T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ISO 27001: 2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURUMSAL RİSK YÖNETİMİ

ÖZGE ALTINPULLUK

YÜKSEK LİSANS TEZİ
MATEMATİK MÜHENDİSLİĞİ ANABİLİM DALI
MATEMATİK MÜHENDİSLİĞİ PROGRAMI

DANIŞMAN
PROF. DR. İBRAHİM EMİROĞLU

İSTANBUL, 2016

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ISO 27001: 2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURUMSAL RİSK YÖNETİMİ

Özge ALTINPULLUK tarafından hazırlanan tez çalışması 22.07.2016 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. İbrahim EMİROĞLU

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. İbrahim EMİROĞLU

Yıldız Teknik Üniversitesi _____

Doç. Dr. Aydın SEÇER

Yıldız Teknik Üniversitesi _____

Yrd. Doç.M.Zahid GÜRBÜZ

Doğuş Üniversitesi _____

ÖNSÖZ

Bu tez çalışmasında ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Risk Yönetimi gerekliliklerini karşılamak için yapılması gerekenler adım adım incelenmiştir ve bu gereklilikleri içeren verilerin girilmesini ve ilgili raporların alınmasını sağlayan bir yazılım geliştirilmiştir.

Özellikle tez konusunu seçerken isteklerimi göz önünde bulundurup bana yardımcı olan tez danışmanım Prof. Dr. İbrahim EMİROĞLU' na teşekkürlerimi sunarım. Ayrıca bu zorlu tez sürecinde benden desteğini bir an bile esirgemeyen ve tezin yazılım geliştirme kısmını üstlenen değerli arkadaşıma, tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen her zaman yanımda olan sevgili aileme teşekkürlerimi bir borç bilirim.

Temmuz, 2016

Özge ALTINPULLUK

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

BGYS Bilgi Güvenliği Yönetim Sistemi

ŞEKİL LİSTESİ

Sayfa

ÖZET

ISO 27001: 2013 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURUMSAL RİSK YÖNETİMİ

Özge ALTINPULLUK

Matematik Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. İbrahim EMİROĞLU

Bilgisayar ağlarının ve internetin yaygın olarak kullanılmaya başlanmasıyla Bilgi Güvenliği oldukça önemli hale gelmiştir. Kurumların çoğunlukla bilgiye, teknolojiye ve sistemlere bağımlı olmasından dolayı Bilgi Güvenliği yaşamsal önemdedir ve bilgi varlıklarının zarar görmekten korunması gereksinimi de bundan kaynaklanmaktadır. Öte yandan, bir çok şirket hala bilgi güvenliği konusunda yeterli ve gerekli önlemleri almamaktadır. Bunun sonucunda da aralarında bir çok büyük ve uluslararası kurumun da yer aldığı pek çok şirket ciddi tehdit altındadır. Bu tehditleri önceden farkedebilmek ve tehditlerin şiddetini azaltabilmek için ISO 27001: 2013 Standardının Risk Yönetimine ve bütününe uyum sağlanması gerekmektedir.

Günümüzde kurumlar hemen hemen her işlemde bir riskle karşı karşıya kalmaktadırlar. Kurumların işlevleri sırasında ortaya çıkabilecek risklerin önceden dikkatli bir biçimde ve ayrıntıları ile tanımlanıp değerlendirilmesi ve bu riskleri minimize edecek veya tam olarak ortadan kaldıracak önlemlerin alınması gerekmektedir.

Bu tez çalışmasında ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Risk Yönetimi gerekliliklerini karşılamak için yapılması gerekenler adım adım incelenmiştir ve bu gereklilikleri içeren verilerin girilmesini ve ilgili raporların alınmasını sağlayan bir yazılım geliştirilmiştir. Bu kapsamda ISO 27001 Standardının referans gösterdiği ISO 27000 ailesi incelenmiştir. Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlar anlamına gelen varlıkların belirlenmesi ve değerlerinin anlaşılması, risk analizinin yapılabilmesi ve önlemlerinin alınabilmesi için büyük önem

taşıdığı belirlenerek sunulmuştur. Risk analizinin yapılabilmesi için ne tür yollar izlenmesi gerektiği ve risk iyileştirmenin nasıl yapılacağı araştırılmıştır. Çalışmanın sonucu olarak bütün bunlar bir yazılımda ilişkilendirilerek bir araya getirilmiştir ve raporlanabilir hale getirilmiştir.

Anahtar Kelimeler: Bilgi, bilgi güvenliği, risk, risk yönetimi, risk analizi

ABSTRACT

ISO 27001: 2013 INFORMATION SECURITY MANAGEMENT SYSTEMS CORPORATE RISK MANAGEMENT

Özge ALTINPULLUK

Department of Mathematichal Engineering

MSc. Thesis

Adviser: Prof. Dr. İbrahim EMİROĞLU

Information Security has become very important since computer networks and internet is widely used. Since Organizations especially depend on information, thecnology and systems, Information Security is highly important. That is why information assets need to be protected from damage. On the other hand, many organizations do not take sufficient and necessary precautions. As a result of that, many organizations, including corporate and international organizations, are under threat. To recognise the threats and reduce level of threats, ISO 27001: 2013 Standard's Risk Management and its overall needs to be conformed.

Nowadays, organizations have risks on almost every processes. Risks that may happen during organizations activities need to be analysed carefully and defined with details and any precautions need to be taken in order to minimize or completely destroy those risks.

In this study, what to be done to meet ISO 27001: 2013 Information Security Management System Risk Management requirements is examined step by step and a software that allows to enter needed information that includes that requirements and to take related reports is developed. In this scope, ISO 27000 family which is referenced by ISO 27001 is analyzed. Defining and estimating assets which mean all valuable and need to be protected properly elements for an organization is very

important in order to analyze risks and take precautions. In order to analyze risks, what ways should be used and how to improve risks are studied. As a result of this research, all of these are developed in a software and made reportable.

Keywords: Information, information security, risk, risk management, risk analysis.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

ISO/IEC 27001 Standardı, bilgi güvenliği yönetim sistemi gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Bilgi güvenliği risk yönetimi, risklerin kurumun hedeflerine ulaşabilmek için her seviyede risklerini belirli bir yöntemle sistematik olarak tespit etmesi, değerlendirmesi, risklerin etkilerini azaltmak için önlemler alması ve bu sürecin etkin işlemesini sağlayacak şekilde izlemenmesidir. ISO 27001 bilgi güvenliği risk yönetimi; işlerin istenilen sonuçlara ulaşılmasını sağlar, iyi yönetişimi destekler, hesap verilebilirlik- şeffaflık- sorumlulukları güçlendirir, kaynak ve çalışmaların öncelikli alanlara odaklanmasını sağlar, akla uygun ve bilgiye dayanan risk almaya imkan verir ve risk gerçekleşmeden önce hazır olmayı sağlar.

1.2 Tezin Amacı

Bu tezin amacı, ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Risk Yönetimi gerekliliklerini karşılamak için nasıl bir yöntem izlenmesi ve nelere dikkat edilmesi gerektiğini incelemek ve geliştirilen yazılımın kuruluşlara bu konuda yol gösterdiğini kanıtlamaktır.

1.3 Hipotez

Geliştirlen yazılım, kurumların ISO 27001 Bilgi güvenliği Yönetim Sistemi Risk Yönetimi gerekliliklerini karşılamak için ihtiyaç duyulan yeterli bilgi ortamını sağlayarak yol göstermektedir.

BÖLÜM 2

YÖNETİM SİSTEMİ

Yönetim Sistemi; bir kuruluşun hedeflerine ulaşmak için takip etmesi gereken prosedürler kümesini tanımlar.

TS ISO IEC 27000: 2012 Standardında Yönetim sistemi şu şekilde tanımlanmıştır: Kuruluşun hedeflerini gerçekleştirmek üzere oluşturulan politikaların, prosedürlerin, kılavuzların ve ilgili kaynakların çerçevesi [1].

Kuruluş ilerleyişinde patronun istediklerini yapma yolunu tercih eden küçük kuruluşlarda belki resmi bir sisteme ihtiyaç olmayabilir. Fakat her bir çalışanın işini yapması gerektiği gibi yaptığından emin olmak için kayıtlar gerektiren ve yapılması gereken işlerin belirli bir prosedüre göre yapılması ihtiyacı duyulan büyük kuruluşlarda resmi sistemlere ihtiyaç duyulur.

ISO Yönetim Sistem Standartları, bir yönetim sistemi kurmak ve yürütmek için bir model sağlamaktadırlar. ISO Standartları uluslararası, uzman fikir birliği ve dahası global yönetim deneyimi ve pratikleri üzerine öneriler sunmaktadır. Firmaları kurumsallaştırmaya götürmektedir.

ISO Yönetim Standartları, hangi sektörde ürün ve ya hizmet üretirse üretsin büyük/ küçük bütün kuruluşlara uygulanabilir şekilde tasarlanmıştır.

2.1 Bilgi

Türk Dil Kurumu' nda bilginin tanımı:

1. İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat

2. Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf

3. İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf

4. Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler

Şeklinde ifade edilmiştir [2].

Bilgi Güvenliği Yönetim Sistemi (BGYS) için TS ISO IEC 27000 madde 3.2.2 bilgi tanımı şu şekildedir: Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır [1].

Bilgiler birçok formda saklanabilir; sayısal form (örneğin; elektronik veya optik ortam üzerindeki veri dosyaları), malzeme form (örneğin; basılı materyaller) yanı sıra çalışanların bilgileri de bilgiyi temsil edebilir.

2.2 Bilgi Güvenliği

Bilgi Güvenliği Yönetim Sistemi (BGYS) için TS ISO IEC 27000 madde 3.2.3 bilgi güvenliği tanımı şu şekildedir: Bilgi güvenliği üç ana başlığı içermektedir; gizlilik, elverişlilik ve bütünlük. Sürekli iş başarısını ve sürekliliği sağlamak amacı ile etkilerin en aza indirgenmesi için bilgi güvenliği uygulama ve yönetimi, tehditlere karşı geniş bir yelpazede göz önünde bulundurulması gereken uygun güvenlik önlemlerini içerir. Bilgi güvenliği, BGYS kullanılarak seçilen bir risk yönetimi prosesi boyunca, seçilen ve yönetilen uygulanabilir bir dizi kontroller uygulanması yoluyla belirlenen bilgi varlıklarını korumak için politikalar, prosesler, prosedürler, kurumsal yapılar, yazılım ve donanım ile elde edilir. Bu kontroller, kuruluşun özel güvenliğinin ve iş hedeflerinin yerine getirilmesini sağlamak için uygulanır, izlenir, gözden geçirilir ve gerektiğinde iyileştirilir.

2.3 Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi, hassas şirket bilgilerini yönetmek için sistematik bir yaklaşım sunar. Bilgi Güvenliği Yönetim Sistemi, bir Risk temelli yaklaşım sunarak

insanları, süreçleri ve Bilgi Teknolojileri sistemlerini kapsamaktadır. Herhangi bir sektörde büyük, orta ve küçük işletmelerde bilgi varlıklarını korumaya yardımcı olur.

Bilgi Güvenliği Yönetim Sistemi (BGYS) için TS ISO IEC 27000 madde 3.2.1 bilgi güvenliği yönetim sistemi tanımı şu şekildedir: Bir BGYS, iş hedeflerine ulaşmak amacıyla kuruluşun bilgi güvenliğinin kurulumu, uygulaması, işletimi, takibi, gözden geçirilmesi ve geliştirilmesi için sistematik bir yaklaşımdır [1].

Bu yönetim sistemi risk değerlendirmeye dayanır ve kuruluşun risk kabul seviyeleri risk yönetimi ve etkin iyileştirme için tasarlanmıştır. Bilgi varlıklarının korunması ile ilgili gereksinimlerin analizi ve uygun varlıkların uygulanması, gerektiği şekilde, bir BGYS' nin başarılı bir şekilde uygulanması için katkıda bulunmaktadır [1].

2.4 Bilgi Güvenliği Yönetim Sisteminin Önemi

Bilgi Güvenliği Yönetim Sistemi (BGYS) için TS ISO IEC 27000 madde 3.4 bilgi güvenliği yönetim sistemi niçin önemlidir tanımı şu şekildedir: Kuruluşun sahip olduğu BGYS' nin bir parçası olarak, kuruluşun bilgi varlıkları ile ilişkili risklerini ifade etmesi gerekir. Bilgi güvenliğinin sağlanması risk yönetimini gerektirir ve kuruluş tarafından kullanılan veya kuruluş içinde olan bilgilerin tüm formları ile ilgili fiziksel, insan ve teknolojik tehditlere karşı riskleri kapsar. BGYS' nin benimsenmesinin, bir kuruluş için stratejik bir karar olması beklenir. Bu kararın, kuruluşun ihtiyaçlarına uygun olarak ölçeklenmesi ve güncellenmesi ile sorunsuz bir şekilde kuruluşa entegre edilmesi gerekir. Bir kuruluşun BGYS' nin tasarımı ve uygulanması, kuruluşun hedeflerinden, güvenlik gereklerinden, kullanılan iş proseslerinden ve kuruluşun büyüklüğünden ve yapısından etkilenir. BGYS' nin tasarımının ve işletiminin; tüm müşteriler, tedarikçiler, iş ortakları, hissedarlar ve diğer ilgili üçüncü taraflar da dâhil olmak üzere kuruluşun tüm paydaşlarının çıkarlarını ve bilgi güvenliği gereklerini yansıtacak şekilde olması gerekir. Birbirine bağlı bir dünyada, bilgi ve ilgili prosesler, sistemler ve ağlar kritik iş varlıklarını oluşturmaktadır. Kuruluşlar ve sahip oldukları bilgi sistemleri ve bilgisayar ağları, bilgisayar destekli sahtekârlık, casusluk, sabotaj, tahrip, yangın ve sel gibi çok geniş kaynaklardan gelen güvenlik tehditleri ile karşı karşıyadır. Bilgi sistemlerinde ve ağlarında zarara neden olan bilgisayar virüsleri, bilgisayar korsanları ve hizmeti durdurma saldırıları gibi yıkıcı kaynaklar daha yaygın, daha iddialı ve daha karmaşık hale gelmeye başlamıştır. BGYS

hem kamu hem de özel sektör kuruluşları için önemlidir. Herhangi bir sanayi kuruluşu için BGYS, e-iş desteğini kolaylaştırır ve risk yönetimi faaliyetleri için gereklidir. Genel ve özel ağlar arasındaki ara bağlantı bilgi varlıklarının paylaşımını arttırmaktadır. Bilgi varlıklarının paylaşımı ile bilgi erişimi kontrolünün ve bilgi işlemenin zorluğu artar. Buna ek olarak, bilgi varlıklarını içeren mobil depolama cihazlarının yaygınlaşması geleneksel kontrollerin etkinliğini zayıflatabilir. Kuruluşlar, BGYS ailesi standartlarını uygulamayı kabul ettiğinde, iş ortaklarına ve diğer ilgili taraflara, tutarlı ve karşılıklı tanınabilir bilgi güvenliği ilkeleri uygulayabilir. Bilgi güvenliği, bilgi sistemlerinin tasarımında ve geliştirilmesinde her zaman dikkate alınmaz. Ayrıca, bilgi güvenliği genellikle teknik bir çözüm olarak düşünülmektedir. Ancak, teknik yollarla elde edilebilecek güvenlik sınırlı olabilir ve BGYS kapsamında uygun yönetim ve prosedürler tarafından desteklenmeden etkisiz olabilir. Bilgi sistemlerine sonradan güvenliğin entegre edilmesi zahmetli ve pahalı olabilir. BGYS, hangi kontrollerin yapılacağının belirlenmesini ve dikkatli planlamayı ve detaylara dikkati gerektirir. Örnek olarak; bilgi varlıklarına, teknik (mantıksal), fiziksel, idari (yönetsel) ya da bunların birleşimi şeklinde gerçekleşecek erişim denetimlerini, iş ve güvenlik gereklerine dayalı olarak yetkili ve sınırlı bir biçimde sağlamak için bir yol sağlar [1].

2.5 ISO 27000 Ailesi

Bu başlık altında Bilgi Güvenliği Yönetim Sistemleri ailesi incelenecektir [3], [4].

2.5.1 ISO/IEC 27000: 2012

ISO/IEC 27000: 2012 Bilgi Teknolojisi- Bilgi Güvenliği Yönetim Sistemleri- Genel Bakış ve Sözlük

ISO 27000 Ailesi standartlar için sözlük içerir, genel bakış ve tanıtım sağlar. Terimler ve Tarifleri içerir.

Kapsam: Bu standard, kuruluşlar ve bireyler için aşağıdaki konuları kapsar:

a) BGYS ailesi standardlarına genel bir bakışı,

b) Bilgi güvenliği yönetim sistemine (BGYS) girişi,

c) Planla-Uygula-Kontrol et-Önlem al (PUKÖ) prosesinin kısa bir açıklamasını,

d) BGYS ailesi standardlarında kullanılan terim ve tarifler

Amaç: ISO/IEC 27000, BGYS ailesi standardların konusunu oluşturan bilgi güvenliği yönetim sistemine genel bakışı ve ilgili terimlerin açıklanmasını sağlar [1].

Bu standard ISO tarafından kabul edilen ISO/IEC 27000 (2009) standardı esas alınarak TSE Bilgi Teknolojileri İhtisas Grubu'na bağlı Bilişim Teknolojileri Teknik Komitesi'nce hazırlanmış ve TSE Teknik Kurulu'nun 19 Temmuz 2012 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir [1].

2.5.2 ISO/IEC 27001:2013 Bilgi Teknolojisi- Bilgi Güvenliği Yönetim Sistemleri-Gerekler

Bilgi Güvenliği Yönetim Sistemi organizasyonlar için gereklilikleri tanımlar, bağımsız denetim ve belgelendirme uygulanabilmesini sağlar. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı denetimlerinde kullanılır.

Kapsam: Bu standard, dokümante edilmiş bir bilgi güvenliği sisteminin (BGYS), kuruluşun tüm ticari riskleri bağlamında kurulması, gerçekleştirilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi için gerekleri kapsar. Bağımsız kuruluşların ya da ilgili tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gerekleri belirtir. Bu standard, tüm kuruluş türlerini (örneğin; ticari kuruluşları, kamu kurumlarını, kar amaçlı olmayan kuruluşları) kapsar [1].

Amaç: ISO/IEC 27001, BGYS işletimi tarafından kuruluşun bilgi varlıklarını ve ilgili risklerini kontrol ve azaltmaya yönelik bir dizi kontrolde dâhil olmak üzere, BGYS'nin geliştirilmesi ve işletilmesi için gerekleri sağlar. BGYS işletimini yapan kuruluşların uygunluğu denetlenmiş ve onaylanmış olabilir. BGYS prosesinin uygun bir parçası olarak belirlenen gerekleri karşılamak üzere kontroller, ISO/IEC 27001 standardı Ek A'da belirtilen kontrol hedeflerinden ve kontrollerden seçilmelidir. ISO 27001 standardı Tablo A.1'de listelenen kontrol hedefleri ve kontrollerde belirtilenlerle uyumlu olarak ISO/IEC 27002 standardı Madde 5 ile Madde 15 arasından doğrudan türetilmiştir [1].

Bu standard, ISO/ IEC 27001: 2013 standardı esas alınarak, TSE Bilgi Teknolojileri İhtisas Grubu'na bağlı TK01 Bilişim Teknolojileri Teknik Komites' ince hazırlanmış ve TSE

Teknik Kurulu' nun 29 Nisan 2014 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir [5].

Bu standard yayımlandığında TS ISO/ IEC 27001: 2006 nın yerini alır [5].

TS ISO/ IEC 27001: 2006 standardı ISO/ IEC 27001: 2006 standardının Türk Standardı olarak kabul edilmiş şeklidir.

ISO 27001: 2013 standardı Risk yönetimi için ISO 31000 standardını referans alırken ISO 27001: 2006 standardı Risk yönetimi için ISO 27005 referans almıştır. Bu maddede ISO 31000 standardı incelenirken ISO 27005 standardı detayları madde 2.5.6 da verilecektir.

2.5.2.1 TS ISO 31000: 2011 Risk Yönetimi- Prensipler ve Klavuzlar

Kapsam: Bu standard, risk yönetimi hakkında ilkeleri ve genel ana hatları kapsar. Bu standard doğası ne olursa olsun, ister pozitif ister negatif sonuçlara sahip olsun, herhangi bir risk türüne uygulanabilir [6].

Amaç: Bu standardın mevcut ve gelecekteki standardlardaki risk yönetim süreçlerini harmonize etmek için kulanılması amaçlanmıştır [6].

Bu standard, ISO tarafından kabul edilen ISO 31000: 2009 standardı esas alınarak TSE Mühendislik Hizmetleri İhtisas Grubu' nca hazırlanmış ve TSE Teknik Kurulu' nun 13 Aralık 2011 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir [6].

2.5.3 ISO/IEC 27002: 2013 Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi için Uygulama Prensipleri

Bilgi güvenliği için uygulama kodu. Bir dizi bilgi güvenliği kontrol hedefleri ve genel olarak kabul görmüş güvenlik kontrolü için iyi uygulamalar hakkında bilgi içerir. Firmalar da sistem kurulumu içerisinde kılavuz rolünde bulunan standarttır. Ek A içerisinde ki 114 Madde için en iyi uygulamalar hakkında bilgi verir.

Kapsam: Bu standard, bilgi güvenliğinin sağlanması için kontrollerin seçilmesinde ve uygulanmasında kılavuz olarak kullanılmak üzere genel kabul görmüş kontrol hedeflerinin ve en iyi kontrol uygulamalarının bir listesini kapsar [1].

Amaç: ISO/IEC 27002 standardı, bilgi güvenliği kontrollerinin uygulanması konusunda kılavuzluk sağlar. Özellikle, ISO/IEC 27001 Madde A.5 ile Madde A.15 belirtilen kontrolleri desteklemek üzere Madde 5 ile Madde 15'te belirlenen en iyi uygulamaları tavsiye eder ve uygulanmaları konusunda kılavuzluk sağlar [1].

2.5.4 ISO/IEC 27003: 2010 Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi için Uygulama Kılavuzu

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Rehberidir.

Kapsam: Bu standard, ISO/IEC 27001 ile uyumlu BGYS'nin kurulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi hakkında daha fazla bilgiyi ve pratik uygulama kılavuzunu kapsar [1].

Amaç: ISOIEC 27003, ISO/IEC 27001 ile uyumlu BGYS'nin başarılı bir şekilde uygulanması için süreç odaklı bir yaklaşımı sağlar [1].

2.5.5 ISO/IEC 27004: 2009 Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi- Ölçme

Bilgi güvenliği yönetimi ölçüm tekniklerini içerir.

Kapsam: Bu standard, ISO/IEC 27001 standardında belirtilen bilgi güvenliğinin uygulanmasında ve yönetilmesinde, kullanılan kontroller ve kontrol hedeflerinin geliştirilmesinde ve BGYS etkinliğinin değerlendirilmesinde ölçümler kullanma konusunda kılavuzluğu ve tavsiyeleri kapsar [1].

Amaç: ISO/IEC 27004, ISO/IEC 27001 ile uyumlu BGYS etkinliğinin değerlendirilmesinde ölçümleri sağlayacak bir ölçüm çerçevesi sağlar [1].

2.5.6 ISO/IEC 27005: 2011 Bilgi Teknolojisi- Bilgi Güvenliği Risk Yönetimi

Bilgi güvenliği risk yönetimi standardıdır. Riskin ne şekilde ele alınacağı ile ilgili bilgiler içerir.

Kapsam: Bu standard, bilgi güvenliği risk yönetimi için kılavuzluğu kapsar. Bu standard içinde açıklanan yaklaşım, ISO/IEC 27001 standardında belirtilen genel kavramları destekler [1].

Amaç: ISO/IEC 27005, ISO/IEC 27001 bilgi güvenliği risk yönetimi gereklerinin tatmin edici bir şekilde uygulanması ve yerine getirilmesi hususunda yardımcı olmak için, süreç odaklı bir risk yönetimi yaklaşımının uygulanması konusunda kılavuzluk sağlar [1].

2.5.7 ISO/IEC 27006: 2011 Bilgi Teknolojisi- Bilgi Güvenliği Yönetim Sistemlerinin Denetimini ve Belgelendirmesini Yapan Kuruluşlar için Gerekler

Akredite olarak BGYS bağımsız denetim ve belgelendirme hizmetleri veren kuruluşlar için rehberlik sağlar. Akredite olmak isteyen kurumların uymakla yükümlü oldukları standarttır. Akreditasyon denetimlerinde standart şartlarının karşılanmasında ISO/IEC 17021'in yanında bu standarda göre de denetlenirler.

Kapsam: Bu standard, ISO/IEC 17021 standardı içinde yer alan şartlara ek olarak ISO/IEC 27001 ile uyumlu BGYS sertifikasyonu ve denetimi sağlayan kuruluşlar için gerekleri ve kılavuzu kapsar. Öncelikle, ISO/IEC 27001 standardına göre BGYS sertifikasyonu sağlayan akredite edilmiş belgelendirme kuruluşlarına destek amacıyla tasarlanmıştır [1].

Amaç: ISO/IEC 27006, ISO/IEC 17021 gereklerini sağlayan akredite belgelendirme kuruluşlarının ISO/IEC 27001 standardında belirtilen gereklere sürekli uyum içinde olmalarını sağlamak için hangi şartları sağlaması gerektiğini açıklamayı amaçlar [1].

2.5.8 ISO/IEC 27007: 2011 Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi Sistemi Denetimi için Kılavuz

Bilgi güvenliği yönetim sistemleri denetim Kurallarını içerir.

Kapsam: Bu standard, ISO 19011 verilen kılavuzluğa ilave olarak; BGYS denetimlerinin yapılması konusunu ve bilgi güvenliği yönetim sistemi denetçilerine yeterlilik konusunda kılavuzluğu kapsar. Ayrıca, genel olarak yönetim sistemleri için geçerli olan içindeki kılavuzluğu kapsar [1].

Amaç: ISO/IEC 27007, BGYS iç ve dış denetimlerine ihtiyaç duyan kuruluşlara veya ISO/IEC 27001 standardında belirtilen gereklere uygun bir BGYS kontrol programı yönetmek için kılavuzluk sağlar [1].

2.5.9 ISO/IEC 27008: 2011 Bilgi Teknolojisi- Denetçiler için Bilgi Güvenliği Kontrolleri Kılavuzu

Bilgi güvenliği kontrollerine ilişkin denetçiler için yönergeleri içermektedir.

Kapsam: Bu teknik rapor, ISO/IEC 27001 ve ISO/IEC 27005'de tanımlanan Bilgi Güvenliği Yönetim Sistemi (BGYS) (Information Security Management System-ISMS) risk yönetimi süreci ve ISO/IEC 27002 içeriğinde yer alan kontrolleri destekler.

Bu teknik rapor, bir kuruluşun bilgi güvenliği kontrollerinin (örneğin kuruluşta teknik uygunluk kontrolü de dahil olmak üzere iş süreçlerinin ve sistem ortamının) gözden geçirilmesinde kılavuzluk sağlar [7].

Amaç: Bu teknik rapor, kamu ve özel şirketler, devlet kuruluşları, kar amacı gütmeyen kuruluşlar da dahil olmak üzere, bilgi güvenliği gözden geçirmelerini ve teknik uygunluk kontrollerini gerçekleştiren her tip ve büyüklükteki kuruluşlara uygulanabilir. Bu standard yönetim sistemleri denetimleri için tasarlanmamıştır [7].

2.5.10 ISO/IEC 27010: 2012

Sektörler arası ve kurumlar arası iletişim için bilgi güvenliği yönetimine dair bilgileri içerir.

2.5.11 ISO/IEC 27011: 2008 Bilgi Teknolojisi- Telekomünikasyon Kuruluşları için ISO/IEC 27002 Standardına Göre Bilgi Güvenliği Yönetimi Sistemi Kılavuzu

ISO / IEC 27002 dayalı telekomünikasyon kuruluşlar için bilgi güvenliği yönetim kuralları içerir.

Kapsam: Bu standard, telekomünikasyon kuruluşlarında Bilgi Güvenliği Yönetimi'nin (BGY) uygulanmasını destekleyen kılavuzu kapsar [1].

Amaç: ISO/IEC 27011, telekomünikasyon kuruluşlarına, kendi sektörlerinde ISO/IEC 27002 kurallarına uyumu ve ek olarak ISO/IEC 27001 Ek-A gereklerini yerine getirmeye yönelik kılavuzluk sağlar [3].

2.5.12 ISO/IEC 27013: 2012

ISO/IEC 27001 ve ISO/IEC 20000-1 entegre uygulanması konusunda rehberlik bilgilerini içerir.

2.5.13 ISO/IEC 27014: 2013

Bilgi Güvenliği Yönetişimi hakkında bilgileri içerir.

2.5.14 ISO/IEC 27015: 2012

Finansal hizmetler için bilgi güvenliği yönetim kurallarını içerir.

2.5.15 ISO/IEC 27016: 2014

Örgütsel ekonomi ile ilgili bilgileri içermektedir.

2.5.16 ISO/IEC 27017

ISO/IEC 27002'ye dayalı Bulut bilişiminin bilgi güvenliği boyutları hakkında bilgiler içerir.

2.5.17 ISO/IEC 27018: 2014

Bulut bilişiminin kişisel olarak tanımlanan bilgiler ile ilgili gizlilik boyutlarını kapsamaktadır.

2.5.18 ISO/IEC 27019: 2013

Enerji sektöründe özel süreç kontrol sistemleri için ISO/IEC 27002 dayalı güvenlik yönetimi kurallarına ait bilgileri içerir.

2.5.19 ISO/IEC 27031:2011

İş sürekliliği için bilgi ve iletişim teknolojisi hazırlığı için yönergeleri içerir.

2.5.20 ISO/IEC 27032:2012

Siber güvenlik için kılavuzluk bilgilerini içerir.

2.5.21 ISO/IEC 27033-1: 2009

Ağ Güvenliği – Bölüm 1: Genel bakış ve kavramlar.

2.5.22 ISO/IEC 27033-2: 2012

Ağ Güvenliği Bölüm 2: Ağ güvenliği tasarım ve uygulama ilkeleri.

2.5.23 ISO/IEC 27033-3: 2010

Ağ Güvenliği – Bölüm 3: Referans ağ senaryoları – Tehditler, tasarım teknikleri ve kontrol sorunları.

2.5.24 ISO/IEC 27033-4

Ağ Güvenliği – Bölüm 4: Güvenlik ağ geçitleri kullanarak ağlar arasında güvenli iletişim.

2.5.25 ISO/IEC 27033-5

Ağ Güvenliği – Bölüm 5: Sanal Özel Ağ kullanarak ağlar arasında güvenli iletişim (VPN) .

2.5.26 ISO/IEC 27033-6

Ağ Güvenliği – Bölüm 6: Kablosuz IP ağ erişimi güvence altına alınması.

2.5.27 ISO/IEC 27034-1: 2011

Uygulama Güvenliği – Bölüm 1: Genel bakış ve kavramlar.

2.5.28 ISO/IEC 27034-2

Uygulama Güvenliği – Bölüm 2: Organizasyon normatif çerçeve

2.5.29 ISO/IEC 27034-3

Uygulama Güvenliği – Bölüm 3: Uygulama güvenliği yönetimi süreci.

2.5.30 ISO/IEC 27034-4

Uygulama Güvenliği – Bölüm 4: Uygulama güvenliği onaylama.

2.5.31 ISO/IEC 27034-5

Uygulama Güvenliği – Bölüm 5: Protokoller ve uygulama güvenliği veri yapısı kontrol.

2.5.32 ISO/IEC 27034-6

Uygulama Güvenliği – Bölüm 6: Özel uygulamalar için güvenlik rehberi.

2.5.33 ISO/IEC 27035: 2011

Bilgi Güvenliği Olay Yönetimi.

2.5.34 ISO/IEC 27036-1: 2014

Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 1: Genel bakış ve kavramlar.

2.5.35 ISO/IEC 27036-2: 2014

Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 2: Gereklilikler.

2.5.36 ISO/IEC 27036-3: 2013

Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 3: Bilgi ve İletişim Teknolojileri tedarik zinciri güvenliği için ilkeler.

2.5.37 ISO/IEC 27037: 2012

Dijital delil belirlenmesi, toplanması, elde edilmesi ve korunması için ilkeleri içerir.

2.5.38 ISO/IEC 27038

Dijital redaksiyon için özellikleri içerir.

2.5.39 ISO/IEC 27040: 2015

Depolama güvenliği

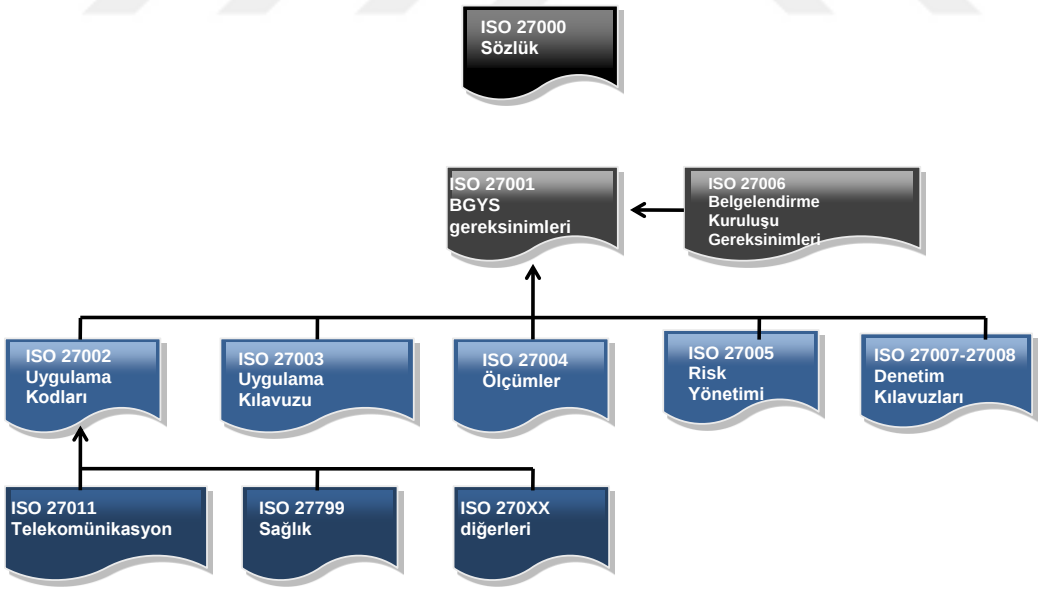
2.5.40 ISO 27799:2008 Sağlık Bilişimi – Sağlık Sektöründe ISO/IEC 27002 Kullanımı ile Bilgi Güvenliği Yönetimi

ISO/IEC 27002 Kullanılarak Sağlık Sektöründe Bilgi Güvenliğinin Sağlanması ile ilgili bilgileri içerir.

Kapsam: Bu standard, sağlık kuruluşlarında Bilgi Güvenliği Yönetimi'nin (BGY) uygulanmasını destekleyen kılavuzu kapsar.

Amaç: ISO/IEC 27799, sağlık kuruluşlarına, kendi sektörlerinde ISO/IEC 27002 kurallarına uyumu ve ek olarak ISO/IEC 27001 Ek-A gereklerini yerine getirmeye yönelik kılavuzluk sağlar.

Şekil 2.1' de ISO 27000 ailesinden ISO 27001 standardı için gerekli olan standartlardan bazıları gösterilemektedir.



Şekil 2. 1 ISO 27000 ailesi

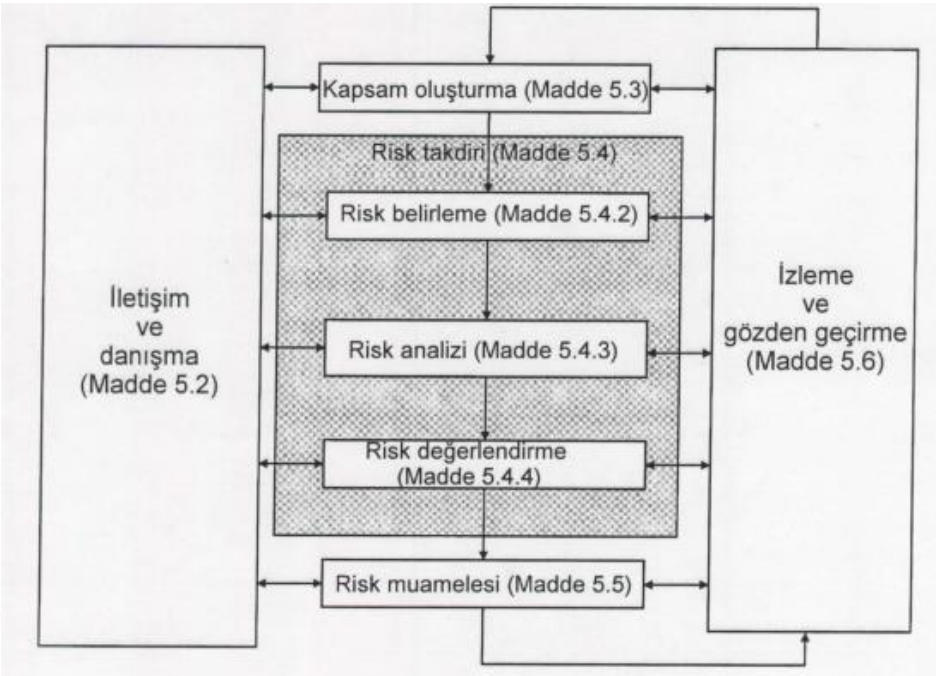
BÖLÜM 3

BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ

Bu başlık altında ISO 27001: 2013 BGYS Standardının atıfta bulunduğu TS ISO 31000: 2011 standardında ve ISO 27001: 2005 BGYS Standardının atıfta bulunduğu ISO IEC 27005: 2008 standardında Risk yönetimi için yapılması gereken Risk değerlendirme ve Risk iyileştirme süreçleri ele alınacaktır. Sonrasında Varlık Envanteri Raporu ve Risk Değerlendirme Raporu anlatılacaktır. Yazılımın veritabanı tabloları için Ek-A incelenebilir.

3.1 Risk Değerlendirme

ISO IEC 27005: 2008 Standardı Figür 1 (Bilgi güvenliği risk yönetim süreci) de ve TS ISO 31000: 2011 Standardı Şekil 3 (Risk yönetim süreci) de ifade edilene göre ve TS ISO 31000: 2011 Standardı madde 5.4.1' de belirtilene göre Risk değerlendirme süreci Risk belirleme, Risk analizi ve Risk değerleme şeklinde üç ana süreçten oluşmaktadır [8], [6]. Şekil 3.1' de Risk belirleme, Risk analizi ve Risk değerlendirme süreçleri ISO 31000 ve ISO 27005' de bahsedildiği gibi akış diyagramı halinde gösterilmektedir.



Şekil 3. 1 Risk Yönetim Süreci

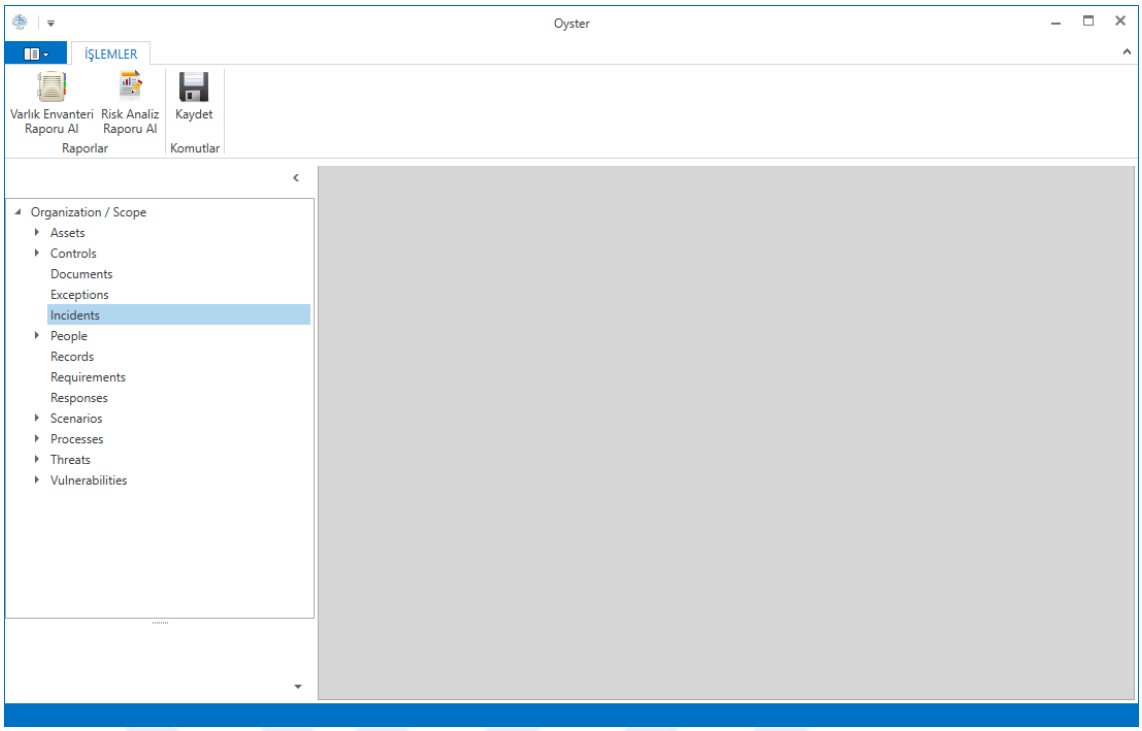
3.1.1 Risk Belirleme

Risk belirleme süreci TS ISO 31000: 2011 Standardı madde 5.4.2 de şu şekilde ifade edilmiştir: Kuruluş risk kaynaklarını, etki alanlarını, olayları ve bunların sebeplerini ve muhtemel sonuçlarını tanımlamalıdır [6].

ISO IEC 27005: 2008 Standardı madde 8.2 de ise Risk belirleme süreci Risk analizi süreci içerisinde 'Risk identification' olarak ele alınmıştır [8]. (Detaylı bilgi 2.1.2 Risk analizi maddesinde verilecektir.)

Bu tez için yazılan programda ISO 27001: 2005 BGYS Standardının Risk yönetim süreci için atıfta bulunduğu ISO IEC 27005: 2008 Standardı da göz önünde bulundurulup TS ISO 31000: 2011 Standardının istemiş olduğu risk belirleme sürecinde bahsedilen 'risk kaynağı' 'tehdit', 'olaylar' 'senaryo' ve 'risk kaynağının sebepleri' ise 'zaafiyet' olarak değerlendirildi.

Şekil 3.2 Uygulama arayüzü şeklinde Tehdit ve Zaafiyet butonları gösterilmektedir.



Şekil 3. 2 Uygulama açılış arayüzü

3.1.2 Risk Analizi

Risk analizi süreci ISO IEC 27005: 2008 Standardına göre Risk tanımlama ve Risk olasılığı olarak iki başlıktan oluşturulmuştur. TS ISO 31000: 2011 Standardına göre ise Risk analizinin oluşturulmasının birinci basamağı şu şekilde tanımlanmıştır: Risk analizi, riskin sebepleri ve kaynaklarının, onların olumlu ve olumsuz sonuçlarının ve bu sonuçların oluşabilme ihtimalinin dikkate alınmasını gerektirir [8], [6].

Bu tez için yazılan programda ISO 27001: 2013 standardının gerekliliklerini karşılamak amacıyla atıfta bulunmuş olduğu ISO 31000: 2009 yani standardın Türkçesi olan TS ISO 31000: 2011 standardında istenilen 'riskin sebepleri', 'riskin kaynakları', 'bunların olumlu, olumsuz sonuçları' ve 'oluşabilme ihtimali' sırasıyla 'tehdit', 'zaafiyet', 'açıklama' ve 'olasılık' olarak ele alınırken ISO IEC 27005: 2008 standardından faydalanıldı.

ISO IEC 27005: 2008 Standardı Risk tanımlama sürecini şu şekilde ayırmıştır: Varlıkların tanımlanması, Tehditlerin tanımlanması, Var olan kontroller, Açıklıkların tanımlanması ve Sonuçların tanımlanması [8].

ISO IEC 27005: 2008 Standardı Sonuçların tanımlanmasını şu şekilde ifade etmiştir: Varlıkların bir listesi, iş süreçlerinin bir listesi ve tehdit ve zayıflıkların bir listesi [8]. Bu nedenden dolayı Sonuçların tanımlanması en son Risk Analiz Raporunda ortaya çıkarıldı.

ISO IEC 27005: 2008 Standardına paralel gidilmesi hedeflendiği için ve ISO 27001: 2013 standardı Ek A kontrollerinden Ek A.8 Varlık yönetimi kontrolünün de gerekliliklerini karşılamak amacıyla bu bölüm Varlık yönetimi ve Risk olasılığı başlıkları altında incelenecektir. Var olan controller ise Risk iyileştirme içerisinde değerlendirilecektir.

3.1.2.1 Varlık Yönetimi

ISO 27001: 2013 Standardının Ek A kontrollerinde rehber gösterdiği ISO 27002: 2013 standardında Ek A.8.1.1 Varlık Envanteri kontrolünde ISO 27005: 2008 standardının baz alınması gerektiği belirtilmiştir [9]. Bu nedenle bu bölümde varlık, varlık grupları ve varlık değeri incelenecektir.

ISO 27001: 2013 Standardının Ek A kontrollerinde rehber gösterdiği ISO 27002: 2013 standardında Ek A.8.1.1 Varlık Envanteri kontrolünde ISO 27005: 2008 standardının baz alınması gerektiği belirtilmiştir. Bu nedenle bu bölümde varlık, varlık grupları ve varlık değeri incelenecektir.

Varlık

Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır. İnsan, bilgi, yazılım, donanım, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir [10]. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Kurum çalışanlarının zihinlerinde, konuşmalarında bulunur.

Varlık grupları

Bilgi Güvenliği Yönetim Sistemi (BGYS) için BS ISO IEC 27005: 2008 Ek B de bilgi güvenliği yönetim sistemi varlıkların belirlenmesine örnekler şu şekildedir [8]:

Özel Varlıklar:

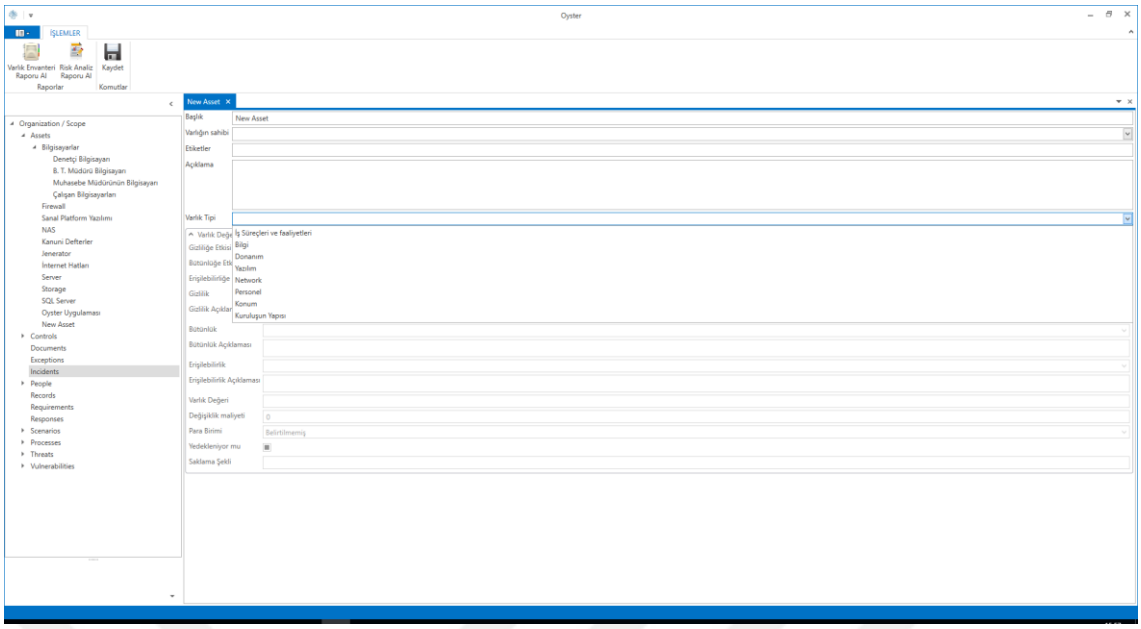
- İş Süreçleri ve faaliyetleri
- Bilgi

Destekleyici varlıklar:

- Donanım
- Yazılım
- Network
- Personel
- Konum
- Kuruluşun yapısı

Bu tez için yazılan programda da varlıklar tanımlanırken yukarıdaki varlık grupları baz alındı.

Şekil 3.3’ de varlık grupları tanımlanırken yukarıda bahsedilen varlık gruplarının baz alındığı gösterilmektedir.



Şekil 3.3 Varlık arayüzü

Varlık değeri

Bilgi Güvenliği Yönetim Sistemi (BGYS) için BS ISO IEC 27005: 2008 Ek B de bilgi güvenliği yönetim sistemi varlık değerini şu şekilde ifade etmiştir: Varlıklar tanımlandıktan sonraki adım kullanılacak ölçeğe ve her varlık için o ölçekte belirli bir değer atanmasına karar verilmesidir [8].

Varlıkların niteleyici değerleri için tipik terimler:

- Önemsiz
- Çok düşük
- Düşük
- Orta
- Yüksek
- Çok yüksek
- Kritik

Şeklindedir.

BS ISO IEC 27005: 2008 Ek B de varlık değerleri yukarıdaki gibi tanımlanmaktadır ve ISO 27001: 2005 Bilgi Güvenliği Yönetim Sistemi Standardında da aynı şekilde uygulanmakta idi. Fakat ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Standardına göre varlık değeri Gizlilik, Bütünlük ve Erişilebilirlik değerlerine göre hesaplanmaktadır.

Gizlilik

Bilginin sadece erişmesine izin verilen kişi veya kitleler için erişilebilir halde olmasıdır. Hedeflenen kişi ve kitleler dışında bilginin başkaları tarafından okunabilir ve/veya yazılabilir, değiştirilebilir, kısaca erişilebilir olması durumunda bilginin gizliliği bozulmuş olur. Bir yetkilendirme durumu söz konusudur.

Bütünlük

Bilginin kaynağında olduğu şekliyle, bozulmadan, değiştirilmeden, tutarlı bir şekilde hedeflenen kişi ve kitleler için erişilebilir olmasıdır. Bir bilginin kısmen bozulmuş veya kısmen değiştirilmiş olması bütünlüğün bozulması anlamına gelmektedir. Gizliliğin ve/veya Erişilebilirliğin kısmen bozulduğu durumlar için geçerli olan bir özelliktir.

Erişilebilirlik

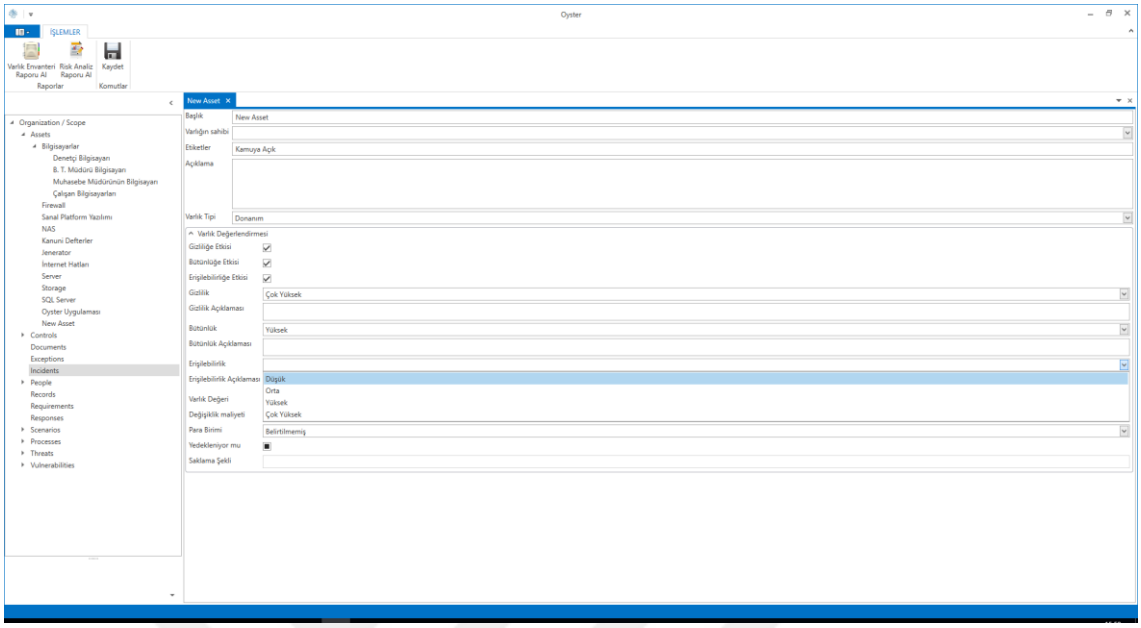
Bilginin ihtiyaç duyulduğunda erişilebilir halde olmasıdır. Gizlilikten farkı, kimlerin bilgiye erişebildiğinden çok, bilginin erişilebilir olup olmaması ile ifade edilmesidir.

ISO 27001: 2013 Standardına göre Gizlilik, Bütünlük ve Erişilebilirlik değerleri için ayrı ayrı sınıflandırma yapılması gerekmektedir. Bu sınıflandırma ISO 27005: 2008 de anlatılan varlığın niteleyici değeri baz alınarak yapılmaktadır.

Bu tez için yazılan programda da varlıklar değerleri için ISO 27001: 2013 Standardı baz alınarak yukarıdaki gibi tanımlandı.

ISO 27005: 2008 Standardında Ek.B.3 maddesinde Etki Değeri hesaplamasının yapılması gerektiği söylenmektedir. Bu doğrultuda yazılan programda tanımlanan varlığın Gizlilik, Bütünlük, Erişilebilirlik değerlerinden etki değeri hesaplatıldı ve 'Varlık Değeri' olarak belirtildi.

Şekil 3.4’ de varlığın Gizlilik, Bütünlükve Erişilebilirlik değerlerinin göz önünde bulundurulduğu gösterilmektedir.



Şekil 3.4 Varlığın gbe değerleri

3.1.2.2 Risk Olasılığı

Bu bölümde risk ve bilgi güvenliği risk değerlendirme yaklaşımı incelenecektir.

Risk

TS ISO IEC 27000: 2012 Standardında risk tanımı şu şekilde ifade etmiştir: Bir olay ve sonucunun olasılıklarının birleşimi [1].

Bilgi güvenliği risk değerlendirme yaklaşımı

BS ISO IEC 27005: 2008 Standardı madde 8.1 uygulama rehberinde risk değerlendirme yaklaşımını şu şekilde açıklamıştır: Risk değerlendirme; bilgi varlığının değerini, olabilecek tehditlerin tanımını, var olan ya da var olabilecek zayıflıkları, var olan kontrollerin tanımını ve bunların risk belirlemesindeki etkilerini, potansiyel sonuçlarının tanımlanmasını ve belirlenmiş risklerin önceliklendirilmesini belirler [8].

Bu tez için yazılan programda ISO 27005:2008 beklentisini karşılamak amacıyla tehdit ve zayıflık ara yüzleri oluşturuldu.

Tehdit

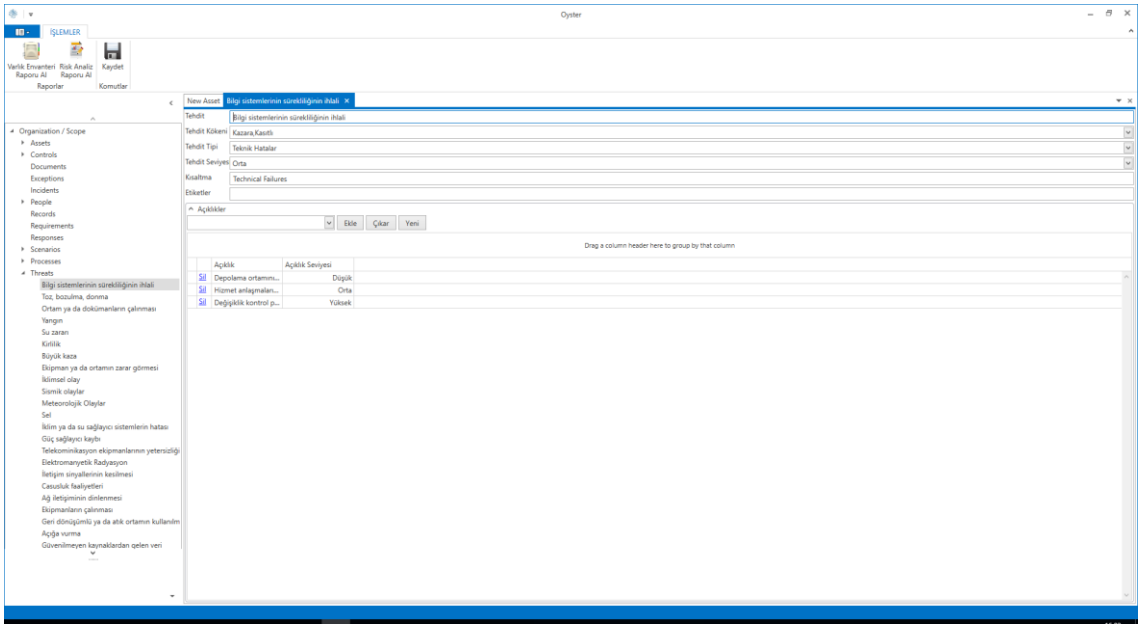
TS ISO IEC 27000: 2012 Standardı madde 2.45 de tehdidi şu şekilde açıklamıştır: Bir sistem veya kuruluşta zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni [1].

BS ISO IEC 27005: 2008 Standardı Ek C Tipik Tehditlere Örnekler bölümünde tehditlerin kasıtlı, kazara ve doğal nedenlerden kaynaklanabileceğini ifade eder [8].

Bu nedenle bu tez için yazılan programda oluşturulan Tehdit arayüzüne Tehdit Kökeni combobox olarak eklendi. Tehdit Kökeni değerleri için 'Kasıtlı', 'Kazara' ve 'Doğal' olmak üzere üç seçenek oluşturuldu.

BS ISO IEC 27005: 2008 Standardı Ek C bölümünde Tehdit Tiplerine olası örnekleri sunmaktadır. Bu tez için oluşturulan Tehdit arayüzünde Tehdit Tipleri, BS ISO IEC 27005: 2008 Standardı Ek C bölümünde verilen Tehdit Tiplerinin gereksinimlerini karşılamak amacıyla şunlar olarak belirlendi: 'Fiziksel Zarar', 'Doğal Afetler', 'Hizmet Aksaması', 'Radyasyon Nedeniyle Rahatsızlık', 'Bilginin İfşası', 'Teknik Hatalar', 'Yetkisiz Faaliyetler' ve 'Yasal Gereksinimlerden Ödün Vermek'.

Şekil 3.5' de Tehdit arayüzünde ISO 27001: 2013 gerekliliklerinin karşılandığı gösterilmektedir.



Şekil 3.5 Tehdit arayüzü

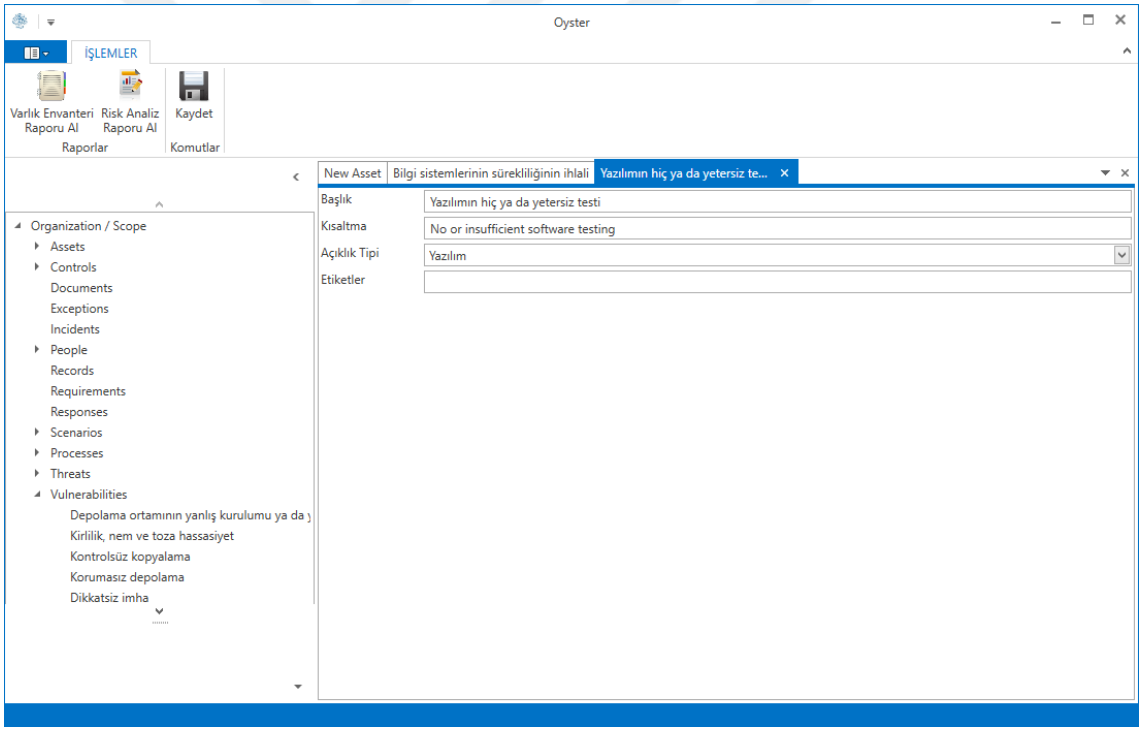
Zayıflık

TS ISO IEC 27000: 2012 Standardı madde 2.46 de zayıflığı şu şekilde açıklamıştır: Bir tehdit tarafından istismar edilebilecek bir varlık ya da kontrol zaafiyeti [1].

BS ISO IEC 27005: 2008 Standardı Ek D Zayıflık ve Zayıflık Değerlendirmesi için Metotlar bölümünde Zayıflık Tipleri şunlardır: 'Donanım', 'Yazılım', 'Network', 'Personel', 'Konum' ve 'Kurum' [8].

Bu tez için oluşturulan Zayıflık arayüzünde BS ISO IEC 27005: 2008 Standardının gereksinimlerini karşılamak amacıyla Zayıflık Tipleri Standartta belirttiği gibi oluşturuldu.

Şekil 3.6' da Zayıflık arayüzünde ISO 27001: 2013 gerekliliklerinin karşılandığı gösterilmektedir.



Şekil 3.6 Zayıflık (zaafiyet) arayüzü

Olasılık değeri

BS ISO IEC 27005: 2008 Standardı Ek E Bilgi Güvenliği Risk Değerlendirme Yaklaşımı bölümünde E.2.3 Riskin olası sonuçlarını ve olasılık değerini değerlendirmek maddesinde tehdidin ve zayıflığın olma olasılıklarından 'Likelihood Value of an incident

scenario’ yani olayın olasılık değerini sayısal olarak ilişkilendirmektedir. BS ISO IEC 27005: 2008 Standardına göre Tehdidin olma olasılığı: ‘Düşük=0’, ‘Orta=1’ ve ‘Yüksek=2’ ve Zayıflığın olma olasılığı: ‘Düşük=0’, ‘Orta=1’ ve ‘Yüksek=2’ şeklinde sayısallaştırma yapılmıştır [8].

Yazılan bu programda Tehdit ve Zayıflık değerleri birebir BS ISO IEC 27005: 2008 Standardından alındı ve Olasılık değeri standardın tarif ettiği gibi Zayıflık ve Tehdit değerlerinin toplamı şeklinde hesaplandı. Böylece Olasılık değerleri 0,1,2,3,4 değerleri olarak bulundu.

3.1.3 Risk değerleme

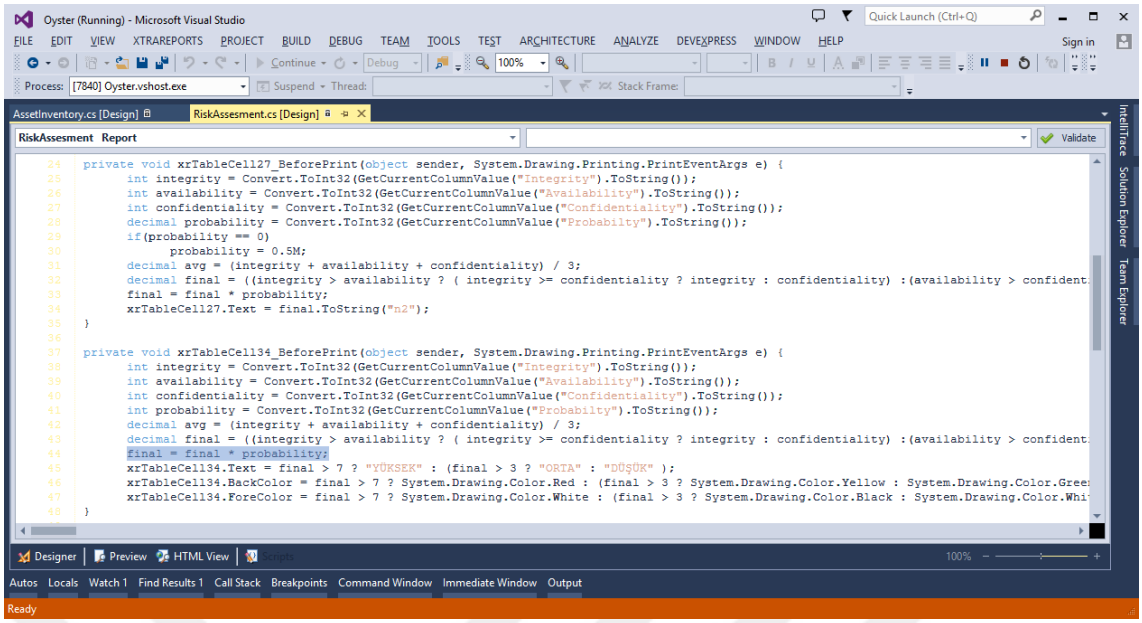
ISO 31000: 2009 Standardında Risk değerlemenin amacı şu şekilde ifade edilmiştir: Risk analizinin sonuçlarına bağlı olarak, hakkında risklerin azaltılmasına ve iyileştirilmenin gerçekleştirilmesi önceliğine gerek olduğuna karar vermede yardımcı olmaktır. Oluşturulan risk kriterleri (risk kabul kriteri vb.) ile analiz süreci sırasında bulunan risk seviyesini kıyaslamayı gerektirir [6].

ISO 31000: 2009 standardının gerekliliklerini karşılamak amacıyla bu tezde risk değeri hesaplanırken ISO 27005: 2008 standardı baz alındı.

ISO 27005: 2008 Standardında ise Risk değeri= Varlık sonuç değeri x Olasılık değeri olarak hesaplanacağı belirtilmiştir [8].

Bu tez için yazılan programda standardın gerekliliklerini karşılayacak şekilde Risk değeri= Etki değeri x Olasılık değeri şeklinde hesaplatıldı.

Şekil 3.7’ de Risk değerinin nasıl hesaplandığı yazılım kodu ile gösterilmektedir.



Şekil 3.7 Risk değeri hesaplama

Risk değeri hesaplanırken kullanılan olasılık değeri TS ISO 31000: 2011 Standardı incelendiğinde tehdit ve zayıflık değerinden seçilmek zorunda olmadığı ve Standardın 5.3.5 Risk kriterlerini tanımlama maddesinde dikkate alınacak faktörler arasında ihtimalin nasıl tanımlanacağını kuruluşun kendisinin belirlemesi gerektiği ifade edilmiştir [6].

Bu durum göz önünde bulunduruldu ve program kuruluşun risklerinin olasılık değerini kendisinin seçme imkanını da sağlayacak şekilde oluşturuldu.

Sonuç olarak bu tez için oluşturulan programda ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Standardı 6.1.2 Bilgi güvenliği risk değerlendirmesi maddesinin d bendinde geçen risklerin gerçekleşme ihtimali ifadesindeki ihtimal yani olasılık değeri ISO 27005: 2008 Standardında hesaplanan olasılık değerinden seçilebilir ya da kuruluş tarafından özel bir olasılık değeri seçilebilir hale getirildi.

3.2 Risk iyileştirme

ISO 27001: 2013 Standardında madde 6.1.3 de, Risk işleme sürecinin ISO 31000: 2009 da verilen ilkeler ve genel kılavuzlarla eş güdümlüdür ifadesine yer verilmiştir [5].

ISO 31000: 2009 Standardında ise Risk iyileştirme gerekliliği şu şekilde ifade edilmiştir: Riskleri değiştirme ve seçenekleri gerçekleştirme ile ilgili bir veya daha fazla seçeneği

seçmeyi gerektirir. ISO 31000: 2009 Standardında aynı zamanda Risk iyileştirme süreci için aşağıdakileri yapmak gerektiği ifade edilmiştir [6]:

- Risk iyileştirmenin değerlendirilmesi,
- Artık risk seviyesinin hoş görülebilir olup olmadığına ilişkin karar,
- Hoş görülebilir değil ise yeni bir risk iyileştirme üretme,
- İyileştirmenin etkinliğinin değerlendirilmesi,

Bu tez için yazılan bu programda 'seçenekler' olarak ifade edilen gerekliliği karşılamak için 'Kontrol' ara yüzü oluşturuldu. 'Risk değiştirme' olarak ifade edilen gereklilik için ise 'Proses' ara yüzüne her bir risk için yani tehdit ve zafiyet için gerekli kontroller seçilecek şekilde kontrol ilişkisi eklendi ve kontrol seçildikten sonra olasılığın değişmesi ile risk seviyesi değiştirildi. Yazılan programa standardın ifade etmiş olduğu 'Risk iyileştirmenin değerlendirilmesi ve Artık risk seviyesinin hoş görülebilir olup olmadığına ilişkin karar ' gerekliliklerini karşılamak amacıyla Olasılık (mevcut kontroller) ve Olasılık (iyileştirme kontrolleri) olmak üzere iki adet olasılık eklendi. Böylece yazılan bu program risk iyileştirme süreci gerekliliklerini de karşıladı.

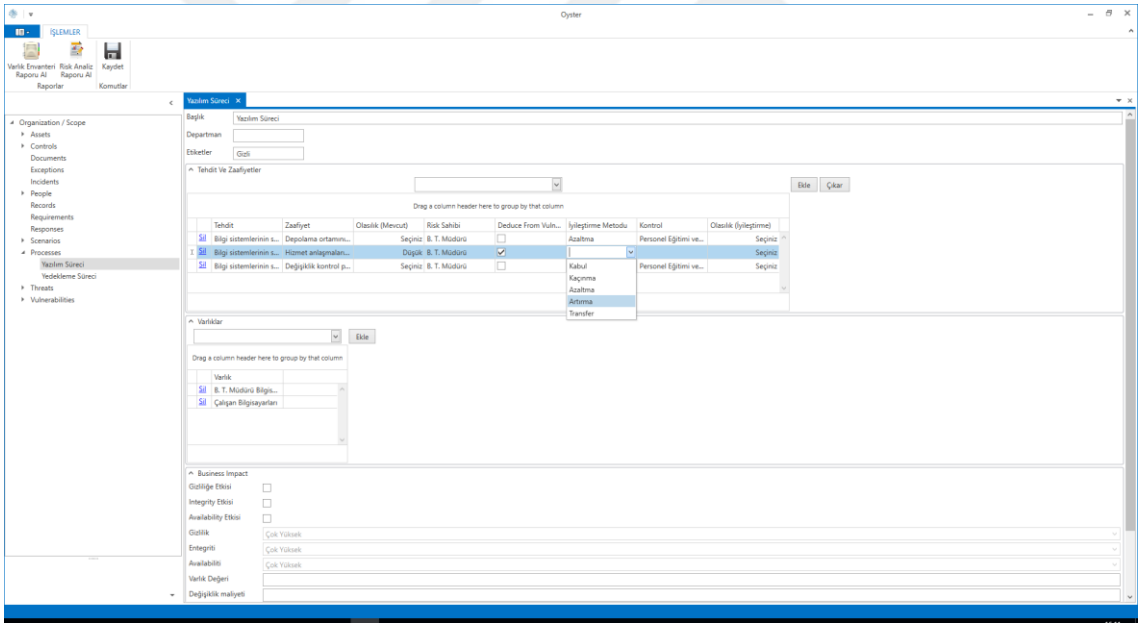
Gerek risk analizinde gerekse risk iyileştirmede risk değeri hesaplandıktan sonra risk üzerinde nasıl bir yol izleneceğine karar verilmesi gerektiği ISO 31000: 2009 Standardı madde 5.4.4 de kısmen ve madde 5.5.1 de tamamen ifade edilmiştir. Şu şekilde anlatılmıştır [6]:

- Riske yol açan faaliyetle başlamama ve devam etmeme kararı,
- Bir fırsatı takip etmek için riskin alınması veya artırılması,
- Risk kaynağını ortadan kaldırma,
- İhtimali değiştirme,
- Sonuçları değiştirme,
- Başka bir taraf veya taraflarla riski paylaşma (sözleşmeler ve riski finans etme dâhil),

Bu tez için yazılan programda ISO 31000: 2009 gereklilikleri göz önünde bulundurulduve risk iyileştirme için seçenekler ‘Proses’ ara yüzünde şu şekilde oluşturuldu:

- Riskten kaçınma: Riske yol açan faaliyetle başlamama ve devam etmeme kararı,
- Riskin artırılması: Bir fırsatı takip etmek için riskin alınması veya artırılması,
- Riski kaldırma: Risk kaynağını ortadan kaldırma,
- Riski azaltma: İhtimali değiştirme,
- Riski azaltma: Sonuçları değiştirme,
- Riskin transferi: Başka bir taraf veya taraflarla riski paylaşma (sözleşmeler ve riski finans etme dâhil),

Şekil 3.8’ de Risk iyileştirme seçeneklerinin Oyster Programında göz önüne alındığı ve standardın gerekliliklerinin karşılandığı gösterilmektedir.



Şekil 3.8 Risk iyileştirme seçenekleri

3.3 Varlık Envanteri Raporu

ISO 27001: 2013 Standardının Ek A.8 gerekliliklerini karşılamak için ve Risk Değerlendirmenin bir parçası olduğundan projede Varlık Envanteri Raporu oluşturuldu.

Varlık Envanteri için ISO 27001: 2013 Standardı gerekliliklerini karşılayan aşağıdaki bilgileri içerecek şekilde bir rapor oluşturuldu:

- Varlığın adı,
- Varlığın tanımı,
- Varlığın tipi,
- Varlığın sahibi,
- Varlığın gizlilik değeri,
- Gizlilik gerekçesi,
- Varlığın bütünlük değeri,
- Bütünlük gerekçesi,
- Varlığın erişilebilirlik değeri,
- Erişilebilirlik gerekçesi,
- Varlığın değeri,
- Varlık etiketi,
- Varlığın yedeklenip yedeklenmediği,
- Varlığın yedeğinin saklanma şekli,

Şekil 3.9’ da Oyster Programı’ ndan sonuç olarak elde edilen Varlık envanteri raporu ve raporun standardın gerekliliklerini karşıladığı gösterilmektedir.

Varlık Adı	No	Tanımı	Varlık Tipi	Sahibi	Gizlilik	Gizlilik Gerekçesi	Bütünlük	Bütünlük Gerekçesi	Erişilebilirlik	Erişilebilirlik Gerekçesi	Varlık Değeri	Varlık Etiketi	Yedekleniyor mu	Saklama Şekli
Storage	1	Server içerisindeki depolama ünitesidir. şirkete ait her türlü gizli bilgi	Bilgi	B. T. Müdürü	Çok Yüksek	Kurumun tüm dataları ve uygulamalarının tutulduğu için gizlilik yüksektir.	Çok Yüksek	Kullanıcıların ve uygulamaların verileri bulunduğundan önemlidir	Çok Yüksek	Kullanıcıların ve uygulamaların verileri bulunduğundan sürekli erişim olmalıdır.	64	Çok Gizli	Evet	
SQL Server	2	Fiziksel serverın içerisindeki sanal serverdır	Bilgi	B. T. Müdürü	Çok Yüksek	Gizli bilgileri sakladığı için önemlidir.	Çok Yüksek	Veri değiştiğinde BT sürecini tamamen etkiler	Çok Yüksek	gerekli durumlarda % 100 erişilebilir halde olmalıdır	64	Çok Gizli	Evet	Server odasında kilitli olarak saklanmaktadır.
Denetçi Bilgisayarı	3	İş için kullanılan bilgisayar	Donanım	Denetçi	Çok Yüksek	İçerisinde şirkete ait gizli bilgiler bulunmaktadır	Yüksek	gizli bilgilerin değişmesi bazı verileri etkilemektedir	Yüksek	istenildiğinde %85 erişilebilir halde olmalıdır	36	Sürece Özel	Evet	
NAS	4	NAS (Sistem yedekleme harici diski) Şirket için gizliliği yüksek Bilgilerinin Yedeklenmesin de kullanılan cihaz	Donanım	B. T. Müdürü	Yüksek	Verileri önemli ve gizli olması	Yüksek	Disk Ünitesi ile yedeklidir, Değişiklik yapılabilmesi için hp protector kullanılmalıdır.	Yüksek	İhtiyaç anında erişilebilirlik ihtiyacı yüksektir.	27	Kuruma Özel	Hayır	
Jenerator	5	Enerji kesintisi esnasında devreye girerek merkez binaya ait elektrik ihtiyacini karsilar.	Donanım	Teknik Destek Müdürü	Yüksek	Yetkisiz kişilerin erişimemesi gereklidir	Yüksek	Olası kesinti durumunda merkez binanın çalışması olumsuz etkilenir.	Orta		18	Hizmete Özel	Hayır	
B. T. Müdürü Bilgisayarı	6	BT müdürünün önemli verilerini sakladığı bilgisayar	Donanım	B. T. Müdürü	Çok Yüksek	İçerisinde şirkete ait gizli bilgiler bulunmaktadır	Çok Yüksek	değiştirilmesi durumunda bir çok süreç ve varlık etkilenmektedir	Çok Yüksek	istenildiği zaman %100 erişilebilir olmalıdır.	64	Çok Gizli	Evet	
Muhasebe Müdürünün Bilgisayarı	7	Muhasebe müdürünün gizli bilgileri bulunmaktadır	Donanım	Muhasebe Müdürü	Çok Yüksek		Çok Yüksek		Yüksek		48	Gizli		

Şekil 3.9 Varlık envanteri raporu

3.4 Risk Değerlendirme Raporu

ISO 27001: 2013 Standardının Madde 6 ve 8 gerekliliklerini karşılamak için Risk Değerlendirme Raporu oluşturuldu.

Risk Değerlendirme için ISO 27001: 2013 Standardı gerekliliklerini karşılayan aşağıdaki bilgileri içerecek şekilde bir rapor oluşturuldu:

Risk tanımlama:

- Riskin bulunduğu süreç,
- Süreçteki tehdite sebep olabilecek açıklık (zaafiyet),
- Süreçteki tehdit,
- Risk sahibi,
- Süreçte var olan kontrol,
- Riskin olma olasılığı,
- Riskin etki değeri,
- Risk skoru ve seviyesi,

Risk iyileştirme:

- İyileştirme metodu,
- İyileştirme kontrolü,
- Riskin olma olasılığı,
- Riskin etki değeri,
- Risk skoru ve seviyesi,

Şekil 3.10’ da Oyster Programı’ ndan sonuç olarak elde edilen Risk değerlendirme raporu ve raporun standardın gerekliliklerini karşıladığı gösterilmektedir.

Risk Değerlendirme Tablosu

Risk Tanımlama													Risk İyileştirme							
							Etki Değeri									Etki Değeri				
No	Süreç	Zaafiyet	Tehdit	Risk Sahibi	Var Olan Kontrol	Olasılık	Özellik	Bütünlük	Erişilebilirlik	Etki Pu	Risk Skor	Risk Seviyesi	İyileştirme Metodu	Kontrol	Olasılık	Özellik	Bütünlük	Erişilebilirlik	Risk Skoru	Risk Seviyesi
1	Yazılım Süreci	Depolama ortamının yanlış kurulumu ya da yetersiz bakımı	Bilgi sistemlerinin sürekliliğinin ihlali	B. T. Müdürü	Personel Eğitimi verilmesi	3	Çok Yüksek	Orta	Çok Yüksek	3,50	10,50	YÜKSEK	Azaltma	Profesyonel destek alınması	2	Çok Yüksek	Orta	Çok Yüksek	7,00	ORTA
2	Yazılım Süreci	Hizmet anlaşmalarının eksikliği ya da yetersizliği	Bilgi sistemlerinin sürekliliğinin ihlali	B. T. Müdürü		1	Çok Yüksek	Orta	Çok Yüksek	3,50	3,50	ORTA			1	Çok Yüksek	Orta	Çok Yüksek	3,50	ORTA
3	Yazılım Süreci	Değişiklik kontrol prosedürlerinin yetersizliği	Bilgi sistemlerinin sürekliliğinin ihlali	B. T. Müdürü	Personel Eğitimi verilmesi	4	Çok Yüksek	Orta	Çok Yüksek	3,50	14,00	YÜKSEK			4	Çok Yüksek	Orta	Çok Yüksek	14,00	YÜKSEK
4	Yedekleme Süreci	BGYS kayıtlarını gözden geçirme için resmi prosedürlerin yetersizliği	Verinin bozulması	B. T. Müdürü		4	Çok Yüksek	Yüksek	Çok Yüksek	3,50	14,00	YÜKSEK			4	Çok Yüksek	Yüksek	Çok Yüksek	14,00	YÜKSEK
5	Yedekleme Süreci	Yazılımın hiç ya da yetersiz testi	Hakların kötüye kullanımı	B. T. Müdürü		2	Çok Yüksek	Yüksek	Çok Yüksek	3,50	7,00	ORTA			2	Çok Yüksek	Yüksek	Çok Yüksek	7,00	ORTA
6	Yedekleme Süreci	Yazılımın bilinen hataları	Hakların kötüye kullanımı	B. T. Müdürü		1	Çok Yüksek	Yüksek	Çok Yüksek	3,50	3,50	ORTA			1	Çok Yüksek	Yüksek	Çok Yüksek	3,50	ORTA
7	Yedekleme Süreci	Erişim haklarının yanlış verilmesi	Hakların kötüye kullanımı	B. T. Müdürü		0	Çok Yüksek	Yüksek	Çok Yüksek	3,50	1,75	DÜŞÜK			0	Çok Yüksek	Yüksek	Çok Yüksek	1,75	DÜŞÜK
8	Yedekleme Süreci	Risk tanımlama ve değerlendirme prosedürlerinin yetersizliği	Hakların kötüye kullanımı	B. T. Müdürü		2	Çok Yüksek	Yüksek	Çok Yüksek	3,50	7,00	ORTA			2	Çok Yüksek	Yüksek	Çok Yüksek	7,00	ORTA
9	Yedekleme Süreci	Kullanılmadığında sistemin kilitlenmemesi	Hakların kötüye kullanımı	B. T. Müdürü		2	Çok Yüksek	Yüksek	Çok Yüksek	3,50	7,00	ORTA			2	Çok Yüksek	Yüksek	Çok Yüksek	7,00	ORTA
10	Yedekleme Süreci	Depolama ortamının yanlış kurulumu ya da yetersiz bakımı	Bilgi sistemlerinin sürekliliğinin ihlali	B. T. Müdürü		3	Çok Yüksek	Yüksek	Çok Yüksek	3,50	10,50	YÜKSEK			3	Çok Yüksek	Yüksek	Çok Yüksek	10,50	YÜKSEK

Şekil 3.10 Risk değerlendirme raporu

BÖLÜM 4

SONUÇ VE ÖNERİLER

Çoğunlukla bilgiye, teknolojiye ve sistemlere bağımlı olmasından dolayı Bilgi Güvenliği yaşamsal önemdedir ve bilgi varlıklarının zarar görmekten korunması gereksinimi de bundan kaynaklanmaktadır. Artan bilgi güvenlik tehditlerinden kurtulmak ve minimize etmek için alınması gereken önlemler hayati derecede önemlidir. Bu tehditleri önceden farkedebilmek ve tehditlerin şiddetini azaltabilmek için ISO 27001: 2013 Standardının Risk Yönetimine ve bütününe uyum sağlaması gerekmektedir. Bu bağlamda yazılan tez, kuruluşları yönlendirerek varlıkları nasıl tanımlanması gerektiğini ve riskleri belirledikten sonra nasıl minimize edilmesi gerektiğini kendine misyon edinmiştir.

Yapılan bu çalışmada, süreçlerdeki riskler belirlenirken iş sürekliliğine etkisi tanımlanmamıştır. Projenin senaryo kısmı geliştirilmelidir.

KAYNAKLAR

[1] TS ISO/IEC 27000 Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Yönetim Sistemleri- Genel Bakış ve Sözlük.

[2] Türk Dil Kurumu, www.tdk.gov.tr, 05 Ocak 2012.

[3] Ekşi B., 2015, http://www.burakeksi.com/iso-27000-ailesi-hangi-standartlardan-olusur, 12 Şubat 2015.

[4] International Organization for Standardisation, Management system standards, http://www.iso.org/iso/home/standards/management-standards.htm, 15 Mayıs 2016.

[5] ISO IEC 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Standardı.

[6] TS ISO 31000: 2011 Risk Yönetimi Prensipler ve Kılavuzlar.

[7] ISO/IEC 27008: 2011 Bilgi Teknolojisi- Denetçiler için Bilgi Güvenliği Kontrolleri Kılavuzu.

[8] BS ISO/IEC 27005: 2008 Information Technology- Security Techniques- Information Security Risk Management.

[9] ISO IEC 27001: 2006 Bilgi Güvenliği Yönetim Sistemi Standardı.

[10] Muharremoğlu G., 2013, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/olasi-zafiyetlerin-tahmininde-temel-bilgi-guvenligi-prensiplerinin-kullanilmasi.html, 26 Aralık 2013.

EK-A

YAZILIMIN VERİTABANI TABLOLARI

Yazılım veritabanı tobloları bu bölümde anlatılmıştır.

A-1 Genel Bilgiler

Vulnerability, zaafiyetlerin(açıklıkların) tutulduğu tablodur.

Thread, tehditlerin tutulduğu tablodur.

Asset, varlıkların tutulduğu tablodur.

Scenario, senaryoların tutulduğu tablodur.

Control, kontrollerin tutulduğu tablodur.

Process, süreçlerin tutulduğu tablodur.

Person, kişilerin tutulduğu tablodur.

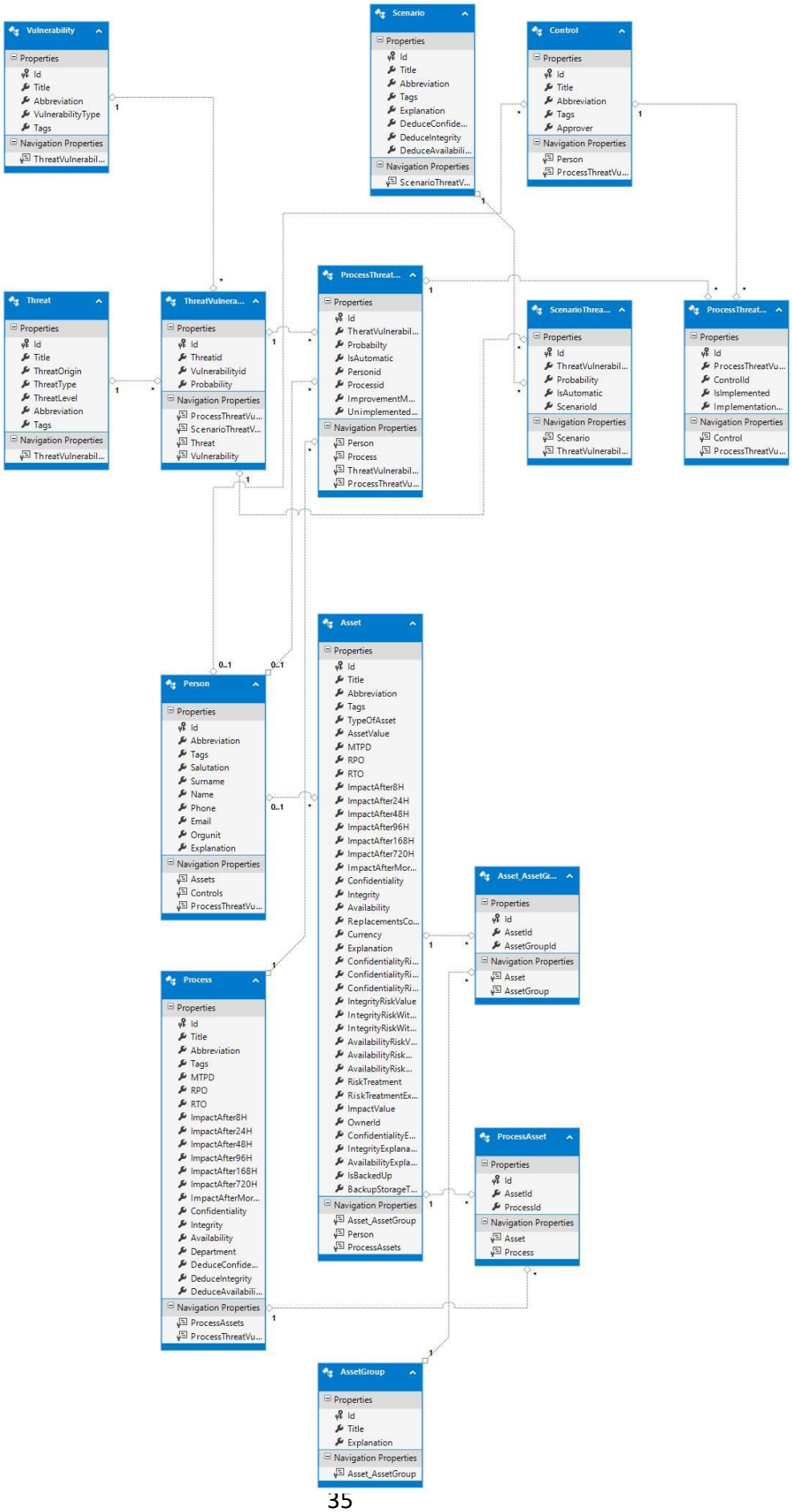
A-2 İlişki Tabloları

ThreatVulnerability, Tehdit ve zaafiyet (açıklık) ilişkisinin tutulduğu tablodur.

ProcessThreatVulnerability, ThreatVulnerability tablosu ile süreçlerin ilişkilendirildiği tablodur.

ScenarioThreatVulnerability, ThreatVulnerability tablosu ile senaryonun ilişkilendirildiği tablodur.

ProcessThreatVulnerabilityControl, ProcessThreatVulnerability tablosu ile kontrollerin ilişkilendirildiği tablodur.


Vulnerability
Properties
Id
Title
Abbreviation
VulnerabilityType
Tags
Navigation Properties
ThreatVulnerabil...
Scenario
Properties
Id
Title
Abbreviation
Tags
Explanation
DeduceConfide...
DeduceIntegrity
DeduceAvailabili...
Navigation Properties
ScenarioThreatV...
Control
Properties
Id
Title
Abbreviation
Tags
Approver
Navigation Properties
Person
ProcessThreatVu...
Threat
Properties
Id
Title
ThreatOrigin
ThreatType
ThreatLevel
Abbreviation
Tags
Navigation Properties
ThreatVulnerabil...
ThreatVulnera...
Properties
Id
Threatid
Vulnerabilityid
Probability
Navigation Properties
ProcessThreatVu...
ScenarioThreatV...
Threat
Vulnerability
ProcessThreat...
Properties
Id
TheratVulnerabil...
Probabilty
IsAutomatic
Personid
Processid
ImprovementM...
Unimplemented...
Navigation Properties
Person
Process
ThreatVulnerabil...
ProcessThreatVu...
ScenarioThrea...
Properties
Id
ThreatVulnerabil...
Probability
IsAutomatic
Scenarioid
Navigation Properties
Scenario
ThreatVulnerabil...
ProcessThreat...
Properties
Id
ProcessThreatVu...
Controlld
IsImplemented
Implementation...
Navigation Properties
Control
ProcessThreatVu...
Asset
Properties
Id
Title
Abbreviation
Tags
TypeOfAsset
AssetValue
MTPD
RPO
RTO
ImpactAfter8H
ImpactAfter24H
ImpactAfter48H
ImpactAfter96H
ImpactAfter168H
ImpactAfter720H
ImpactAfterMor...
Confidentiality
Integrity
Availability
ReplacementsCo...
Currency
Explanation
ConfidentialityRi...
ConfidentialityRi...
ConfidentialityRi...
IntegrityRiskValue
IntegrityRiskWit...
IntegrityRiskWit...
AvailabilityRiskV...
AvailabilityRisk...
AvailabilityRisk...
RiskTreatment
RiskTreatmentEx...
ImpactValue
OwnerId
ConfidentialityE...
IntegrityExplana...
AvailabilityExpla...
IsBackedUp
BackupStorageT...
Navigation Properties
Asset_AssetGroup
Person
ProcessAssets
Person
Properties
Id
Abbreviation
Tags
Salutation
Surname
Name
Phone
Email
Orgunit
Explanation
Navigation Properties
Assets
Controls
ProcessThreatVu...
Asset_AssetGr...
Properties
Id
AssetId
AssetGroupId
Navigation Properties
Asset
AssetGroup
Process
Properties
Id
Title
Abbreviation
Tags
MTPD
RPO
RTO
ImpactAfter8H
ImpactAfter24H
ImpactAfter48H
ImpactAfter96H
ImpactAfter168H
ImpactAfter720H
ImpactAfterMor...
Confidentiality
Integrity
Availability
Department
DeduceConfide...
DeduceIntegrity
DeduceAvailabili...
Navigation Properties
ProcessAssets
ProcessThreatVu...
ProcessAsset
Properties
Id
AssetId
ProcessId
Navigation Properties
Asset
Process
AssetGroup
Properties
Id
Title
Explanation
Navigation Properties
Asset_AssetGroup
0..1
1
*

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	:Özge ALTINPULLUK
Doğum Tarihi ve Yeri	:13.03.1986/ Domaniç
Yabancı Dili	:İngilizce
E-posta	:ozge.altinpulluk@hotmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Y. Lisans	Mat. Mühendisliği	YTÜ	-
Lisans	Mat. Mühendisliği	YTÜ	2010
Lise	Fen Bilimleri	Kütahya Atatürk	2004

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2014 - 2016	Vericert Belgelendirme	Denetçi
2012 - 2012	Axis Danışmanlık	Danışman
2009 - 2010	YTÜ Bilgi İşlem	Öğrenci Asistan