman hızlıca paylaşmaya çalışıyorum vs. onun haricinde paylaşımımız olmuyor.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Bu biraz uzun bir konu. Çok kısaca özetleyeyim size. Denetim yaparken sizin bir iç denetim rehberiniz var. İç denetim rehberinde yazan testleri uygulamanız gerekir. Rehberde ne yazmışsanız onu yaparsınız. Bakın çalışma usul ve esasları başka bir şey. İşte denetçi şunu yapar, denetçinin görev ve sorumlulukları bunlardır, bu başka bir şey. 'Charter' dediğimiz bir de denetimin rehberi yani nasıl yapacağınız başka bir şey. 'Charter'da çalışma usul ve esaslarında daha doğrusu sizin kime bağlı olduğunuz, hangi raporlamaları yaptığınız yazarken, rehberde her şey yazar, işi nasıl yapacağımızı mesela sizin sorduğunuz soru çok genel bir soru. Ama özel olarak spesifik hale getireyim sizin için, şöyle denetimde zaten aslında bir analitik testler var hatırlayabildiğim kadarıyla, bir de 'substantifik' testler var. Yani analitik test dediğimiz nasıl anlatayım sadece siz analitik prosedürle geçebileceğiniz bir testten bahsediyorum. Karşılaştırma yaparsınız, iki tane varlığı karşılaştırırsınız. Geçen senesi üçtü, bu senesi beş olmuş. Beş bölü üç eksi bir, yüzde kaç arttı? Bu bir analitik testtir. Yani yüzdesini alarak ilerlersiniz. Dikey analiz, yatay analiz, bunların hepsini biliyorsunuz zaten meslek olarak. Bir de şimdi geçen sene üçtü, bu sene beş oldu diyoruz ya bu beş acaba gerçekten doğru mu? Yani rasyonelizasyon test yapıyorsunuz yani detay testlere giriyoruz. Burada analitik olarak geçmiyoruz. Üçten beşe çıktı çünkü bunun sebebi şuydu demiyoruz, artık analitik test yapmıyoruz. Beş ama beş doğru mu ya geliyoruz. Üçten beşe çıktı, yılda şu kadar arttı dememek. Beş gerçekten beş mi, değil miyi test etmek 'substantive' bir test. Yani 'test of details' diyoruz buna. 'Substantive' testler nasıl yapılır? Beşin öncelikle hangi bileşenleri var? İşte beş tane bir den oluşuyor diyoruz. O beş tane bir acaba beş yapıyor mu, onları topluyoruz. Yani 'test of details'e giriyoruz. Bu neyse işte bir mutabakat mektubu mu, bir kira analizi mi her neyse. Mesela rasyonelizasyon testi dediğimiz bunun da detayı var. Burada bir rasyo testi yaparsınız. Mesela bir örnek vereyim size aklınıza yatsın. Bir yerin kirası 1 lira olsun, aylık kirası, yıllık kirası ne kadardır defterde? Bir baktınız 13 lira

yazıyor ama 12 lira çıkıyor sizde değil mi? Rasyonalizasyon testi yani akılcılık rasyo testi yaptığımız zaman 12 Lira çıkıyor ama defterde 13 Lira yazıyor o zaman 1 liralık bir farkımız çıktı, doğru mu? İşte bu sizin çıkartmış olduğunuz bulgu aslında fark. Çünkü farkı yakaladınız. Bu mesela şeyden geldi ‘substantive’ testler yani burada detaya girdim ama siz sorunca ne tür testler yapıyorsunuz diye bu tür testler yapıyoruz. Gidiyoruz mesela bir yerde kira analizi yapacağız ya da metrekare hesabı yapacağız, metrekarede farklı yazıyor, kirası farklı diyoruz ki bakın burada deminki 13 Lira’ya 12 Lira verdiğim örnek gibi düşünün. O 1 Lira’lık fark nereden geliyor diye soruyoruz? Aa doğru söylüyorsunuz böyle farkımızın olmaması lazım gibi kendileri zaten kabul ediyorlar ve orada artık nerede aksiyon alınacaksa o konuda aksiyon alıyorlar.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Bir kere ‘top end the top’ denilen bir kavram var. Yani bu yukarının patronun ya da işte yönetimin kararı ile ilgili bir şey. Yönetim eğer sizin arkanızdaysa kapatılmayan ya da açık bırakılan bulgu diye bir şey olamaz, adam işsiz kalır. Eğer denetimin yazmış olduğu bir şeyse mümkün değil, çok geçerli bir sebebinizin olması lazım. Adam diyecek ki 6 ay sonra kapatacağım ben bulguyu. Buraya bir yatırım harcaması yapacağım, bununla ilgili bütçe alacağım, 6 ay geçti, ee yatırımı yaptım mı, yaptım, bütçeyi aldım mı, evet, bulgu var mı hala, evet var, bir dakika kardeşim sen bize yatırımı yaptırdın, aksiyonu aldırдың, bulgu nasıl var anlat bakalım, hala neden müşteri kaybı var, ya da hala neden müşteri memnuniyetsizliği var, doğru yere mi yatırım yapmadık, alman gereken cihazın gerçekten o kalitede bir cihaz mı almadın, harcamışsın, para koymuşsun ama müşteriler hala memnun değil, oradaysa hesap soran bir kimliği var. Tabiri caizse kötü yüzü yani anlatabiliyor muyum? Denetim sopası diyelim denetim sopası ortaya çıkıyor. Gerçekten hesap sorma, sorumluluk almaktan kaçan bir birimi hesaba getiriyor olmanız lazım. Hesabını veremiyorlarsa da burada onların performansının da tekrar

değerlendirilmesi gerekebilir. Denetim bulgularının şakası yoktur. Bir kere erteler, iki kere erteler, üçüncü de işsiz kalır adam. Siz orada aksiyon aldirmayacaksanız ne işiniz var direktör olarak. Bazen öyle bir durum oluyor ki o aksiyonu kapatarak binlerce müşteri kazanıyorsunuz. Bazen de o aksiyonu açık bırakarak binlerce müşterinin kaybedilmesine imza atıyorsunuz. O yüzden denetçi risk almaz. Denetçi üst yönetime, Yönetim Kuruluna raporda belirtir. Yönetim Kurulu der ki benim için 'okay'. Bulgu açık olmasına rağmen üst yönetimin bilgisi dahilinde kapatılmıştır. Ben size yüksek riskli bulgulardan bahsettim. Düşük riskli bulguları zaten takip edersiniz. Adam belki onu yıllarca kapatamaz. Tabi bizde ona karşı daha müsamahakar davranıyoruz onlar üzerinde. Daha fazla üzerine yürümeyiz adamın, zaten düşük riskli bir şey. Yüksek riskli konuda üst yönetime çıkartırız, yönetimin kararı burada denetçinin yanında olmak mı, adamların yanında olmak mı, hem denetçinin hem adamın yanında olmak mı? Bu üçüncü seçeneğin olmasını beklerim ben hem denetçinin hem adamın yanında olmasını çünkü bu sefer size yönetim ve denetçisi gelmiş gözüyle bakılıyor.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Yapılan her denetimin sonunda denetim raporu yazılır. Yönetim Kuruluna raporlama yapıyoruz. Burada biraz soruşturma, inceleme durumu da var. O yüzden günlük elde edilen bulgular içinde hemen bir rapor yazıyoruz. Yönetim Kurulunun isteği üzerine CEO'ya raporlama yapıyoruz. Yönetim Kurulu yılda iki kere raporu okuyor, varsa yorumlarını yapıyor.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Kendimizi geliştirmek için bir KPI setimiz var. Dediniz ya performansınızı nasıl ölçüyorsunuz aslında iç denetim bir ismi var bunun 'control self assesment' deniyor buna. Kendi öz değerlendirmesini yapıyor. 'Control self assesment' aslında bir standart. Standartlarda bunun yeri var, iç denetim standartlarında. Kırmızı kitapta geçer bu. Kırmızı kitabı vardır iç denetimin. Kırmızı kitapta 'control self assesment'

aslında beş yılda bir böyle kaliteli şirketler kendilerini, iç denetim departmanlarını denetletirler. Gelir bir tane bağımsız denetim şirketi, o şirketin iç denetim birimini denetler. Neler eksik, neler fazla denetim sırasında? Denetim başlamadan önce denetim planını ilgili iş birimleri ile paylaşmış mı, denetim planı için toplantı yapılmış mı, toplantıdan sonra ön rapor aşamasında, ön rapor aşamasını bırakın çalışma kağıtlarının oluşturulması aşamasında denetim çalışma kağıtları doğru bir şekilde toplanmış mı falan filan şeklinde bizi denetler. Burası bu dediğim şey için denetim açısından öz değerlendirme yapacak olursam ben de güçlü değilim bu anlamda. Yani güçlü değilimden kastım bu kadar vaktim bu tip bir öz değerlendirmeye yok. Mesela öz değerlendirmenin bir parçası müşteri memnuniyet anketidir. Yapmıyorum. Karşı geldiğim bir konu müşteri memnuniyeti anketleri işte ne bileyim öz değerlendirme denetim alanlarından bir tanesidir. Denetim sonrasında denetim raporunu alan ilgili iş birimi denetçiye puan vermiş mi, denetime kaç vermiş beş üzerinden. Benim karşı geldiğim bir konu bu. Neden? Çünkü denetim tek taraflı olarak bence değerlendirilmemesi gerekir. Bir de ben müşteri olarak baktığım zaman karşı taraf denetimi böyle avucunun içinde görmüş oluyor. Yani anlatabiliyor muyum? Orada bir algı var. Aa ben şimdi sana puan mı vereceğim, gel bakayım bir diyor, iki diyor, üç diyor ya da bazıları var çok arasını bozmak istemiyor, beş diyor. Hangisi doğru ölçemiyorsunuz bu anlamda. Ben mekanizmanın aslında 360 derece çalıştığından yanayım. Yani ben de puan vereceğim o da bana puan verecek. O bana puan veriyorsa ben ona puan veriyorsam standartlarda yok bu. KPI'larımızdan bir tanesi denetimi zamanında bitirmek. Denetimin kalitesini ölçmek. Denetim kaliteli mi? Orada da gidiyorsunuz üst yönetime denetim raporunu paylaştığımız üst yönetime zamanında bitirilmiş mi, istediğiniz planda işte ne bileyim ortada bir plan var, 11 tane denetim bitireceğim diyorsunuz bir planda ama 9 tane bitirebilmişsiniz. 11 denetimin tamamını bitirememişsiniz bu aslında bir handikap baktığınız zaman. Başka ne var KPI'lar arasında, eğitimlerini almak var, sertifika almak var denetçi KPI'larından bir tanesidir. CIA, CFE, CPA yani SMMM birkaç tane daha var, bağımsız denetim

gibi sertifikaları almak olabilir. Zamanında bitirmek, kaliteli denetim yapmakla beraber sertifika almak gibi bazı ölçüm kriterleri var.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Bir koordineli bir sistem var. Merkezi denetimle de uygulanıyor. Sürekli denetim yapıyorsunuz. Sürekli denetim dediğiniz sistemsel denetimi yapıyorsunuz. Sistemleri açılıyorsunuz SAP' sa SAP , değilse Logo Tiger. Bir konunuz var, tahsilat ya da bir konunuz var, prim hesaplamaları. Sistemdeki prim hesaplamalarını periyodik olarak kontrol edebiliyorsunuz. Yani periyodik olarak sürekli kontrol edemezsiniz tabi. Periyodik olarak kastımız periyodik süre vermeniz lazım altı ayda bir mi, üç ayda bir mi, bunu veriyorsunuz ve orada siz merkezi yani yerinizden hiç kalkmadan Mardin'e hiç gitmeden, Mersin'e hiç gitmeden, Karadeniz'e hiç gitmeden, İzmir'e hiç gitmeden, İstanbul'dan, evinizden kontroller yapabiliyorsunuz sisteme bağlanmak kaydıyla. Bu tür merkezi olarak yapmış olduğunuz 'continuous audit' adı altında sistemsel denetimlerimiz var. Bir de şu var denetim planından bahsetmişim ya hani bir denetim planı çıkartıyoruz ve denetim planına uyuyoruz. Denetim planı denetim evreninden geliyor. Denetim evreninin belki beş yüz tane denetimi çıkıyor vs. yüz tane denetimi çıkıyor işte yıl içerisinde biz on denetim yapabiliyorsak, yüz tane denetimi on yılda yapacağız ama diyoruz ki dinamik olsun. Değiştirilebilir denetim yapısı olsun. Ama yine de ben on tane denetim tamamlayayım. On tane tamamlayayım ama sekiz numaralı denetimi çıkartayım ya da başka birini sekiz numaraya koyayım çünkü on tane denetim zaten benim performansım. Bir insan 8,5-9 saniyeden daha erken koşamıyor değil mi? Yani bu mümkün değil, fizyolojik olarak mümkün değil ya da dünyada Hüseyin Bold 9,5 saniye mi 9,8 saniyemi ne yaptı. Onun altına inilemiyor demek ki insanoglunun da bir kapasitesi var. Denetimde öyle yani denetim iki kişi ile yılda en fazla on denetim yapabilirsiniz. On bir denetim, on iki denetimde zorlanırsınız. Dünya rekoru kırmanız gerekir her zaman da dünya rekoru gelmiyor böyle düşünün. Dolayısıyla merkezi denetim dediğimiz sistem aslında sizin söylediğiniz

şey. İkiye ayırdım ben cevabı, bir tanesi 'continious audit' dediğimiz dünyada kabul edilmiş üç beş senedir uygulanan bizim bir önceki şirkette çalışırken uyguladığımız merkezi olarak, sistemsel olarak uyguladığımız bir denetim tekniği. Bir de rutin denetimler içerisinde yapmış olduğunuz denetimler var. Sürekli dönmeniz gerekiyor aynı konuda ama onlar biraz daha fazla 'nonrutin'. Ama bunlar bu ikinci söylediğim, 'nonrutin'den kastım üç sene de bir döneceğiz belki beş sene de bir döneceğiz biz onlara. Terk ettikten sonra daha sık sinyal göndermeyeceğiniz denetimler olabiliyor bunlar. Yani atıyorum 2018'de yaptığımız bir denetimi 2019 ile 2020'de hiç yapmadık. 2021'de yapmamız gerekiyorsa yapmamız gerekiyor bu da 'continious audit' ama daha süreleri daha uzun 'continious auditler' buna tam olarak 'continous audit' dememek lazım bunlara aslında.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

İç denetimin faydası açıkçası değer katmaya çalışan bir yapıdan bahsediyoruz. Yönetim Kuruluna, ortaklara, pay sahiplerine şirketin aslında bizim açımızdan bakarsak, çekirdeği çitleyen son kullanıcıya sadece çitleyen değil, onu yiyen, leblebiyi yiyen, fıstığı yiyen son kullanıcıya kadar sorumluluğu olan geniş bir yelpazesi olan bir durumu içeriyor. Dolayısıyla sizin aslında bütün bu gruplara karşı tüketiciden tutun burada bir yapıdan bahsettik, bakkal yapısından bahsediyorum. Eve kadar giriyor, insanlar çünkü bu yapı da evlerine kuruyemiş alıyorlar ve bu şirketten alıyorlar. Bu şirketin sizin itibarınızı koruyor olmamız lazım. Tabiri caizse siz, sizin için bu şirketin kalitesi yani sizin için çok önemli olması lazım ve dolayısıyla şirkete değer katan bir birim olmamız lazım, birincisi bu. Şirkete bir değer katarken ana tema değer katmanız lazım. İkinci temalar hep sonradan gelir. Siz değer kattığınız zaman o değer ne olduğu sonradan gelir. Bunlar parasal değerler olabilir, çok büyük paralar kazandırabilirsin ya da çok önemli derecede riskleri engellersiniz. Ne diyelim, ceza riskini engellersiniz. Kanunen kabul edilmeyen giderlerle ilgili işte muhasebe kökenli olmanızdan dolayı hatalı bir muhasebeleşmenin önüne geçme riskinden dolayı ceza gelmemeyi sağlarsınız falan

filan. Bunlar hep alt kalemler, değer değerlerinin altındaki faaliyetlerde bu tür önlemlerdir. Açıkçası siz ne kadar iyi önlerseniz şirketin itibarını o kadar yükseğe çıkartırsınız. Dolayısıyla itibar riskini yönetmiş olursunuz, kur riskini yönetmiş olursunuz, diğer finansal riskleri yönetmiş olursunuz, müşteri memnuniyeti riskini yönetmiş olursunuz, sigorta riskini aslında siz üstlenmiş oluyorsunuz. Bir tür sigorta fonksiyonu gören bir birimsiniz. Bu nedenle iç denetim artık hani bir parasallaştırmadım ama tabiri caizse her yiğidin harcı değil. Dolayısıyla siz alında bir sigorta mekanizması olarak çalışan bir birimsiniz siz. Düşünün artık sigortasız çalışmak mı, sigortalı çalışmak mı? Hani iç denetim sizce neden önemlidir? Sigortasız çalışan bir işçi olarak düşünün kendinizi firmanızda sigortanızı size yatırmasalardı siz çalışır mıydınız orada? İç denetim olmadan tabiri caizse firmalar çok kısa süre belki hareket edebilirler. Bir süre giderler sonra bir yerde motor bozulduğu zaman bir yerde patlayacaklardır. Ceza yedikleri anda tekrar iç denetim birimi kuralım derler. Anlatabiliyor muyum? Böyle düşünün.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Benim söylemek istediklerim bunlar sadece ve sadece denetimi anlatırken insanlara sizde şunu söyleyebilirsiniz benden nacizane birkaç tane tavsiye olsun size. Denetçi at gözlüğüyle bakmaması lazım birincisi. Şimdi bir de tam tersini savunacağım bazen de at gözlüğüyle bakması lazım. Şimdi standartlarda yer alan mutlak değer kavramı denetçi standartlarının koymuş olduğu gerçekten bu konuda hiç ne diyelim şey göstermeyeceği tevazu mu diyelim onu yapmayacağı nokta. Gelir arttırıcı, gider azaltıcının yanında, gelir azaltır, gider arttırır diyorum ya burada stok yoksa stoğu 'life-of' eder. Gider stoğu siler. Ne yaptınız? Gideri arttırdınız, ee hani kar sağlayacaktık şirkete? O yüzden şey veremezsiniz ne diyelim dönem sonu primini karı üzerinden, EBITDA (Earnings Before Interest, Tax, Depreciation and Amortization) üzerinden veremezsiniz çünkü bir denetçi karınızı azalttığı için EBITDA'nızı kısıttığı için siz primlendirmeyi denetçiye ya da şirkete böyle

verirseniz kişiler kaybeder. Yani ben kaybederim açıkçası ben aslında bulmuş olduğum ‘payding’ için cezalandırılmış oluyorum. Böyle bir yaklaşımın asla olmaması lazım. Mutlak değerden kastım budur. Eksi bir şey bulursanız aslında bu pozitifdir burada ‘right-off’ ederseniz aslında o stoğu niçin ‘right-off’ ettiniz, IFRS ya da Türkiye vergi mevzuatına göre aslında siz ceza yememek için o stoğu ‘right-off’ ettiniz. Doğru bir şekilde defterlerinizde o stoğu gösterebilmek, o vergiyi ödeyebilmek için stoğu ‘right-off’ ettiniz. Dolayısıyla sizin için olmazsa olmazlardan bir tanesidir mutlak değer yaklaşımı. Bunu genelde finansçı arkadaşlar iyi bilir. Biz de finansçı olduğumuz için bulmaya çalışıyoruz. Denetim, denetçilere tekrar söylüyorum risk asla ve asla tek yönlü aksiyon ya da KPI veremez. Gideri arttır, geliri azalt diyemezsiniz. Patronlar böyle yapar, burada patronları yermek lazım. Burada at gözlüğüyle bakmak lazım. At gözlüğü takma kısmına geliyorum, at gözlüğü takarsınız bazen de kulaklarınız kapatmanız lazım, düz bakmanız lazım. Neden? Karşınızda bir tane adam var, satıştan bir personel. Adam suçlu, hata yapmış. Geniş bakarsanız adam sizin arkadaşınız, size çok destek olmuş. Dar bakarsanız atmanız gerekiyor ama adam şirketi zarara uğratmış. Orada artık yapmanız gerekeni yapacaksınız. At gözlüğüyle bakacaksınız. Arkadaş diye birşey yok. O yüzden orada ilgili bir yargıya ulaşacaksınız bunu bağımsız bir şekilde yapmanız lazım. Geniş tutup ben aynı gemideyim onunla falan diyemezsiniz orada. Demin dedim ya denetçi aslında onlar için bir iş ortağıdır bilmem ne, danışmanken böyle danışman fonksiyonundayken öneriyor standartlar, danışmanlık ve güvence ver diyor. Danışmanlık verirken böylesiniz açılıyorsunuz kalbinizi ama kalbinizi kapatmanız lazım. Karşınızda bir tane suçlu var. Gerçekten ama gerçekten orada şirketin menfaatlerini gözetmeniz lazım, yatırımcının, şirket sahiplerinin, iş ortaklarının, çalışanların menfaatleri. Ben sizi sevmesem de sizin orada haklarınızı koruyorum olmam lazım. Bu adamı çok seviyor olmama rağmen adamın yapmış olduğu o kadar yemek ısmarlamaları, yardımlar vs. bilmem ne hepsini unutuyor olmam lazım. At gözlüğü bu adama düz bakıyor olmam lazım, prosedür neyse onu uyguluyor olmam lazım, bu harekette cümlelerime son veriyorum.

Ek 10: J Katılımcısı Mülakatı

- Yaşınız: 31
- Eğitim seviyeniz: Yüksek Lisans (okuyor)
- Toplam iş tecrübeniz: 6 Yıl
- Kurumunuzda çalışma süreniz: 1 yıl 2 ay
- Kurumunuzun sektörü: Giyim, perakende
- Kurumunuzun çalışan sayısı: 4.086

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Beş kişilik bir ekibiz. 1 direktör, 1 uzman, 1 asistan, 2 de yöneticiyiz aslında. Ağırlıklı olarak planlı bir yapımız var ama şirketin takip ettiği etik hat da aynı zamanda soruşturma süreçleri de iç denetim biriminde. Onlar daha çok plansız ihbar, bildirim vs. gibi bir konu geldiğinde kaynağı oraya da ayırabiliyoruz. Planlı denetimler için yeterli bir kaynak, gelen farklı talepler kaynak ihtiyacını artırabiliyor.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

İç Denetim Direktörü ile fonksiyonel olarak Denetim Komitesi'ne, idari olarak CEO'ya bağlı çalışmaktadır. Yani şu anki yapıda idari olarak CEO'ya bağlıyız ama halka açık şirket olduğumuz için zaten Riskin Erken Saptanması Komitesi ve Denetim Komitesi zorunluluğu var halka açık şirketlerde. Bir de tabi halka açıklık oranı çok yüksek, %60'larda. Denetim Komitesi sorumluluğunda ilerliyor iç denetim biriminin faaliyetleri bizde. Dolayısıyla iç denetim komitesine ve zaten Yönetim Kurulu adına görevde aldığımız için Yönetim Kurulu'na da bağlı çalışıyoruz.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Risk odaklı süreç denetimleri, mağaza denetimleri ve etik denetimler. Süreç denetimlerimiz var, az önce saydığım ekibin bir kısmı aslında mağaza tarafı. Orada da bir kaynağımız var. Planlı denetim yapısı mağaza denetimleri yapılıyor. Bir de etik hat dediğim etik denetimler bizim kapsamımızda. Şu an yapı biraz yeni olduğu için üç yıllık bir denetim yapısı. Danışmanlık henüz gündeme gelmedi ama ufak ufak bir haftalık, iki haftalık danışmanlık çalışmalarımız oluyor. Benim danışmanlık alanım genelde büyük danışmanlıklar olur üst yönetimin dahil olduğu, büyük projelerin olduğu. Burada henüz böyle tecrübemiz olmadı ama burada bir haftalık, iki haftalık çalışmalara destek olduk danışmanlık kapsamında. Yani planlı ve etik denetimler haricinde böyle bir talep gelirse cevap veriyorum.

Kurumunuzda denetimin amaç, kapsam ve sorumlulukları belirlenerek risk odaklı denetim planı mı oluşturuluyor? Denetim planı oluşturulurken önceliklendirilen alanlar nelerdir?

Mevzuata ve standartlara uygun olarak oluşturulmuş bir iç denetim yönetmeliği var. Biz ona 'charter' diyoruz. Yönetim Komitesi'nden onay alınması gerekiyor. Onaylı 'charter'ımız var. Bu onaylı 'charter' oluşturulurken IIA Uluslararası İç Denetim Enstitüsü'nün belirlemiş olduğu standartlara göre bir 'charter' oluşturuyoruz ve zaten bu standartlarda ülkelerin yasaları ve mevzuatıyla uyumlu olması lazım. Dolayısıyla o mevzuata aykırı olması çok mümkün değil. Bir de bizim hukuk birimimiz var o 'charter' hukuk biriminin de gözleminden aynı zamanda geçiyor. Herhangi bir yorumu, hukuki yorumu var ise onlarda paylaşıyor. Gerekli revizyonlar yapıldıktan sonra aslında Denetim Komitesi onaylıyor sonunda. Soruda bahsedildiği üzere süreç denetimlerimiz risk odaklı planlanmaktadır. Kurumsal Risk Yönetim (ERM) çalışması sonrasında oluşan risk önceliklerine göre denetim evreni ve öncelikleri oluşur ve bu evrene göre denetim planı belirlenir ve Denetim Komitesi tarafından onaylanarak yürürlüğe konulur. İç denetimin aslında

bahsetmediğim bir fonksiyonu daha var. Risk yönetimini de biz yapıyoruz şirkette. Bir risk yönetim departmanı olmadığı için burada da risk yönetimini iç denetim departmanı üstlenmiş vaziyette. Bunun sebebi de denetim planımızı risk odaklı yapabilmek için aslında biz risk yönetiminden esasında temel sorumlu departman biz değiliz. Bu üst yönetimin CEO'ya bağlı bir risk yönetimi departmanı olmalı normal ideal uygulamada. İç denetimde bu risk yönetimi faaliyetlerinin doğru yürütülüp yürütülmediğini aslında kontrol eder, güvence verir normal yapılarda. Buradaki yapıda risk yönetimi henüz olmadığı için bizim de denetim planlarımızı risk odaklı yapmamız gerektiği için risk yönetimini biz yürütüyoruz. Orada zaten belli bir metodoloji var. ERM dediğimiz bir kurumsal risk yönetimi metodolojisi var, o COSO Küpü. O COSO Küpü'ne bağlı kalarak riskleri belirliyoruz en başında. Daha sonrasında tabi şirketin hedeflerine uygun bir şekilde olması lazım, bu risklerimizi ilgili 'sea level'larla paylaşıyoruz. Onlardan eklemeler, çıkartmalar alıyoruz. Bunları çıkartalım, bunları da ekleyelim. Bu riskler tabi belli bir kategoriye sahip operasyonel, finansal, itibar, yasal riskler gibi 4 tane stratejik ve operasyonel ana kategorilere sahip aslında. Bu kategorilere göre de biz belirli 'sea level' yöneticilerimize atıyoruz. Onlardan gelen geri dönüşe göre nihai bizim risk envanteri oluşuyor. Bu risk envanterini daha sonrasında değerlendiriyoruz. Ölçme ve değerlendirme aşamamız var. Buna puanlama diyoruz. Herkes kendi görüşüne göre x riskine puan veriyor. Etki-olasılık değeri nedir? 1'e 4, 3'e 2 gibi bir puan aralığı var 1-4. O ölçek aralığında bir puan vermelerini istiyoruz. Daha sonra bütün alanları iç denetim olarak konsolide ediyoruz. Bir manipülasyon müdahale etmeden onların ortalamalarına göre her riskin bir nihai skorunu oluşturuyoruz. O skora göre de günün sonunda sıralıyoruz. Yani risklerin önceliklendirilmesi sürecine geçiyoruz. En yüksek skoru alan risk bizim için en öncelikli risk olmuş oluyor. Bu riskleri sonra süreçlere bağlıyoruz. X riski hangi departman ile bağlı, Y riski hangi departmana bağlı? Daha sonra riskler bağlandıktan sonra da artık denetim evreleri oluşuyor. Denetim evrelerinde de ilk önce şu departman daha riskli görülmektedir. Denetim planının bu kadar kaynağını buraya ekleyelim. Tabi bunların hepsi

Denetim Komitesi ve üst yönetimle beraber yapılan süreçler. Özetle buradaki yapımız risk odaklı bir denetim planıyla ilerliyoruz.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

İdeal uygulamada yılda bir oluşturmaktır. Ancak mevcut planın pandemi gibi olağandışı durumlardan tamamlanamaması sebebiyle mevcut plan takip eden dönemlere sarkabilmektedir. Normal şartlarda yılda bir. Plan sıklığı yılda birdir. Dünya’da da yılda birdir, burada da. Biz zaten denetim planlarımızı üç beş yıllık çok yapmayız. Altı aylık yapsak da revizyondur aslında o plan değildir. Genelde bir yılda hangi konulara bakılacağı belirlenir ve yıl içinde üst yönetimin önceliği değişebiliyor bu konuyu da planımıza ekleyebilir misiniz, şu konuyu da dahil edebilir miyiz, dediği konularda aslında planda birkaç tane konu bir sonraki plana da sarkabiliyor. Pandemi gibi durumlarda fiziki denetim yapamadığımız için ziyaretlerimizi yurt içi ve yurt dışı ziyaretlerimizi yapamadığımız için tamamen ‘roumood’ denetim ile yapabildiğimizi yapıyoruz. Aslında burada da o fiziki denetim gerektiren konuları biraz ötelemiş oluyoruz. Onun haricinde yani ideal uygulama ve bizim de uyguladığımız mevcut yapıda biz yılda bir denetim planı yapıyoruz.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir?

Burada denetim süreci metoduna göre değişiyor. Yani burada esas yapı aslında süreci anlamak ve kavramak. Denetime başlamadan önce ana çerçeveyi anlamamız lazım en öncelikli konu bu aslında. Bunun içinde belli başlı bilgi kanalları var şirket içinde erişebileceğimiz. Bunlar bir süreç özelinde konuşursak, o sürecin nasıl işlediğini, nasıl faaliyetlerin yürütüldüğünü anlatan iş akış diyagramları, ‘work flow’ları. Yani prosedürler olabilir, burada bizim en çok faydalandığımız organizasyon şeması. Yapıyı bilmemiz lazım. Oradaki ‘live otority’yi iyi bilmemiz lazım. Geçmiş denetim raporları bence en iyi kaynaktır burada. Eğer bir denetim yapılmışsa buradaki bulgular veya süreçleri zaten bire bir özet yapıyla raporlara

koyduğumuz için orada en hap bilgiyi, en özel, en özet bilgiyi oradan elde ediyoruz. Bir daha Amerika'ya gitmene gerek kalmıyor bir raporu yazmak için. Bulguların aksiyon planları, aksiyon takip çalışmaları bunlarda çalışmanın ön hazırlık aşamasına dahil edilebiliyor. Bu gibi bilgiler arasında yani denetimin bizzat operasyonun denetim hakkında, süreç hakkında bize bilgi verebilecek ön bilgileri aslında temin ederek ön hazırlık aşamamızı yapıyoruz. Onun haricinde ön hazırlıkta bir 'to-do-list' olabilir, o denetçinin yapış tarzına göre değişir ama kendi yaklaşımından yola çıkarak bir denetimde neler yapacağını bir 'to-do-list' yapar. Bunun bir süre planlaması yapılarak 'to-do-list'ler, testler, görüşülecek kişiler, bu kişilerle ne zaman görüşeceğini detayına kadar programı belirlemek, hangi belgeleri önceden okumak lazım, işte yukarıda bahsettiğim akış diyagramları, prosedürler, geçmiş raporlar gibi bunlar aslında önceden bakmış olduğumuz kaynaklar denetime başlamadan önce ve netice olarak bu bilgiler ışığında da denetime ilişkin risk kontrol matrisleri aslında biz hazırlamamız lazım. Burada da yani RCM (Risk Control Management) yapısı her yerde yok. Yani ilk çalıştığımız kurumda biz tamamen 'free format' yapıyorduk. Bir sürece başlıyoruz, 'wolfrue' yapıyoruz. Yani oradaki süreci bir gözlemliyoruz, inceliyoruz prosedürel veya işte kişilerle görüşerek bütün yapıyı anladıktan sonra bir test yapılacak konuların listesi çıkıyor. Bu bir RCM'in matrisi üzerinden değil tamamen denetçinin süreci çarpan yolla düzülür mantığıyla gidelim, görelim, inceleyelim bütün neleri yapıyı analiz edelim, ondan sonra neleri test edeceğim, onlara karar verelim. Bu gibi yaklaşım zaten ama RCM dediğimiz şey gene şirketin bir kurumsal hafızasıdır, risk yani bu denetim hafızasıdır. Burada bir bakılacak konular önceden çıkarılmıştır. Geçmiş iş tecrübelerinden de bunu çıkartmış olabilirsin çünkü süreçler çok benzer oluyor. Sonunda da süreçlere başladığımız noktada buna yeni eklemeler o RCM'in içinde olmayan, sürecin içinde olmayan konular varsa çıkartmalar yaparak RCM'i nihai hale getiriyoruz. Günün sonunda o risk maddelerinin hepsini tek tek test etmemiz gerekiyor. RCM'in oluşturulması önemli bir süreç. Bir de tabi Denetim Direktörü'nün ve denetçinin fikir alışverişinde bulunuyor olması şu konulara da

bak, bu konularda önemli gibi çünkü bodoslama direk bir denetime gitmiyoruz. Önceden bir fikir alışverişi yapmamız gerekiyor ve o şirketi daha iyi tanıyan bir arkadaş var ise belki de onunla bir fikir alışverişi yapıp, geçmişte denetim yapmış olan bir denetçi var ise ondan da bilgi alışverişi yaparak ön hazırlığımızı tamamlamış oluyoruz. Bu akışta genellikle değişiklik olabiliyor her denetçi her denetimde farklı bir akış izleyebiliyor. Ben genel hatlarından yola çıkarak birkaç örnek vermeye çalıştım.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Bu çok öznel bir cevap olacaktır. Bunu ölçebilmek çoğu kurumda mümkün değildir. Ancak iç denetim olarak geçmiş bilgi ve birikimlerimizden edindiğimiz 'know-how' ile tüm risk alanlarını suistimal, yasal, operasyonel, finansal ve itibar vb. tespit edip üst yönetime sunarak aksiyonların alınmasına katkı sağlamaktayız. Yapmış olduğumuz denetimler ile bu risk alanları periyodik olarak test edilip mevcut risklere ilişkin güvence verilmektedir.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

İç Denetim departmanı olarak Kurumsal Risk Yönetim sürecini de takip ediyoruz. Bu noktada RCM kapsamındaki tüm adımlarda iç denetim de, üst yönetim de bulunmaktadır. Risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi, raporlaması ve aksiyonların monitör edilmesi. RCM süreci bizde demiştik, risk yönetimi sürecini biz yönetiyoruz. Burada risklerin belirlenmesi, analiz edilmesi, değerlendirilmesi ve raporlanmasına kadar süreç bizde ve bu riskleri raporladıktan sonra riskli 'level'lar ile ilgili fonksiyonların bulguya aksiyon almalarını bekliyoruz ve bu aksiyonların alınıp alınmadığı ile ilgili de Denetim Komitesi'ne üç ayrı raporlama yapıyoruz. Yani burada aksiyonun monitör edilmesini bekliyoruz aslında. Ne aksiyonlar alındı günün sonunda üst yönetime bilgi veriyoruz. Yani iç denetçi bulguların aksiyon yönetimiyle benzer bir görev var burada. Risk

yönetimindeki o risklere ilişkin aksiyon alınması, alınıp alınmadığını üst yönetime üç ayda bir raporluyoruz Denetim Komitesi dönemlerinde.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Çalışanlara uyum, etik ve risk yönetimi gibi periyodik eğitimler verilmektedir. Ben bir eğitim alıyorum şu anda. Bir eğitim verebilmem için benim de bir eğitici eğitim almam lazım şirkette. Burada da temel sebep risk yönetimini organize ediyoruz. Şu an şirket içinde önceden de yaptığımız gibi şimdi bunu biraz daha profesyonel bir yaklaşım yapalım dediler. Zaten etik ve uyum eğitimleri bunun haricinde İnsan Kaynaklarının vermiş olduğu farklı rüşvet, yolsuzluk ve şirketin oryantasyon programı kapsamında yeni başlayanlara vermiş olduğu şirketin yapısını, kurallarını anlatan bir oryantasyon var zaten. Buna ek olarak risk yönetimi de buna dahil olmuş oldu.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Süreç denetimleri, risk yönetimi, periyodik IT testleri, sızma, ‘fishing’ vb.. Bahsettiğim süreç denetimleri aslında en önemlisi risk yönetimiyle aslında bir nebze rahatlatmış oluyoruz. Şu an IT tarafında daha proaktif bir test yöntemi uygulanıyor. Haftada bir, ayda bir, yılda bir belli başlı testler yapılıyor. Sızma testi, ‘fishing’ testelerdir, işte sistem ‘database’ testidir, ‘hackleme’ testidir, bu tarz testler yapılıyor. Süreç denetimlerinde kendi departman özelinde biraz önce bahsettiğim ön hazırlık tamamlandığında bir RCM listemiz var. Risk kontrol matrisi. O risk kontrol matrisindeki bütün maddeleri atıyorum bir insan kaynakları denetimi yapacaksa eğer İnsan Kaynaklarındaki bütün işe alım, bordrolama, eğitim, izin süreçleri, prosedürler, işten çıkış, aklınıza gelebilecek bütün İK süreçleri ile ilgili bir RCM listemiz var. Risk kontrol matrisi oluşturuyoruz. O matrisin sonucunda maddelerin hepsini tikliyoruz. İşe alımda bunlar yapılmış mı,

yapılmamış mı, prosedürlere uygun hareket edilmiş mi, edilmemiş mi, bu belgesel sorunlara girilmiş mi, girilmemiş mi gibi bu tarz bütün konuları tek tek bakarak atıyorum 50 tane risk kontrol matrisi vardır, o 50 tane riski tespit etmemiz lazım. Tespit ettikten sonra da ilgili test eğer ilgili risk kontrol matrisi etkinse herhangi bir çalışma kağıdı yapmamıza gerek yok. Riskli değilse o kontrol onunla ilgili test dökümanlarımızı kendi şablonumuza göre muhafaza ediyor olmamız lazım burada. Çünkü güvence süreçlerimiz var, iç denetimin denetimi dediğimiz bir süreç var. Bu iç denetimin denetimi bizden bazı çerçeve istiyor. Bazı yapı standartlarına uyup uymadığını kontrol ediyor aslında. İç denetim standartlarına uygun çalışma kağıdı oluşturmuş muyuz, testlerimizi yapmış mıyız, örneklekimizi bu iç denetim standardına uygun belirlemiş miyiz veya örneklekimizi yeterli sayıda belirlemiş miyize kadar gelen kalite güvence süreci var. Biz finansal bir denetim yaparken bir milyonluk excel datasını inceliyorken, örneklem bin TL'lik bir örneklem çok yetersiz kalacaktır. O yüzden örneklemi çok iyi belirlemek gerekiyor çünkü sağlıklı bir güvence vermemiz lazım. Bir milyonluk datanın içinde biz yaklaşık %60'ına kadar tekabül eden bir datayı inceledik ve herhangi bir sorun olmadığını gözlemledik, buna yönelik güvencemizi veriyoruz diyebiliriz veya sorunları tespit ettik gibisinden bir şey söyleyebilmemiz için yeterli örneklemi aslında inceliyor olmamız lazım. Bunun sonucunda da testlerimizi tamamladıktan sonra risk kontrol matrisi tamamlandıktan sonra bunların bulgulaştırılması, mutabakat yazısı aslında yani bulgu bulgu olmayabiliyor. Her bulduğunuz test sonucundaki tespit bir bulgu olmayabiliyor. Bunun bir mutabakatını direkt yapan arkadaşlardan mutabakatını yapmamız gerekiyor. Bu mutabakat yapıldıktan sonra gerçekten bunun bir bulgu olduğuna kanaat getirildiği noktada artık bulguların taslak olarak üst yönetime sunulması akabinde Yönetim Kuruluna ve Denetim Komitesi'ne bunların sunumunun yapılması gibi bir süreç var. Aslında temel olarak bu şekilde.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Yapıcı ve çözüm odaklı. Yani şimdi orada da şirket kültürü çok önemli. Daha önceki şirketlerde herhangi bir sorunla karşılaşmadım. Yani bulgulara veya denetimin yapısına yaklaşımları genelde insana yapıcı ve çözüm odaklı yaklaşıyor. Çünkü orada şey çok önemli iç denetimin yaklaşımı. Nasıl bir tutum ile departmana yaklaştı, nasıl bir süreçle yaklaştı? İnsanların yaklaşımını etkiliyor ister istemez. Burada biz de aynı gemideyiz, biz de şirketin bir elamanı, çalışanıyız ve bu risklerin bertaraf edilmesi hepimizi ilgi alanında tutuyor olacak yaklaşımı genelde itibar gören bir yaklaşım. Ama polislik yaklaşımı ile eski tip elinde sopayla giden bir denetim onlar çok eskide kaldı. Bu şekilde gidilirse korkulabiliyor bilgi paylaşmama olabilir, itibar riski olabiliyor, sağlıklı bilgi alışverişi olmuyor o tarz yaklaşımda. Günün sonunda şu anki metodolojide böyle bir şey ile karşılaşmadım. Her zaman yapıcı ve çözüm odaklı yaptığımız tespitler çalışmalar yeterince saygıyı görüyor.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Plan doğrultusunda denetimlerin tamamlanması akabinde yayınlanmaktadır. Burada bir sıklık yok. Biz süreç denetimlerini tamamladığımız noktada üst yönetime raporlamamız gerekiyor veya mağaza denetimlerimizi tamamladığımız noktada raporun hazırlanıp süreç sahipleri ile üst yönetimle paylaşılması lazım. Ama Denetim Komitesi ile raporların sıklığı üç ayda bir, bütün raporlar Denetim Komitesi ile haricen paylaşılır. Bunları da biz her istediği zaman atmamız, üç ayda bir Denetim Komitesi zamanlarında raporlayalım gibi bir metodolojimiz var ama üst yönetim ile raporlarımızı yayımlandığı, tamamlandığı gün yayınlıyoruz.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Denetim Komitesi tarafından ve 5 yılda bir kalite güvence hizmeti ile. Az önce biraz değindim Denetim Komitesi'nin temel görevlerinden biri de aslında bizim performansımızı denetliyor olması. İç Denetim Direktörü kendi ekibinin performansına bakmaz ama İç Denetim Direktörü muhasebe ve finans departmanının performansına bakar. Denetim bağımsız olduğu için bağımsız denetim tarafından yapılır ve beş yılda bir uygulanır. Her yıl denetlenmez çünkü çok yüksek faturalar keser bağımsız denetim şirketleri ve bu yüzden beş yılda bir denetleniyor. Başka bir performans değerlendirmesi çok da sağlıklı olmaz. Şirketin bir İK departmanının denetlemesi olmaz çünkü biz onu denetliyoruz oda bizi denetliyor oluyor. O çok sağlıklı olmuyor genelde bunu denetimi bilen, iç denetimi bilen şirketler tarafından yapılması gerekiyor.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Alınan önemli sorumluluklar ile, katma değerli çıktılar ile, güven tesis edilerek. Burada katma değerli çıktı çok önemli. Ben altı yıldır bunu çok iyi gözlemledim açıkçası. Katma değerli bir çıktı üretiyorsanız günün sonunda hakikaten bunun müşterisi oluyor. Siz hiçbir şey yapmasanız bile sizden farklı çalışmalar yapmanız isteniyor. Danışmanlık yapmanız isteniyor, güvence hizmeti haricinde, bir klasik denetim süreçleri haricinde. Şöyle bir danışmanlık lazım, bu konuya da bakabilir misiniz, hatta yani ilk çalıştığım yerde şirket özelinde RCM çalışması yaptık. RCM bizim yapmamız gereken bir şey değil ama bizim departmanda bilgisi olan arkadaşlar vardı, RCM yapmak için çok ciddi bir veri analitiği bilgisi gerekiyor. Günün sonunda RCM'in ne olduğunu biliyoruz departman olarak, yani pazarlama departmanı denetimi yaptığımız için 'squeal' bilginiz olduğu için bunu siz yapar mısınız gibi bir teklif geldi bize. Yani böyle ara ara eğer katma değerli iş yaptığınızı gösterebilerseniz çıktılarıyla buradan süreklilikte olur, güven de tesis edilir. Bir de

alınan sorumluluklarında bu noktada da önemli olduğunu düşünüyorum sadece basit işlere bakabilecek sadece kendi denetim planınıza bağlı iş yaparsanız size gelen taleplerde o çerçevede olur. Daha proaktif, şirketin hakikaten bir dinamik bir departmanı ve süreçlere hakim bir departman olduğunuzu gösterirseniz ve bu noktada önemli sorumluluk alırsanız artık bunun sürekliliğini çünkü burada talepler artmaya başlıyor. Sadece denetim planı veya soruşturmalar değil daha farklı talepler de gelmeye başlıyor departmana. Şu konulara da bakın, bu konulara da bakın, bir noktada kaynak arttırmaya gidebilir aslında bir talep oluşabiliyor.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Aslında bütün konuşma boyunca söyledik. Şirketi güvenli alanda tutma, risk ve tehditleri bertaraf etme. İç denetimin belli başlı sorumlulukları vardır. Şirketin şeffaf, hesap verebilir, 'accountable' olması, şirket varlıklarının korunmasını sağlamak, yasalara uyulmasını sağlamak, rapor ve bilgilerin doğruluğunu teyit etmesi, halka açık şirketlerde bu daha önemli bir konu, şirket politika, prosedür ve kurallarına doğru ve tam uygulanması sağlamak, operasyonel verimliliği sağlamak, etkin iç kontrol sistemlerinin kurulmasını, işletilmesini ve gözlemlenmesini aynı zamanda sağlamak, hile ve suistimallerin tespiti, önlenmesi ve caydırıcı olması, ideal uygulamaları 'benchmark' gibi önerebilir. Bunlar önemli yani sadece bulguyu tespiti yaptım benim sorumluluğum bitti yaklaşımı çok itibar görmüyor. Aynı zamanda bir öneriyle gitmemiz lazım. Burada da 'benchmark' önemli geçmiş tecrübelerimizden öneriler önemli. Yani iç denetimin bence en 'overall' sorumluluğu 'governance' yönetiştir, 'corporate governance'dır. Şirketin kurumsal yönetim anlamında belli standartlara ve belli bir seviyeye ulaşmasına hizmet eder aslında iç denetim bunu sağlayıp sağlamadığını denetimleriyle de kontrol eder ve buna güvence verir diyebiliriz.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

İç denetim içerik olarak çok farklı görev tanımlarını ve operasyonları içerebilmektedir. Mağaza süreci olan bir kurumda iç denetçi stok sayımı, 'checklist' denetimi gibi denetimler yapabiliyorken, hiç saha ziyareti yapmadan yazılan bir senaryo ile de denetimler merkezi olarak da yapılabilmektedir. İç denetimin nasıl bir misyona sahip olacağı, hangi 'tool'ları kullanarak bu misyonu gerçekleştireceği konusu en temel ve önemli konu olmaktadır. Bu üst yönetimin bu misyon ile aynı çizgide olması ve destekliyor olması elzem bir konudur. Konvansiyonel denetim araçları artık rafa kaldırılma aşamasında ve robotlar her alana girdiği gibi iç denetim mesleği üzerinde de etkisi olmaya başladı. Bu bağlamda denetçilerin güncel trendleri takip ediyor olması önemli bir husus. Bahsettiğim gibi iç denetim çok farklı görev tanımlarını ve operasyonları içerebilir. Yani iç denetim deyince stok sayımcı arkadaşta iç denetçi olabiliyor veya işte senaryo denetimi yazan arkadaşta veya bilişim teknolojileri denetimi yapan arkadaşta iç denetçi olabiliyor. Orada bir ayırım maalesef yok. Yani iç denetçi, perakende denetçi, süreç iç denetçi, IT gibi yavaş yavaş ayrılmalar başladı ama herkes kendine iç denetçi diyebiliyor. Şirketin kaynağı ile yapılan bir iç denetim olduğu sürece iç denetçi oluyor aslında yani işte iç denetçi stok sayımı, 'checklist' denetimi gibi denetimler yapanlarda var, senaryo veya süreç denetimi olarak yapanlar da var. Yani işte iç denetimin nasıl bir misyona sahip olacağı hangi 'tool'ları kullanarak bu misyonu gerçekleştireceği konusu önemli. Bunu ben ilerleyen zamanlarda kendime de hep bir KPI koydum. Bir departman eğer benim sorumluluğuma verirse en önem vereceğim konulardan biri departmanın misyona sahip ve hangi 'tool'ları kullanarak bu misyonu gerçekleştirebileceği bence önemli. Yani onay aşamasında hangi personellerin, hangi yetkinlikte çalışanların istihdam edileceğinin belirlenmesi lazım. Bu üst yönetimin misyonu ile aynı çizgide olması lazım. Siz hayal dünyasında yaşıyor olabilirsiniz. Yani üst yönetimin de buna destek veriyor, kaynak ayırıyor olması lazım. Yani ben BT

denetimi yapıyorum iç kaynakla demeniz yeterli. BT denetçisine üst yönetimin onay veriyor olması lazım. Maliyetli bir çalışan arkadaş olduğu için, BT denetimleri biraz az bulunduğu için Türkiye’de o yüzden biraz her şirket yönetmek istemiyor. Yani aslında bahsettiğim gibi Türkiye’de de dünyada da artık denetimler evrilmeye başladı. Konvansiyonel eski yöntem denetim araçları artık fazla kullanılmaması, burada veri analitik ‘tool’ları kullanılmalı. Bence artık denetçinin kendini güvenli alanda tutması da önemli. Kendini garanti altına alması içinde bu ‘tool’ları öğrenmesi lazım bir parça. ‘Our studio’ programları kullanmayı bilmek gerekiyor. Artık yapay zeka denetimin içine de girmiş durumda. Bu trendleri bence çok yakın takip etmesi lazım iç denetçinin ve iç denetim departmanının aslında bu konuda bir farkındalığının olması lazım. Yani arkadaşlar yeni ne var, dünya ‘fraud’ işi artık nasıl yapılıyor, bu algının sürekli açık olması lazım. Çünkü bugün ‘higher studio’yu konuşuyoruz yarın başka birşey konuşuyor olacağız. Bu farkındalığın her zaman açık olması lazım. Yani trendlerin takip edilmesi açısından önemli bence yani benim söyleyebileceğim bunlar.

Ek 11: K Katılımcısı Mülakatı

- Yaşınız: 38
- Eğitim seviyeniz: Yüksek Lisans
- Toplam iş tecrübeniz: 14 yıl
- Kurumunuzda çalışma süreniz: 9 yıl
- Kurumunuzun sektörü: Havacılık
- Kurumunuzun çalışan sayısı: 15.000+

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Benimle beraber iç denetim ekibinde 4 kişi var, 2 kişi risk ve iç kontrol ekibinde var, bir başkanımız var, bir kişi de uyum fonksiyonunda var. Toplamda 8 kişi var. Eğer şirket yönünde değerlendirirsek sayı aslında bizim daha öncesinde denetim ekimiz daha büyüktü ancak bu yeniden yapılandırma pandemi vs. bu süreçte sayı azaldı. Bazı ekip üyelerini iş gereklilikleri gereği iç kontrol, risk uyum gibi fonksiyonlarda değerlendirmek zorunda kaldık. Kontrol tarafındaki iki kişi aslında önceden denetim tarafındaydı ve eskiden sadece iç denetim fonksiyonu olarak vardı. Şimdi bu iç kontrol risk yönetimi ve uyum fonksiyonu gelince biraz ekip dağıldı ama şuandeki denetçi sayısı yeterli değil şirketin büyüklüğünü göz önünde bulundurursak.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Fonksiyonel olarak CEO'ya bağlıyız ama halka açık şirket olduğumuz için Denetim Komitesi'ne bağlıyız fonksiyonel olarak organizasyonel yapıda CEO'ya bağlıyız.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleştiriyor?

Şimdi şöyle bir denetim kainatımız var ve bu denetim kainatı içerisinde şirketlerimizin hepsinin tek tek süreçleri çıkartılmış durumda ve bu çerçevede hangi süreçler var ise bunların denetimleri yapılıyor. Bunun içerisinde tabii neler var; insan kaynakları, iç kontrol, satın alma, uyum fonksiyonu ya da IT'sel bazı şirketin altyapı durumlarına göre ayrı ayrı denetimler, işletim sistemleri, veri tabanları, kurumsal iletişim ya da pazarlama fonksiyonu dediğim gibi hangi şirket hangi organizasyon yapısında hangi süreçler var ise ki bunların içerisinde havalimanlarına özel operasyonel süreçler, 'airdrom' ve teknik denetimler hepsi bu denetim kainatının bir paçası.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Denetim kainatının içerisinde risk değerlendirmesi var. Risk değerlendirmesine göre elimizdeki kaynak ve yıl içerisindeki mevcut çalışma gün sayısına göre bir plan yapılıyor planlamaya göre denetimler yapılıyor.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Dediğim gibi kendi oluşturduğumuz bir metodolojimiz var. Bu metodoloji içerisinde bahsetmiş olduğum tüm şirketler için ki aşağı yukarı ana şirketleri baz alalım, burada 15 tane şirket var. Ankara'daki havalimanı, İzmir, Gazipaşa, Bodrum, yurtdışındaki iştirakler Tunus, Sudi Arabistan gibi havalimanları ya da kendi servis şirketlerimiz var. Bu işte yiyecek içecek alanında faaliyet gösteren 'BTA' ya da işletme hizmetleri gibi 'lunch' operasyonları yürüten ya da 'duifree' yürüten şirketlerimiz var. Bunların her birisinin de kendi iş süreçleri var. Bu iş süreçlerinin risk değerlendirmesine göre bir puanlama metodolojisi var. Bu hukuksal, uyum, regülasyon vs. gibi belirli notlamalar kullanıyoruz. Bu notlamalar üzerinden bağlanan iç kontrol yapısını değerlendiriyoruz ki bu iç kontrol yapısını tabi aşağı yukarı denetim fonksiyonu 13-14 yıldır var. Daha ilk yapılırken ilgili süreç sahipleriyle görüşülüp iç kontrollerin ne durumda olduğu yönünde bir puanlama verilmiş ama biz denetim ekibimizle birlikte bulgular, denetim sonuçları var olan kontrol puanlamasını değiştirebiliyoruz. Bunun üzerinden belirli harmanlamalar yaparak risk değerlendirmesi ortaya çıkıyor. Çok fazla detaya girmeyim burada. Dediğim gibi onun ayrı bir algoritması vs. var ve yıl içerisinde böyle bir yapılacak bütün süreçlerin aslında aşağı yukarı binden fazla süreç oluyor bu kadar şirketin içerisinde. Puanlamaya göre risk değerlendirme notu çıkıyor. Bu risk değerlendirme de şunlar göz önünde bulunduruluyor. En son ne zaman denetime gidilmiş, bu denetimde denetim raporu notu ne olmuş, ne kadar bulgusu varmış, işte en son 3 yıl önce gidilmesi, en son 5 yıl önce gidilmiş olması vs. bunların her birinin ayrı ağırlıklandırmaları var ve bunun sonucunda da risk

değerlendirmesine göre bir önceliklendirme çıkıyor. Bu önceliklendirme de eğer çok uzun süre gitmediğimiz ya da gittiğimizde notu kötü olan bir rapor var ise ve bu şirketin iç kontrol yapısına verdiğimiz not düşükse değerlendirdiğimiz bu operasyonel, finansal ve repütasyon gibi kavramlardan gelen notlandırmalar etkiliyorsa bunlar en yukarıda olur ve ben hani elimdeki kaynağa göre o yıl içerisinde bu denetimleri aşağı yukarı ne kadar sürede tamamlayabilirim. Diyorum ki elimdeki kaynakla, bu kadar iş günüyle 12 tane denetim yapabileceğim. Bu 12 denetimi öncesinde seçiyorum. İzinleri vs. her şeyi düştükten sonra hala boşluk kalıyorsa 13. sıradakini alıyorum. Burada tabi şöyle değişkenlerde olabilir, diyelim ki ilk 12-13 denetim arasında yok. Denetim Komitesi'nin ya da CEO'nun ya da şirket içerisindeki yönetsel organların talep etmiş olduğu denetimler olursa bu sefer onun 'adjustment' olarak notunu arttırıp bir üst seviyeye taşıyıp mesela 13. sıradakini daha aşağıya çekerek ya da değer notunu arttırarak onu öne çekiyorum ve bu sayede plana almış oluyorum. Yani yönetimin burada vermiş olduğu görüşlerde dikkate alınmıyor.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Denetimin aslında risk dediğimiz kavram bir göreceli kavram. Henüz gerçekleşmemiş olan bir şeyden bahsediyoruz. Eğer risk gerçekleşmişse zaten artık buradan hasar ya da kayıp dediğimiz olay meydana gelmiş oluyor. Haliyle iç denetimin aslında bir suistimali ya da hasarı ne kadar önlediği konusu tamamen soyut bir kavram. Çünkü siz gidiyorsunuz bir denetim yapıyorsunuz ve buradaki iç kontrollerin ne kadar etkin olup olmadığını süreç içerisinde değerlendiriyorsunuz. Bunun sonucunda birçok bulgu yazıyorsunuz ve sonrasında da aksiyonların alınmasını takip ediyorsunuz. Haliyle buradaki aksiyonlar alındığı için ortaya bir hasar çıkmadığından denetim gerçekten işini yaptı mı yapmadı mı konusunu ölçümlemek çok mümkün değil.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Yani bizim amacımız direk risk yönetimi yapmıyoruz çünkü dediğim gibi bu organizasyonel yapı içerisinde bundan sonra bir iç kontrol ve risk yönetimi ekibi var. Denetim sadece denetime yoğunlaşacak. Bir de uyum fonksiyonu var. Hepsini birbirinden ayıştırdık. Risk yönetimi anlamında birincil noktada tabi bizim böyle bir şeyimiz yok ama denetimlerimizi bu risk değerlendirme metodolojisinden ve şirketin önceliklerine göre kendi risk değerlendirmemiz içerisinde bu ‘input’ları eklememiz gerekiyor ki doğru noktalarda denetimlerimizi yapabilelim. Örnek veriyorum şirketin bir risk değerlendirmesi var, risk değerlendirmesi sürecinde bu daha öncesinde siber güvenlik olabilir ya da iş sürekliliği olabilir vs. gibi kavramlar olabilir ama pandemi vs. gibi kavramlar risk yönetimi açısından üst sıralara geldi haliyle. Ben buradaki risk yönetiminden gelen bu veriyi kendi iç denetim süreçlerimde değerlendirmem lazım ki buna göre ben de denetimlerimde o risk değerlendirmesini yaparken, planlamamı yaparken göz önünde bulundurabileyim. Haliyle aslında risk yönetimi ekibiyle yakın çalışmam gerekiyor ki o ‘done’leri alıp kendi planımda göz önünde bulundurabileyim.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Risk yönetim departmanının böyle bir eğitim planlaması var mı bilmiyorum ama iç denetim ekibi olarak personelleri elimizden geldiğince bilinçlendirmeye çalışıyoruz.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

IIA standartlarında var olan gözlem, örnekleme metodolojisine göre test ya da ilgili kişilerle görüşme gibi bütün teknikler yani IIA’nın içerisinde belirtmiş olduğu bütün standartları takip etmeye çalışıyoruz.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Kişisel görüş olarak söylemeyeyim, söylersem zaten hoş bir şey değil. Birisi geliyor sizin yaptığımız işte sen bu işi yanlış yapıyorsun ve hani ya da bu işi ne kadar biliyorsun gibi reaksiyonlar olabiliyor. Çok fazla şirketimiz olduğu için çok olumlu yaklaşanlar da var, makul seviye de yaklaşanlar var ya da bu şekilde rezistans gösteren, bulguyu kabul etmeyen ya da itiraz odaklı yöneticilerimiz vs. olabiliyor. Ama bizim denetimin amacı sadece şey değil, yani ben bulguyu yazdım, bu bulguyu yazıp gidiyorum şeklinde bir yapımız yok. Bu yapı içerisinde IIA standartlarının gerektirdiği açılış toplantısını yapmak ilgili denetim planını önceden paylaşmak yapacağımız çalışmaları ve kanıtları toplamak ve bu kanıtları da ilgili kişilere sunmakla mükellefiz. Uluslararası standartlarda yapmamız gerekiyor. Daha sonrasında denetim çalışmasının sonunda kapanış toplantısı yapıp bu kapanış toplantısında da tüm bulgular üzerinde hem fikir kalıyoruz. Yani dediğim gibi çok istisnai durumlarda uyuşmadığımız konular olabiliyor. Bu bakış açısı olabilir ama biz elimizden geldiğince elimizde zaten kanıtlar toplayarak bu ilgili dökümanlar olabilir, yapmış olduğumuz test çalışmaları olabilir, gözlemler olabilir, saha çalışmasında bu kanıtları toplayarak karşı tarafla zaten paylaşıyoruz. Bu bulgulara da yaklaşımımız genelde şu oluyor, ya biz ikna olacağız burada bu işin kontrollü bir şekilde yapılması gerekli. Kontrol ortamının sağlandığı ya da burada bir kontrol olmadığı ve bir yanlışın olduğunu ya da bir risk noktasının olduğunu ve oluşabilecek riskin ne olabileceğini karşı tarafa anlatmamız ve onları ikna etmemiz gerekiyor. Bu biraz da hani denetçinin iş yönetim yaklaşımıyla alakalı. Bunun sonucunda genelde yaklaşım bugüne kadar dediğim gibi istisna bir ya da ikidir uzlaşamadığımız. Bulguları genelde kabul edilmiş olarak çıkıyoruz bu bir, iki istisnada da üst görüşü yazıyoruz ama bu çok çok nadir dediğim gibi 12 yıllık süreçte bir ya da iki tanedir.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Her denetim sonrası mutlaka raporlama yapılıyor bu da denetim standartlarının, X şirketinin diyelim ya da şimdi şöyle bizde denetimi yaparken şöyle bir yöntem kullanıyoruz, dediğim gibi 15 tane şirketimiz var. Bir süreç süreç yaptığımız denetimler var. Örnek vereyim holdingde bir satın alma pozisyonu var, holding satın alma sürecinin ayrıyeten denetimi yapılabilir ama bunun yanında bir de şube denetimi dediğimiz ya da şirket denetimi dediğimiz bir kavram var. Örnek veriyorum Ankara'ya gittiyseniz biz Ankara'daki bütün süreçlerin denetimini yapıyoruz. Yani Ankara'da bulunan insan kaynakları, bordro, satın alma, mali işler yani içerisinde muhasebe, bütçe, finansal raporlama ya da havalimanının operasyonları ve IT uygulamalarına özel bütün testlerimiz o şirket içerisinde yaptığımızda tamamını yapıyoruz. Holding seviyesinde ağırlıklı olarak süreç bazlı gidiyoruz çünkü merkezi birçok fonksiyon aslında. Örnek veriyorum, satın alma fonksiyonu merkezi o yüzden diğer şirketlerinde onay merci olduğu için onları süreç bazlı yapıyoruz. Haliyle her denetimden sonra bir süreç denetimi de olsa şirket denetimi de olsa normal standart iş yükü planlamasıyla elimdeki kaynak ve bu denetim ne kadar sürede bitti, örnek veriyorum Ankara'da bir denetim yapacağım, bu toplamda 450 adam saatinde tamamlayacaksan ona göre kaynak planlaması yapıyorum. İki ya da üç hafta içerisinde bu saha çalışmasının tamamlanması hedefleniyor. Bunun bir hafta öncesi planlama safhası. Bu dediğim iki ya da üç hafta saha çalışması. Sonrasında bulguların raporlanması, taslak raporunun hazırlanması ve yayınlanması gibi çalışması iki ila üç hafta süren bir çalışma var. Yani bir denetim ortalama 1-1,5 ay arasında tamamıyla bitmiş oluyor ve sonrasında raporlanması yapılmış oluyor mutlaka.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Tabii ki bizde sonuçta İnsan Kaynakları bünyesinde bir performans yönetim sistemi var. Bu performans yönetim sisteminin bir parçası da denetimciler. Altı ayda bir ara

değerlendirme, yıl sonunda da tam değerlendirmeden geçiliyor. Yıl başlarında zaten buna göre performans hedefleri belirleniyor kendi içimizde. Ayriyeten denetim standartlarını daha iyi taşıyabilmek için KPI'lar var. Bu performans değerlendirmesi bu KPI'lardan besleniyor. Halka açık bir şirket olduğumuz için zaten bağımsız denetimden de geçiyoruz, bağımsız denetimle yani zaten IIA standartlarında iş yapmaya çalışıyoruz. 5 yılda bir ortalama bağımsız denetim kalite güvencesinden geçiyoruz ve raporlarımızda zaten IIA standartlarına uygun olarak iş yaptığımızı buna göre belirliyoruz.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Şimdi denetim fonksiyonunun ülkemizde sürekliliği iki şekilde mümkün. Bir yasal mevzuatla, bu BDDK'nın kendi bankalar açısından düşünürsek, BDDK'nın kendi çıkarmış olduğu yönetmelikler gereği şirketlerde ya da bankalarda bir iç denetim fonksiyonunun olması zorunlu tutuluyor. SPK düzenlemelerinde ya da BDDK içerisinden gelen bazı kanun düzenlemeleri var. Bu biraz zorunlu olarak bazı şeyleri kurumsal yapı içerisinde yapılması gerekliliğini zorlayan bir yapı. Bunun haricinde bir de tabii şirketi kurumsallaştırmak isteyen bu yapılar içerisinde yasal olarak zorunluluk olmasa da profesyonel olarak yapanlar var. Biz çok şükür ki her iki tarafında izinden gidiyoruz. Kanuni olarak zaten burada bir iç denetim fonksiyonu olması gerekiyor. Ayriyeten bir de yönetimin buradaki farkındalığı çok önemli. Yani bugüne kadar CEO'nuzdan olsun diğer şirket yöneticilerimizden olsun çünkü bizim yapıda sadece holdingde denetim mekanizması var, bir iç denetim mekanizması var. Bu diğer tüm şirketleri de denetlemekle mükellef. Diğer şirketlerimizde bir denetim fonksiyonu yok. Yani merkezi olarak çalışmalarını yapıyoruz ve hani hem şirket yönetimi hem yönetim kurulu gerek mevzuattan kaynaklanan gerekse şirketin bu yapısal büyüklüğünden kaynaklanan konumda denetimin önemini farkında. Bir diğer noktada bizim zaten bir yabancı ortaklığımız var. Onlarda denetim fonksiyonunun ne kadar önemli olduğunun farkında ve aslında sürekliliğini bu şekilde sağlıyoruz.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

İç denetimin faydasını çok fazla ölçümlemek dediğim gibi risk gerçekleşmediği için çok ölçmek kolay değil ama hedefimiz zaten şu, yönetimin beklentisi ne, öncelikle bunu anlamaya çalışıyoruz ve yönetimin beklentisinin yanında uluslararası standartlar ve süreç içerisinde iç fonksiyon değerlendirmesi, iç denetim çalışması ve bu çalışmanın üst yönetime sunulması yönetimin zaten oluşan raporlar sonucunda bulgu ile ilgili bir reaksiyon görebiliyorsak zaten denetim başarılı olmuştur demektir. Biz biraz CEO'muzdan da görüşünü alıyoruz. Yeri geldiği zaman bu bulgularla ilgili direk kendisi sürece dahil olabiliyor. Bunun da zaten üç ayda bir Denetim Komitesi içerisinde raporlamalarımızı sunumlarımızı yapıyoruz. Halka açık şirket olduğumuz için onlar da takibini yapıyorlar ve risklerin önlenmesi konusunda ya da ortaya çıkması konusunda onlarda bu çalışmalardan memnunlar. Geliştirilmesi gereken alanlar olduğunda ya da farklı bir bakış açısı gerektiğinde bu süreci destekliyorlar.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok. Benim söyleyeceklerim bu kadar iç denetim ile ilgili birçok şeyin üzerinden geçtik.

Ek 12: L Katılımcısı Mülakatı

- Yaşınız: 35
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 11,5
- Kurumunuzda çalışma süreniz: 4,5 yıl
- Kurumunuzun sektörü: Otomotiv
- Kurumunuzun çalışan sayısı: 6.500

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

4 kişi çalışıyor. Şu an bizim kadromuz 4 kişi ama biz 3 kişi çalışıyoruz. Bazen 4 oluyoruz bazen 3 oluyoruz. İstanbul ofis ve Bursa ofisimiz var bizim. Bursa'da üretim var. Genel müdürlük İstanbul'da. Ben İstanbul'da ikamet ediyorum. İki tane denetçi Bursa'da çalışıyor. Normalde de İstanbul'da benim yanımda bir kişinin daha olması lazım ama o zaman birini alıyoruz. Sonra o terfi ediyor, başka bir yere geçiyor. Burasının denetimin 'turnover'ı yüksek. Yetiştirip gönderiyoruz. Aslında biraz böyle bir misyonumuzda var. Yeterli mi sorusu tabii ki yani 6.500 kişilik şirket büyüklüğünde bir organizasyon burası. Özellikle Bursa tarafı, endüstriyel taraf çok fazla fonksiyon var orada. Bazen yeterli gibi görünüyor ama bazen de daha fazla olsak dediğimiz dönemler oluyor ama bunu 4, 4 olmazsa en fazla 6 ya da 8 olması lazım. Yani yeteriz diyemem, bu şeye bağlı biraz yönetimin ne kadar büyük denetim ordusu istediğine bağlı olarak değişir. Şu anda biz şirketin denetim ihtiyacını karşılayabiliyoruz 'output'umuzla. Çıktılarımızda etkin. Yönetim Kurulu da bundan memnun. Daha fazla olsak bir yerde şey yaratırız gibi geliyor bana, atıl adamlar olmaya başlar bir süre sonra. Biz farklı bir model benimsiyoruz öyle söyleyim ben size. Biz dönem dönem bizim burada iç kontrol fonksiyonumuz da var aslında. Bütçe ve endüstriyel kontrol fonksiyonumuz var burada. Dönem dönem onlardan personel desteği alıyoruz. Yani personel desteği derken denetim projesi bazlı onların da ilgi alanlarına giren, sorumluluk alanlarına giren personeli biz denetimlerimize dahil ediyoruz. Dolayısıyla proje bazlı sayımızı arttırabiliyoruz. Tamamen biz yönetiyoruz, denetim yönetiyor, denetim planını biz yönetiyoruz akışı biz yönetiyoruz. 'Review' yapıyoruz, böyle etkinliği arttırmaya çalışıyoruz yani şirketteki personeli de optimum seviyede kullanmaya çalışıyoruz aslında. Tabi oradan da şey sağlamaya çalışıyoruz, birincisi denetimin etkinliğini arttırmaya çalışıyoruz, ikincisi uzun vade de denetime kaynak sağlayacak personeller yetiştirmeye çalışıyoruz o taraflarda. Böyle bir iş birliği yapıyoruz. Şimdi ben 4,5 yıldır buradayım, L Yönetim A.Ş. gibi bir şirketin bütün fonksiyonlarını

denetlemek, gözden geçirmek herhalde çok iyi tempoda 6-7 sene falan sürer. Biz %80 civarında şeyi kabul ettik, bu zamana kadar fonksiyonların denetimlerini kabul ettik. %80'ini kabul ettik diyebilirim. Fonksiyonu oturtuktan sonra zaten bütün fonksiyonları gözden geçirdikten sonra şimdi çok böyle fazla sayıda denetçinin de çok fazla anlamı yok. O yüzden hani ben çok uzattım sorunuzun cevabını da 4 kişi, 4 ya da 5 kişi bu ölçekte bir şirket için ideal. Bizim topluluk şirketlerinde de benzer sayılar var.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Burada şöyle şirketin Genel Müdür'ü, biz Genel Müdür'e bağlı olarak çalışıyoruz. Ben direk Genel Müdür'e raporluyorum ama Genel Müdür Yönetim Kurulu üyesi dolaylı olarak aslında Yönetim Kuruluna raporlamış oluyoruz. Onun sebebi de şu, İtalyan ortaklı olduğumuz için Yönetim Kurulu çok aktif çalışan bir Yönetim Kurulu değil. Yani %100 Türk şirketi kadar Yönetim Kurulumuz o kadar aktif değil. İtalyan ortaklar olduğu için periyodik toplanır. Dolayısıyla bizim oradaki kantağımız Genel Müdür oluyor. Genel Müdür de Yönetim Kuruluna bağlı, Yönetim Kurulu üyesi olduğu için dolaylı olarak Yönetim Kuruluna raporlama yapmış oluyoruz. İlk raporlama ama çeyrekler itibari ile toplanan Yönetim Kurulu toplantılarına ben de katılıyorum. Risk Komitesi adı altında orada da Yönetim Kurulunu denetim ve bulgular hakkında bilgilendiriyoruz. Aslında dolaylı olarak da Yönetim Kuruluna raporluyoruz. Direk Genel Müdür'e dolaylı olarak Yönetim Kuruluna bağlıyız.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Şirkette hangi iş yapılıyorsa, hangi süreç varsa şimdi bizim temelde üretim var. Bahsettiğim gibi üretimin yanında tedarik zinciri var, satın alma var, satış var, satış sonrası var ve yedek parça satış organizasyonumuz var. Bunların hepsiyle ilgili denetim yapıyoruz. Şey yok yani biz şuna bakmayız, şuraya bakmayız, şunlar

denetim kapsamı dışındadır diye bir ayırımımız yok. Şirkette ne yapıyorsa bizim kapsamımız içindedir.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Denetim planını yıl içerisinde denetime başlamadan önce yapıyoruz yani biz önce hangi operasyonları denetleyeceğimizi yılbaşında belirlemiş oluyoruz. Sonra önümüzdeki yıl için bir denetim planı oluşturuyoruz hafta hafta.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Şöyle yapıyoruz her sene Aralık ayında bir değerlendirme yapıyoruz. Bu zamana kadar hangi fonksiyonlarda denetim yaptık. Bir kere oradaki denetim bulgularımıza bakıyoruz. Aksiyon takip planlarımıza bakıyoruz. Yani aksiyonların ne kadarı tamamlanmış, ne kadarı tamamlanmamış, sürekli takip ediyoruz zaten standartlar çerçevesinde. Ve bu zamana kadar hangi fonksiyonları hiç denetlemedik onları gözden geçiriyoruz. Sonra önümüzdeki yıl için bir denetim planı oluşturuyoruz hafta hafta. Bu biraz daha kaba denetim planı oluyor yani şöyle kaba derken örnek veriyorum 2021'in Ocak ayında 2020'nin masraflarını denetleyeceğiz, masraflarını gözden geçireceğiz, işte yedek parça satış organizasyonunu gözden geçireceğiz, işte atıyorum satış sonrası operasyonları gözden geçireceğiz, üretim verimliliğini gözden geçireceğiz diye biz ana hatlarıyla bir denetim planı belirliyoruz. Detaylı denetim planını yıl içerisinde denetime başlamadan önce yapıyoruz yani biz önce hangi operasyonları denetleyeceğimizi yıl başında belirlemiş oluyoruz. Bunu da genel müdüre sunuyoruz önce, daha sonra Denetim Komitesi'ne sunuyoruz çünkü onlarda bazen şey diyebiliyor, ya bu denetimi yapmayın onun yerine şu denetimi yapın onların da kafalarındaki risk algısına göre denetlenecek yerleri belirleyebiliyoruz. Ama bütün denetim planımız hem Genel Müdür hem de Denetim Komitesi'nden geçer. Onların onay verdiği bir denetim planı üzerinden gideriz. En önemli hedefimizde zaten denetim planını tamamlamaktır. Örnek veriyorum 10 tane denetim planladıysak yıl sonunda kaç tanesini tamamladığımızın

hesabını veririz. Zaten bunu çeyrekler itibari ile de Yönetim Kuruluna sunuyoruz yani sürecin nerede olduğunu, aksiyon planının adetini sunuyoruz. Aksiyonların ne kadarının tamamlandığını onlarla paylaşıyoruz. Bir de bulgularımızı aksiyon planlarımızı düşük orta yüksek diye derecelendiriyoruz. Yüksek seviyelerdeki aksiyon planlarını ayrıca detaylı olarak paylaşıyoruz.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Bunu ölçmek çok kolay değil aslında bakarsanız zaten bizim en önemli fonksiyonumuz burada şirkette aktif bir denetim fonksiyonunun olduğunu şirkete göstermek. Yani işte o yüzden yılda 10 tane denetim planlıyoruz aslında. Buradaki yılda 10 tane denetim planlamasının en büyük amacı mümkün merteye bütün fonksiyonlara dokunabiliyor olmak, şu mesajı veriyor olmak, burada bir denetim fonksiyonu var, çalışıyor, aktif, periyodik olarak da yaptığımız işleri gözden geçiriyor, hatalarımızı tespit ediyor, kötü niyetli işlem varsa onlarla ilgili de aksiyon alıyor. Sadece burada subjektif bir yorum yapabilirim ne kadar önlediğini ölçmek çok kolay değil çünkü. 4,5 yıldır L Yönetim A.Ş.'de gerçekleşen çok katastrofik bir risk yok. Yani işte şurada çok acayip bir kaybımız olmuş, burada çok büyük suistimal olmuş, burada çok büyük risk almışız gibi gerçekleşen bir şey yok. O anlamda şey diyebilirim L Yönetim A.Ş.'de denetim riskleri önemli ölçüde engelleyebiliyor. Bunu bir de şuradan anlıyoruz şeylerden önce genelde fonksiyonlar yeni bir iş devralmadan önce bize soruyorlar. Biz böyle bir 'process' devreye almaya başlayacağız denetim anlamında, kontrol riski anlamında biz de bir 'default' var mı gözden geçirebilir misiniz diye genelde bize talep olur. Bu zorunlu değildir aslında ama sonuçta ajandalarında böyle bir şey olması şeyin göstergesidir, üst yönetimin ajandasında bu tarz şeylerin olması bunların göstergesidir. Demek ki biz şirketin üst yönetimine şey mesajını vermişiz bir 'default' varsa bu belki 3 yıl sonra bile ortaya çıkar. Dolayısıyla bir denetimin filtresinden geçse iyi olur mesajını

vermişiz. Bu sorunuza ancak bu şekilde cevap verebilirim. Yani riskleri ne derecede önlediğinin ölçümü hiçbir şirkette mümkün değildir zaten.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

Bahsettiğim aksiyon planları var ya aksiyon planlarının tamamlanması da benim en önemli hedeflerimden bir tanesi. Yani ben söyledim artık bundan sonrası sizdedir, yapacaksınız bunları değil, işte o önem derecesinden bahsettim ya düşük, orta, yüksek, yüksekler için çok kısa süre veriyoruz. Onlara bir tamamlanma tarihi ‘set’ ediyoruz. Tamamlanmalarını da takip ediyoruz. Eğer yüksek seviyede ve tamamlanmadıysa neden tamamlanmadığını sorguluyoruz. Eğer fonksiyonla tamamlanması konusunda el sıkışamıyorsak da bu sefer bunu üst yönetime bunu eskale ediyoruz üst yönetime ve Yönetim Kuruluna. Yani o riski tamamen fonksiyonlara bırakmıyoruz. Arkasında duruyoruz aslında biraz peşinden koşuyoruz. Eğer çok büyük yüksek risk gördüysek özellikle tamamlanmamış için ‘push’ ediyoruz yönetime. He şu olabilir ben bu riski alıyorum diyebilir Genel Müdür veya Yönetim Kurulu. Tamam ben böyle bir riski alıyorum, bunu ben yönetirim diyorsa o zaten bizim aksiyon takip tablomuzda risk yönetim tarafından alınmıştır diye geçiyor. Yarın bir gün bunun hesabını tabi ki ben vericem ama neticede bizim dökümanlarımızda o işaret edilmiş oluyor. Yarın bir gün dönüp baktığımızda bu riski yönetim almıştır, aksiyon alınmamıştır diye biz takip ediyoruz. Yani fonksiyona bırakmıyoruz aslında bakarsanız.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

İç denetimle ilgili eğitim vermiyoruz ama şöyle ilgili eğitim veriyoruz. Bizim bir etik kurallar politikamız var şirkette. O da bizim sorumluluğumuzda. Şirketin etik kurallarının yönetimi de iç denetimin sorumluluğunda. Uyum aslında ‘compliance’ adı altında etik tarafı tamamen bizde. Şöyle yapıyoruz şirkete giren her personelin bir oryantasyon süreci var. Yaklaşık bir haftalık bir eğitim sürecinden geçiyor. Saha

çalışanı da dahil hepsinin oryantasyon programında bir etik eğitimi var ve biz yıllık online etik eğitimi, zorunlu etik eğitimi var. Personelin o anlamda farkındalığını arttırmaya çalışıyoruz. Personel yönetmeliğindeki kurallar var zaten, işe girerken etik ilkeler ve kuralları okuyup imza atar personeller. Yani o anlamda bizim bir de şey var şirket içerisinde bizim iletişim platformumuz var. Orada da ayda bir etik kurallarla ilgili 'post'lar atıyoruz etik farkındalığı canlı tutmak için. Tabi bir de ihbar hattımız var. İhbar hattını da biz yönetiyoruz şirkette. Etik farkındalığı biraz yüksek seviyede tutmaya çalışıyoruz bu anlamda.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Hepsini yapıyoruz o denetim konusundan konusuna değişir ve fonksiyonun kullandığı 'tool'lara göre de değişiyor. Bir örnek üzerinden gidersek, örnek veriyorum satın alma denetimi yapıyorsak satın alma denetiminde inceleme yapıyoruz ama satın alınan malzemenin fiyatlarına bakıyorsak yeniden hesaplama yapıyoruz. O hesaplama metotlarına göre fonksiyonun belirlediği hesaplama metotlarına göre biz bir örneklem seçiyoruz, biz malzeme satın alıyoruz tabi ağırlıklı otomobili oluşturan her bir malzeme ayrı ayrı satın alınıyor. Her bir malzemenin seçtiğimiz her bir malzemenin fiyatlarını hangi periyodu inceliyorsak 2020-2019 o dönemin fiyatlarını baştan hesaplıyoruz. Eğer örnek veriyorum depo denetimi yapıyorsak, tedarik zinciri denetimi yapıyorsak bu sefer saha denetimi yapıyoruz. Yerinde inceleme yapıyoruz, gözlem aslında. Malın girişinden atölyeye üretim hattına gidişine kadar ki süreci gözden geçiriyoruz. Verimlilik alanları tespit etmeye çalışıyoruz. Bunları sistemdeki verilerle, datalarla, sahadaki dataları, sahadaki gözlemlerimizle örtüştürmeye çalışıyoruz. Yani bütün metotları kullanıyoruz aslında bakarsanız. L Yönetim A.Ş. ağırlıklı olarak bir üretim tesisi. Her ne kadar dışardan bir satış şirketi gibi gözüksede aslında işin büyük çoğunluğu üretim. Dolayısıyla bizim vaktimizin çoğunluğu sahada geçiyor yani masa başında çok oturmayız öyle söyleyim size.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

İç denetimin etki gücü yüksek. Yüksek olmasının sebebi biraz şey ben şimdi size şöyle söyleyeyim, birincisi biz Genel Müdür'e bağlı olarak çalışıyoruz, ona bağlı olarak şirketteki yaptırım gücümüz yüksek. İkincisi denetim işlemi şöyle bir işlemdir, denetimin yarısı teknik yetkinlik gerektirir, diğer yarısı da temsil gücü gerektirir. Yani işte bunu nasıl söyleyebiliriz, denetçinin de bir etki gücü olması lazım karakter olarak. Anlatabildim mi demek istediğim şeyi? Yani teknik yetkinliğinin de olması lazım. Onunla birlikte denetçinin de karakter olarak da bir etkinlik gücünün olması lazım. İletişiminin iyi olması lazım, fonksiyonlarla mesafesinin iyi olması lazım. Dediğini yaptırabilen bir yönetici vasfını taşıyor olması lazım. Ama bunu teknik yetkinlikleriyle birlikte taşıyor olması lazım. Yani şimdi çok despot ya da çok yaptırım gücü yüksek bir adam olursunuz ama teknik yetkinliğiniz olmaz. Bu sefer şey derler yani ejderha olsa ne yazar, adı mülayim derler. Bu ikisinin böyle güzel harmanlandığı bir ekip olursa denetim ekibi zaten genel müdüre bağlı olmuş olmasının vermiş olduğu etki gücüyle şirkette yaptırım gücü yüksektir. Yani tabi bunu kötüye kullanmaması lazım müfettişin. Orada da iletişim devreye giriyor. Biz bunu nasıl yönetiyoruz? Biz her denetimde soruşturmayı ayrı tutuyorum çünkü soruşturma bambaşka bir iş, yani soruşturma da uzlaşmana gerek yok. Soruşturmada, suistimalde bir kötü niyet vardır. Tespit varsa sorgusunu yaparsın, sorgusunu alırsın, iş akdini sonlandırır, feshedersin. O biraz daha üst perdedir ama normal denetim sürecinde biz şunu yaparız, örnek veriyorum bir tane denetim bulgusundan bahsedelim, ben önce denetim bulgusunu uzman seviyesinde, en düşük seviyede el sıkışırım. Bak senin burada böyle böyle aksiyonlar alman lazım. Bir kere uzmanla biz uzlaşırız, sonra bunu yöneticisine götürürüz bak burada böyle bir hata var, burada böyle böyle bir aksiyon almanız lazım. Yöneticisi de 'okay' der veya 'hayır ben böyle bir aksiyon almak istemiyorum' diyebilir. O zaman sen nasıl bir aksiyon alacaksın bu hatayı düzeltmek için diye yöneticisinden 'feedback' alırsın. Yani biz orada hep uzlaşa

uzlaşa şeye kadar gelir, Genel Müdür Yardımcısı'na kadar geliriz. Bir kere zaten bizim yazdığımız her aksiyon planı üst yönetimle uzlaştığımız aksiyon planıdır zaten. Oda böyle bir aksiyon almayı kabul etmiştir. Onlar aksiyon almayı kabul ettikten sonra ben genel müdüre raporlarım. He şu olabilir, bizim önerdiğimiz aksiyonu hiç almak istemeyebilir. Genel müdür yardımcısı da almak istemeyebilir. O zaman işte Yönetim Kuruluna veya Genel Müdür'e deriz ki, böyle bir riskimiz var, fonksiyonun üst yönetimi bu konuyla ilgili aksiyon almak istemiyor şu gerekçelerle, sen ne diyorsun? Biz Genel Müdür'ün o etki gücünü kullanmıyoruz aslında. Biz ne zaman ki fonksiyonla uzlaşamıyoruz o zaman Genel Müdür'ün yetkisini kullanmaya başlarız. Dolayısıyla sizin sorunuzun cevabı bizim yaptırım gücümüz o iletişimden geliyor. Anlatabildim mi? Şöyle bir şey olsa, bilmiyorum başka fonksiyonlar daha başka çalışıyor olabilir ama bu standartta böyledir zaten. Biz bunda da standarda uygun uygulama yapıyoruz. He şu olabilir, biz tespit yaparız direk Genel Müdür Yardımcısı'na göndeririz mesela adam daha konunun ne olduğunu bilmeden, ekibiyle herhangi bir iletişim kurmadan, üst yönetimden yukarıdan aşağı böyle bir şey indirirseniz vahiy gibi bu sefer denetçi dirençle karşılaşabilir. Kötü iletişim sonucu olarak yaptırım gücünü de zaman zaman kaybedebilir. Biz yaptırım gücünü uzlaşmadan alıyoruz, işte orada biraz fonksiyonlarla iş birliğinden alıyoruz. Anlatabildim mi? Zaten biz doğruyu bulmaya çalışıyoruz. Doğru da bir tanedir. Benim doğrum, senin doğrun yoktur. Yani ortada bir tane doğru vardır. Beraber bir doğru bulmaya çalışıyoruz. Uzlaştığımız zaman zaten yaptırım gücü de kendisi geliyor zaten iletişimin doğal sonucu olarak. Biz bu zamana kadar burada hep böyle yönettik. Bu bize ne sağladı? İşte o bahsettiğim şeyi de bu sağlıyor. Güçlü iletişim olduğu zaman bize de talepler gelmeye başlıyor. Biz böyle bir 'process' yapacağız siz de bir gözden geçirebilir misiniz? Çünkü tecrübe olarak hep şey var biz denetimle beraber yaptığımız çalışmalarda hep fayda sağladık, fonksiyon olarak da fayda sağladık, şirket olarak da fayda sağladık. Biz daha sonradan böyle şeylerle karşılaşmak yerine önden

önlem alalım diye bize danışmanlık talebinde bulunuyorlar. Yaptırım gücümüz özet olarak aslında uzlaşma iletişim yönteminden geliyor.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Genel Müdür'e ayda bir raporlar hariç bu arada raporları yayınladıkça Genel Müdür'e gönderiyoruz. Yönetim Kuruluna çeyrekler itibari ile üç ayda bir.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Tabi Genel Müdür bizim de performansımızı denetliyor. Her sene başında hedef alıyoruz. Yıl sonunda hesap veriyoruz. İşte bahsettiğim plana ne kadar uymuşuz? Kaç tane aksiyon planı yazmışsınız? Ne kadarını tamamlayabildiniz? Şeyde yapıyoruz, ne kadar verimlilik, ne kadar tasarruf sağlamışsınız? Hata bulup ne kadar iade fatura kesmiş tedarikçilere? Ne kadarlık finansal kazanç getirmiş, değer yaratmışsınız? Ya da ne kadar fırsat bulup finansal kazanç, değer yaratmışsınız? O tarz hedeflerimiz var. Yılda kaç tane şikayet gelmiş mesela yılda kaç tane şikayet gelmiş bunun aslında şeyidir, şirketteki etik farkındalık ne seviyede? Eğer hiç şikayet gelmiyorsa bu şey anlamına gelmez, yani şirkette her şey pürpak gidiyor, hiç bir sorun yok anlamına gelmez. Hiç şikayet gelmiyorsa bir problem vardır. İnsanlar etik ilkelerin farkında değildir. 6.500 kişilik yerde hiç problem olmaması mümkün değil. Bize ne kadar çok şikayet geliyorsa bu şey anlamına gelir, yani biz ne kadar iyi farkındalık yaratmışsınız anlamına gelir. Bizim böyle 6-7 tane KPI'mız var. Temelde onlar üzerinden Genel Müdür bizi değerlendiriyor. Aslında dolaylı olarak da Yönetim Kurulu değerlendirmiş oluyor. Bizim performansımızı onlar değerlendirmiş oluyor.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Yıllık gerçekleştirilen iç denetim planına örnek veriyorum 10 denetim planlandıysa doğru kaynak aktarımı ile optimum dengenin sağlanması sayesinde iç denetimin sürekliliği sağlamaya çalışıyoruz.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Bu zor bir soru yani şimdi bana sorarsanız tabii ki şey çok faydalı bir fonksiyon bir kurum için. Çünkü bir organizasyonu denetçisiz bırakırsanız bir süre sonra tahribatlar, erozyonlar olmaya başlar. Yani biz şu an burada az önce de söylediğim gibi katastrofik çok büyük anlamda şeyle karşılaşmıyoruz. Bu zamana kadar karşılaşmadık. He ufak tefek mutlaka şey olmuştur ama hata tespitleri. Zaten bizim işimiz bu ama bu bahsettiğim atıyorum ben yılda 2 milyonluk değer yaratıyorum şirket için. Şirket yılda 2 milyar kar eden bir şirket, üç aşağı beş yukarı yani 2 milyar içerisinde 2 milyon çok şey değil aslında bakarsanız, çok böyle materyal bir tutar değil. Dolayısıyla ben şey diyebilirim yani en azından bu şirket özelinde iç denetim fonksiyonu o kontrol algısını, denetim algısını çok iyi oluşturmuş. Bir fonksiyon atıyorum şöyle örnek vereyim bugün denetim grubunu kapatsak şirkette belki iki sene yine aynı şekilde devam eder. Hiçbir problem olmaz şirkette ama üçüncü yıl ve dördüncü yıldan itibaren erozyonlar başlar. Çünkü şey olacaktır, bir rahatlama olacaktır fonksiyonlarda, özellikle riskli fonksiyonlarda. O denetim fonksiyonunun sadece bu şirket için değil bütün şirketler için belli ölçeğin üzerinde şirketler için kesinlikle olması gerektiğini düşünüyorum.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok.

Ek 13: M Katılımcısı Mülakatı

- Yaşınız: 29
- Eğitim seviyeniz: Lisans
- Toplam iş tecrübeniz: 8 yıl
- Kurumunuzda çalışma süreniz: 3 yıl
- Kurumunuzun sektörü: Telekomünikasyon

- Kurumunuzun çalışan sayısı: 5.000+

Kurumunuzda iç denetim faaliyetini yürüten iç denetçi sayısı nedir? Bu sayıyı yeterli buluyor musunuz?

Biz global bir şirket olduğumuz için aslında 80 ila belki 100 arası 100 olduğunu düşünmüyorum, bir ara öyleydi ama bir 80 kişi olabilir. 30'dan fazla ülkeye hizmet veriyoruz o yüzden biraz kalabalık değiliz aslında normal. Global bir şirkete göre normal bir kadro bence ama tahminim olan rakamlar bu şekilde. Yurt dışına bağlı bizim şirketimizde şöyle biz bir havuz gibi düşünün, buradaki Türkiye'deki bir kişide örnek veriyorum Almanya ülkesinde Türkiye'ye çalışabilir. Sadece Türkiye'de genel olarak bulunan ve sorumluluğunun her ülkede aslında sorumluluğunun çoğu ilgili bulunduğu markette olan kişiler var. Ama bizde herkes mutlaka kendi ülkesi dışında bir ülkede bir çeyrek mutlaka çalışır. Evet sayıyı yeterli buluyorum. Bizim için yeterli. Normalde bizim son iki ayda iki arkadaş 'Senior Manager'ımız ve ekip arkadaşımız ayrıldı. Ondan sonra daha önce de bir arkadaşımız ayrılmıştı. Şu an iki kişiyiz, işte ben 'Audit Manager' oldum. Bir de 'Audit Executive' var. Dolayısıyla şu an iki kişiyiz ama bunu çok dikkate almamak lazım. Toplam kadromuz bizim beş kişi falan ama yani mesela biz şöyle çalışıyoruz, şu an mesela Türkiye'de beş kişiyiz ama bizim örnek veriyorum, üç tane 'audit' yapıyoruz, birini ben yapıyorum, birini ekip arkadaşım yapıyor, bir tanesini Hindistan'daki ekip arkadaşım yapıyor. Biz hep böyle dolayısıyla havuz gibi düşünürseniz aslında hani lokal markete tek bir kişide kalsa hiç fark etmez yani yarın hiç kimsede kalmayacak diyebilirler. Dolayısıyla yapılacak işler belli ondan sonra o ülkede yerleşik biri var ya da yok, yoksa diğer ülkedeki biri yapıyor.

Kurumunuzda iç denetim birimi kime bağlı olarak çalışıyor?

Yönetim Kuruluna, Denetim Komitesi'ne bağlıyız.

Kurumunuzda iç denetim faaliyeti kapsamında hangi denetimler gerçekleşiyor?

Her şeyi yapabiliyorsunuz, ‘payroll’ da yapabiliyorsunuz, envanterde yapabiliyorsunuz, ‘data privacy’ da yapıyorsunuz, hazine denetimi de yapıyorsunuz. Biz de sadece öyle bir konuda denetim yapmak gibi bir şey yok aslında. IT denetimi de yapıyorsunuz. IT ve ‘business’ ayrımı da bizde yok.

Kurumunuzda iç denetim planı hangi sıklıkta oluşturuluyor?

Her şirketin bir risk envanteri oluyor. Bir risk ekibi oluyor. Risk envanteri ile birlikte bütün Genel Müdür Yardımcıları ve Genel Müdür’le de görüşerek zaten risk bazlı olarak her sene denetim planı yapıyoruz. Riskler sürekli ‘update’ olduğu için sene içinde yaptığımız planı aynı şekilde bırakmıyoruz. İşin açıkçası çeyreklik plan gibi düşünebilirsiniz.

Kurumunuzda iç denetim faaliyetine başlamadan önce hazırlık aşamasında izlenen adımlar nelerdir? Önceliklendirilen alanlar nelerdir?

Şimdi şöyle bildiğiniz gibi her şirketin bir risk envanteri oluyor. Bir risk ekibi oluyor. Bununla ilgili sene boyunca çalışan çeyrek ‘review’ler yapan, global bir şirket olduğumuz için de hem şirketin stratejisi var, hem lokal market stratejisi var, hem de ‘top-ten’ risklerimiz var. Ayrıca tabii ki ‘update’ olacak güncel risklerde zaten bu ‘top-ten’ risklerin içinde de dahil olduğu için aslında şirket ‘top-ten’ risk dediğimiz aslında her şey var zaten strateji, regülasyon riski, finansal risk. Şirket yeni bir girişim yapacaksa vs. ve globalden de gelen stratejiyle ‘risk assesmentlar’ı ve şirketin ‘high risk policy’leri ve ‘top-ten’ risk envanteri ile birlikte bütün Genel Müdür Yardımcıları ve Genel Müdür ile de görüşerek ek olarak buna artı yani bu ‘fact’ diye somut şeyleri deyim artı olarak onlarla da görüşerek zaten risk bazlı olarak her sene denetim planı yapıyoruz. İşin açıkçası çeyreklik plan gibi düşünebilirsiniz çünkü sürekli riskler ‘update’ olduğu için sene içinde yaptığımız planı aynı şekilde bırakmıyoruz. Mutlaka her çeyrek ‘review’ ediyoruz ve o ‘top-

ten' risklerdeki bir risk çok önemliye geçmiş olabilir, diğerleri sıra değiştirmiş olabilir ya da sene başında asla olmayan bir şey 'urgent' bir şey olmuş olabilir. Bakmamız gereken yerler ya da yeni regülasyon gelmiş olabilir. Ona göre hiçbir şekilde sene başında bu onaylandı artık bundan şaşamayız diye asla bir şey yok. Çeyreklik olarak yeni güncellenen risk yapısına göre güncellemelerimizi yapıyoruz. Bizim kurumumuzda hemen hemen her sürecin 'process' risk dökümanı oluşturulmuş durumdadır. Çünkü bizim kurumumuzda şöyle bir şey var. Bir lokal marketteki 'auditor'lar var, bir grup globaldeki 'auditor'lar var ki bu 'auditorlar' her ülkeye çalışırlar lokal market ya da gruptaki fark etmez, bir 'quality assurance' ekibimiz var, bir de 'governance' ekibimiz var. Her ekipten kontaklarla bizim bütün sürekli gelişim planları yapılır bizde ve sürekli 'virtual team'leri oluşturulur. Dolayısıyla bizim zaten sürekli bir 'continious' olarak 'improve' sürecimiz olduğu için bütün süreçlerin 'process risk' dökümanları hazırlanmış durumdadır. Hemen hemen hepsinin bunlarda düzenli olarak kurulan 'virtual team'lerle 'review' edilir ve 'update' edilir 'end to end' bütün şirkette olması gereken kabaca süreçlerin işte 'process' risk kontrol, 'control activity' hatta bazıları için test senaryolarına kadar hazırlıyoruz. Ve işte bunun için zaten düzenli çalışan bir ekibimiz var. Artı bir de 'virtual' ekibine destek olan ekibimiz var. Bizim denetimlerimizin planlama aşamasında bu arada biz denetimlerimizi örnek veriyorum 7-8 ülkede aynı anda aynı 'scop'la yaparız. Çok az sadece birim markete özel 'single audit' yapıyoruz. Ee dolayısıyla denetimlerimizi zaten planlama aşamasında, planlama aşaması aslında denetimin planlama aşamasından bir ay önce başlar. Çünkü bütün marketlerin bir araya gelmesi data analitiği yapıyoruz. Çok fazla o senaryoların belirlenmesi herkesin datalarını talep etmesi, marketlerin buna hazırlanması vs. iki haftalık bir 'official planning' planlama sürecimiz var. Ama bu data analitiği öncesi dediğim süreç 'annous'la beraber vs. kendi içimizdeki koordinasyon süreci aslında denetim planında yaklaşık bir ay önce başlar. Official olarak iki hafta planlama, dört hafta 'field work' iki ya da üç hafta 'reporting' olmak üzere denetimin 'scop'una göre bir de kompleks bir 'audit' mi yoksa 'basic' bir 'audit' mi çünkü

bazı ‘audit’ler çok ‘basic’ bazıları çok kompleks oluyor. Ona göre bu kriteri korumak hedefiyle her zaman için bazısı işte iki hafta değil de üç hafta raporlaması olan ya da fiziksel olarak dört hafta değil de, dört hafta olan ‘case’ler tabiki var yani ama genel olarak bir standart var ‘time-line’da ve onu bozmadan ilerlemeye çalışıyoruz. Ama her ‘audit’ kendi ‘start-date’inde başlar ve 31 Mart’ta bizim mali yılımız yıl sonu diyelim yıl sonunda da hepsi biter. Hani bir sonraki mali yıla devam etme durumu söz konusu değildir.

Kurumunuzdaki iç denetim faaliyetleri iç kontrollerin etkinliği ve verimliliği sağlamak amacıyla meydana gelebilecek riskleri ne derece önüyor?

Bu soruya cevap verilmemiştir.

Kurumunuzun ve iç denetçilerin riske kaşı ve riskin yönetilmesi sürecinde üstlendikleri görev ve sorumluluklar nelerdir?

İş sahiplerinde kesinlikle. Tabii ki denetimin bağımsızlık ilkesi gereği tespit edilen risklerle ilgili bu riskler için aksiyon almakla ilgili bütün sorumluluk iş sahiplerindedir. İlgili kimse ilgili departman ya da ilgili fonksiyon o kişiler tarafından tespitlere dair aksiyon planları oluşturulur ve onlar tarafından aksiyon alınır biz sadece takibini yapıyoruz.

Kurumunuzda iç denetim ve risk yönetimi konularında personellere eğitim veriliyor mu?

Evet, bizim şirketimizde her şeyin eğitimi vardır. Riskle ilgili, denetimle ilgili, ‘data privacy’ ile ilgili, iş sürekliliği ile ilgili her şeyin. Çünkü bizde global şirket olmanın şöyle bir şeyi var ‘high risk policy’ler var mesela işte iş sürekliliği ‘economic senctions’ ondan sonra işte ‘fraud investigaiton’ ondan sonra ‘data post provention’ ‘data privacy’ vs. bu ‘high risk policy’e konu olan şeylerle konularla ilgili iç denetim ‘risk management’ mutlaka ama mutlaka her sene en az bir kere düzenlenen hata böyle daha ‘high’ riskli konularda altı ayda bir tekrar eden eğitimler oluşturulur.

Kurumunuzda iç kontrollerin etkinliğini ve verimliliğini sağlamak amacıyla uygulanan test yöntemleri nelerdir?

Şimdi data analitik uyguluyoruz, fonksiyonel test uyguluyoruz, performans test uyguluyoruz, 'observation test' uyguluyoruz, 'sample testing' uyguluyoruz. Tabi ki 'sample'dan daha çok data analitik, 'full popülasyon testing' yapmaya çalışıyoruz ama bütün metotları uyguluyoruz hepsini, tamamen sürecin yapısına göre ama data analitik fiiks, hepsinde full popülasyon için yapmaya çalışıyoruz.

Kurumunuzda iç denetçilerin denetim faaliyeti sonunda edilen bulgulara yaklaşımı nedir/nasıldır?

Riskleri tespit ettikten sonra bunları 'finding' dedikleri bulgulara dönüştürüyoruz. Raporumuzu yazıyoruz. Raporumuzdaki bulguları 'steakholder'larımızla beraber konuşuyoruz. Konuştuktan sonra zaten riskleri onlara da açıklıyoruz tespitlerimizle beraber ve orada 'recomandaiton'larımız oluyor. Tabi ki bu riski tespit edecek ya da bu riski engelleyecek ya da bu riski kontrol altında tutabilecek bizim önerimizce şöyle şöyle şeyler yapabilirsiniz diyoruz ama tabi ki aksiyon sahipleri bizim önerilerimizi dikkate alarak o riski nasıl ortadan kaldırmak isteyebilir, kontrol altında tutmak isteyebilir ya da tespit etmek isteyebilir onunla ilgili aksiyon planlarını bizlere veriyorlar ve o aksiyon planları belirlendikten sonra zaten raporlarımıza da aksiyon planlarını ekleyerek raporumuzu yayınlıyoruz ve o aksiyonları da biz düzenli olarak her ay yani aslında bir aydan da fazla oluyor bu biraz 'continious factoringe' giriyor. Çünkü zaten biliyor oluyorsunuz ama her ay en az düzenli olarak ayda bir kez takip etmek zorundayız mutlaka 'last' aksiyon planı (çok aklım İngilizceye gidiyor ya sorun olur mu bilmiyorum ama) o yüzden tabi ki 'audit management' sistemimiz var bizim de kullandığımız orada kayıt altına almak durumundayız. Aksiyon takibinde bazı kurallarımız var. 'High' aksiyon yüksek riskli bir bulguysa bunun aksiyonu yüksek riskli oluyor ve bunun üç ay içerisinde çözülmesini istiyoruz ya da en azından daha uzun vadeli bir şeyse üç ay içerisinde en azından bir 'minigating action'ların alınmasını istiyoruz riskin daha

az seviyeye indirilmesi için. Bu şekilde aslında kurallarımız var diyebilirim genel anlamda.

Kurumunuzda iç denetim raporu hangi sıklıkla raporlanıyor?

Her denetimin bitmesinin ardından her denetimin raporu yayınlanır. Şöyle diyelim her çeyrekte bir denetim raporu çıkar.

Kurumunuzda iç denetim biriminin performansı denetleniyor mu? Denetleniyorsa nasıl?

Evet işte 'quality assurance' ekibimiz var dediğim onlar zaten seçiyorlar 'audit'leri ve bizim zaten çok büyük IBR metodolojimiz var nerdeyse bir ansiklopedi gibi detaylı ve bütün tek tek 'end chand' kuralları belli olan oraya uyumluluğumuz kontrol ediliyor. Bir de her beş senede bir dışarıdan bağımsız bir firmadan zaten 'quality review'de alıyoruz ayrıca.

Kurumunuzda iç denetim faaliyetlerinin sürekliliği nasıl sağlanıyor?

Şöyle bizim denetim sayıları zaten her bir marketin kendi büyüklüğüne göre belirleniyor. Mesela Türkiye'de 10-11 denetim varken, Almanya'da 15-16 denetim oluyor. Dolayısıyla zaten o hem planlanması hem o sayıların belirlenmesi tamamen şirketin sahip olduğu diğer şirketlerin ve yani ne kadar 'SOX Audit' gibi düşünebilirsiniz oradaki materyality mantığı hani atıyorum 27 farklı şirketiniz var ama her biri aynı boyutta değil. Dolayısıyla onlara her birinin boyutuna göre yerleriyle 'compaire' ettiğiniz şekilde orantılı şekilde dağıtılıyor. Dolayısıyla yeterli buluyorum bir marketin denetlenme sayısı senede minimumu 6-7'dir. Daha azı yoktur diye düşünüyorum.

Kurumunuzda yürütülen iç denetim faaliyetinin faydası sizce nedir?

Şöyle risklerin aslında bağımsız bir parti tarafından tespit edilmesi ve risk analizlerinin aslında iş süreçlerini geliştirmek için doğru noktaya konulmasıyla doğru 'audit' planlamasıyla beraber aslında şirketin ihtiyacı olan aynı zamanda iş

sürekliğini de 'improve' etmek için riskleri tespit edebilmek için ilgili alanların tespit edilmesi ve onlarla ilgili aksiyon aldırılması üst yönetimin 'evayer' olmasının sağlanması ilgili konuların onlar tarafından takip edilebilmesinin sağlanması daha sonra tabii ki şirketin bir çok alanından haberdar olarak 'advisory' yapma şansında olması ve zaten hani kaliteli iş çıkardıkça iş sahiplerinin de senden denetimin yanı sıra aslında bu yeni bir işe girdiğin zaman 'advisory' istiyor olması tavsiye istiyor olması ve dolayısıyla aslında bakarsanız daha belkide risk gerçekleşmeden müdahale edebileceğin tarafa doğru teşvik etmeye aslında ona doğru vesile olmaya neden olması diye açıklayabilirim belki.

Bunlara ek olarak eklemek istedikleriniz var mı? Varsa nelerdir?

Yok, benim analatacaklarım aslında bu kadar.

Ek 14. İç Denetim Standartları

Nitelik Standartları

Uluslararası İç Denetçiler Enstitüsü tarafından Uluslararası İç Denetim Standartları aşağıdaki gibi açıklanmıştır. (TİDE, IIA Uluslararası İç Denetim Standartları, 2017, s.4-23)

1000–Amaç, Yetki ve Sorumluluklar: İç denetimin amaç, yetki ve sorumlulukları iç denetimin tanımı, etik kurallar, standartlar ve temel prensipler ile uyumlu iç denetim yönetmeliğinde açıkça belirtilmelidir ve İç Denetim Yöneticisi periyodik olarak yönetmeliği gözden geçirmek ve Yönetim Kuruluna onay için sunmak zorundadır.

1010–Zorunlu Rehberin İç Denetim Yönetmeliğine Tanınması

1100–Bağımsızlık ve Objektiflik:

1200–Yeterlilik ve Azami Mesleki Özen ve Dikkat

1300–Kalite Güvence ve Geliştirme Programı

Performans Standartları

2000–İç Denetim Faaliyetinin Yönetimi: İç denetim faaliyeti işletmeye değer katacak şekilde yönetilmek zorundadır.

2100–İşin Niteliği: İç denetim risk odaklı sistematik ve disiplinli bir yaklaşımla işletmenin risk yönetimi, yönetim ve kontrol süreçlerini değerlendirerek iyileştirilmesi yönünde katkı sağlamak zorundadır.

2200–Görev Planlaması: İç denetim faaliyetini sürdüren kişiler amaç, kapsam, kaynak dağılımı ve zamanlama konularını dikkate alarak yazılı ayrı bir plan hazırlamak zorundadır. Bu plan işletme hedeflerini, stratejilerini ve görevle ilgili riskleri içermelidir.

2300-Görevin Yapılması: İç denetim görevinin amacına ulaşması için yeterli bilgilerin edinilmesi, analiz edilmesi, değerlendirilmesi ve kayıtlı hale getirilmesi zorunludur.

2400-Sonuçların Raporlanması: İç denetim faaliyetinin sonuçları raporlanmak zorundadır.

2500–İlerlemenin Gözlenmesi: Raporlanan sonuçların durumunun izlenmesi için İç Denetim Yöneticisi tarafından bir sistem kurulması ve uygulanması zorunludur.

2600–Risklerin Kabul Edildiğinin İletilmesi: İşletmede üst yönetim tarafından kabul edilemeyecek bir riski İç Denetim Yöneticisi riski kabul etme kararını alırsa konuyu üst yönetime iletmek zorundadır. Eğer İç Yönetim Yöneticisi konunun sonuca ulaşmadığı kanaatine varırsa durumu Denetim Komitesi'ne ve Yönetim Kurulu'na bildirmek zorundadır.