T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ISO/IEC JTC 1/SC 27 "BT GÜVENLİK TEKNİKLERİ" STANDARDLARININ SİBER GÜVENLİĞE KATKISI

İsmail Sinan TATLIGİL

Danışman
Dr. Öğr. Üyesi Ali BOYACI

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI
İSTANBUL – 2020

KABUL VE ONAY SAYFASI

İsmail Sinan TATLIGİL tarafından hazırlanan **" ISO/IEC JTC 1/SC 27 "BT Güvenlik Teknikleri" Standardlarının Siber Güvenliğe Katkısı"** adlı tez çalışması 13/07/2020 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Siber Güvenlik Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman	**Dr. Öğr. Üyesi Ali BOYACI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi M. Cem KASAPBAŞI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Prof. Dr. Ali BULDU** Marmara Üniversitesi	.....

Onay Tarihi : **24/07/2020**

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 24.07.2020 tarih ve 2020/288 numaralı Yönetim Kurulu Kararının 1. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "İsmail Sinan TATLIGİL" (TC:19493261454) adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

24/07/2020

İsmail Sinan TATLIGİL

İÇİNDEKİLER

Sayfa

ÖZET

Yüksek Lisans Tezi

ISO/IEC JTC 1/SC 27 "BT GÜVENLİK TEKNİKLERİ" STANDARDLARININ SİBER GÜVENLİĞE KATKISI

İsmail Sinan TATLIGİL

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Siber Güvenlik Anabilim Dalı

Danışman: Dr. Öğr. ÜyesiAli BOYACI

2020, 59 sayfa

Bu çalışmada,

ISO/IEC JTC 1/ SC 27 Komitesinin hazırlamış olduğu ISO 27001 Bilgi Güvenliği Yönetim Sisteminin, ISO 27002 ve ISO 27005 standartları ve komitenin diğer yayınladığı standartlar ve kılavuzlarının birlikte kullanılarak uygulandığı takdirde kuruluşların siber güvenliğine katkıları ele alınmaktadır.

Siber güvenliğin bir parçası olan bilgi güvenliğinin etkin bir şekilde uygulanması için gerekli olduğu değerlendirilen komitenin hazırladığı ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27007,ISO 27008, ISO 27009, ISO 27010, ISO 27011, ISO 27013, ISO 27014, ISO 27016, ISO 27017, ISO 27018, ISO 27019, ISO 27021, ISO 27031, ISO 27036, ISO 27701, ISO 30111 standarları değerlendirilerek hazırlanmıştır.

Anahtar Kelimeler: Bilgi güvenliği, bilişim güvenliği, güvenlik standartları, ISO 27001, ISO 27002, kişisel verilerin korunması, sızma testi, siber güvenlik.

ABSTRACT

M.Sc. Thesis

THE CONTRIBUTION ISO/IEC JTC 1/SC 27 "IT SECURITY TECHNIQUES" STANDARDS TO CYBER SECURITY

İsmail Sinan TATLIGİL

İstanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Cyber Security

Supervisor: Assist.Prof. Dr. Ali BOYACI

2020, 59 pages

In this Study,

If the ISO 27001 Information Security Management System prepared by the ISO / IEC JTC 1 / SC 27 Committee is used together with the ISO 27002 and ISO 27005 standards and other standards and guidelines published by the committee, the contributions of organizations to cyber security are discussed.

ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27007, ISO 27008, ISO 27009, ISO 27010, ISO 27011, ISO 27013, ISO 27014, ISO 27016, ISO 27017, ISO 27018, ISO 27019, ISO 27021, ISO 27031, ISO 27036, ISO 27701, ISO 30111 standards prepared by the committee, which is considered to be necessary for the effective implementation of information security, which is a part of cyber security, have been prepared by evaluating.

Keywords: Cyber security, informatics security, information security, ISO 27001, ISO 27002, penetration test, protection of personal data, security standards.

TEŞEKKÜR

Bu araştırmada karşılaştığım akademik zorlukları, bilgi ve tecrübesi ile aşmamda yardımcı olan değerli hocamız Dr. Öğr. Üyesi Ali BOYACI'ya,

Sibernetik kelimesini kelime dağarcığıma ekleyen değerli hocamız Prof. Dr. Ayhan SONGAR'a teşekkürlerimi sunarım.

Araştırmanın yürütülmesinde maddi ve manevi yardımlarını gördüğüm Sevgili Eşim ve Oğlum'a teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan tüm aileme sonsuz sevgi ve saygılarımı sunarım.

İsmail Sinan TATLIGİL
İSTANBUL, 2020

ÇİZELGELER

SİMGELER VE KISALTMALAR

AES	Advanced Encryption Standard
AMD	Amendment
APT	Advanced Persistent Threat
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilgi Teknolojileri
COR	Corrigendum
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
ISMS	Information Security Management System
ISO	Industry Standards of Organisation
ITSM	Information Technology Service Management
JTC	Joint Technical Committee
OTP	One Time Password
PII	Personally Identifiable Information
SC	Subcommittees
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
TOTP	Time Based One Time Password
UPS	Uninterruptible Power Supply
WPA	Wireless Protected Access

1. GİRİŞ

Dünyada ve ülkemizde bilişim güvenliği ihtiyacı her geçen gün artıyor. Bilişim güvenliği, günümüzde Siber Güvenlik olarak adlandırılıyor. Siber güvenlik çok geniş bir kavram olduğu gibi güvenliği de çok kapsamlı ve geniş bir yelpazeyi kapsıyor.

Tüm dünya, siber güvenliği sağlamak adına bir çok yöntem kullanıyor. Bu yöntemler katılan ülkerlerle birlikte bir standart haline getiriliyor. Bu standartlar oluşturulurken tüm ilgili ülkelerin uzmanları genel olarak uygulanması gereken gereklilikleri belirliyor. Belirlenen bu gereklilikler ülkelerin standartlaştırma ve akreditasyon kurumlarınca onaylanarak yürürlüğe konuluyor.

Siber güvenlik alanı sürekli geliştiği ve yeni teknolojiler dahil olduğundan sürekli geliştirilmekte ve yeni standarlar geliştiriliyor. İlgili ülkelerin tamamı tarafından kabul edilmiş olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi ise siber güvenlik için temel oluşturuyor.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi genel olarak uçtan uca güvenlik konularını ele alıyor. İnsan Kaynakları, Fiziksel Güvenlik, Tedarikçi Güvenliği, Bilişim Sistemleri Güvenliği, Bilişim ile ilgili yada etkilenen kanun ve yönetmelikler bir kurum ve kuruluş için gerekli olan tüm konuları kapsıyor.
Fakat standartlar yapısı gereği 1 kişilik kuruluş içinde 10.000 kişilik kuruluş içinde uygulanabilir olması gerekiyor. Bu sebeple standartlar nasıl yapılacağını tarif etmez, ne yapılması gerektiğini belirler. Örneğin standart sizden yemek yemenizi ister.

Ne yiyeceğinizi (Sebze, Et, Balık, Tavuk vd.) tanımlamaz?
Nasıl Yiyeceğinizi (Elle, Kaşıkla, Çatalla, keserek vd.) tanımlamaz ?
Yiyeceğiniz yemeği nereden alacağınızı yada hangi marka yiyeceği alacağınızı tanımlamaz?

Bu sebeple standart sizden sadece yapılması gerekeni ister. Yemek yemeniz ile ilgili neler yapabileceğiniz ile ilgili soruları ise yayınlamış olduğu diğer standartlarla ilişkilendirerek bu kılavuz standartları kullanmanızı tavsiye eder.
ISO 27001 Bilgi Güvenliği Yönetim Sisteminin de içinde bulunduğu ISO/IEC JTC 1/SC 27 Komitesinin yayınlamış olduğu 191 adet standarttan, kuruma uygun olanlarıyla birlikte kullanılması, siber güvenliğe daha fazla katkı sağlayacaktır.

Tez içerisinde standartların yıl revizyon numaraları (ISO/IEC 27001:2013) ile ele alınmamıştır. Bunun sebebi standartlar sürekli geliştirilmesi sebebiyle standartlara erişimin daha kolay sağlanması amaçlanmaktadır.

Bu tez çalışması sürerken ISO/IEC JTC 1/SC 27 komitesi 27001 standardının 2020 revizyonuna son taslak çalışmasını yapmaktadır.

2. LİTERATÜR ÖZETİ

Ganbat, (2013), Bilgi Güvenliği üzerine ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO 27005 Bilgi Güvenliği Risk Yönetimi standartlarını ele alarak ISO 27001 Bilgi Güvenliği Risk Yönetimi içerisindeki Gizlilik, Bütünlük ve Erişebilirlik kavramlarına uygun olarak risk yönetimi için yayınlanmış olan standardı ele almaktadır.

Mete, (2010), Bilgi İşlem Merkezlerinde ISO 27001 Bilgi Güvenliği Yönetim Sisteminin uygulanmasını ele almakta ancak ISO 27001 dışında başka bir standardı ele almamaktadır. ISO 27001 içerisinde bulunan EK-A kontrollerinin oluşmasını sağlayan ISO 27002 standardından bahsetmiştir.

Kandemirli, (2012), Bilgi Teknolojileri Güvenliği ve Sigorta şirketinde ISO 27001 Bilgi Güvenliği Yönetim Sistemi çervesinde uygulanması ile ilgili olarak ISO 20000 Bilgi Teknolojileri Hizmet Yönetimi ve COBIT (Control OBjectives for Information Technologies) standartlarını ele alarak uygulma olarak ele almıştır. Fakat ISO 20000 Bilgi Teknolojileri Hizmet Yönetimi standardı içerisinde ayrı bir madde olarak Bilgi Güvenliğini ele almaktadır. COBIT ise ISO 'ya ait olmayıp ISACA kar amacı gütmeyen kuruluşa aittir.

Gürcan, (2014), ISO 27001 Tabanlı Bir Yaklaşımla Finans Sektörü İçin Bilgi Güvenlik Yönetimi Gereksinimlerinin Değerlendirilmesinde, National Institute of Standards and Technology (NIST) ve ITIL standardlarını ele almıştır. Ancak ISO içerisinde 18/07/2017 tarihinde sonlandırılan ISO 27015 Information Security Management Guidelines For Financial Services standardını ele almamıştır.

Gencer, (2015), ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım'da ISO 27000, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006, ISO 27007, ISO 27011 ve ISO 27099 standartlarının olduğunu atıf yaparak sadece bahsetmektedir.

Altınpulluk, (2016), ISO 27001: 2013 Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi içerisinde Komitenin yayınladığı standartların başlıklarını Türkçe olarak yazmaktadır. ISO 27005 standardını ele almakta ve ISO standarlatı içerisindeki ISO 31000 Kurumsal Risk Yönetimini de değerlendirmektedir. Ancak Kurumsal Risk Yönetimi ile ilgili ISO 31010 Risk Değerlendirme Teknikleri standardını ele almamaktadır.

Kılıç, (2019), ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye'de Hukuk Bürolarında Bilgi Güvenliği Yönetimi içerisinde sadece komitenin yayınladığı standartların standart numaralarından bahsedilmekte ve öz değerlendirme soruları ISO 27001 standardının tamamını kapsamamaktadır.

Erdoğan (2020), Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ISO 27001 Standardının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi çalışmasında standardın Ek-A kontrolleri listelenmiş fakat nasıl hayata geçirileceğine dair bilgi içermemektedir.

3. SİBER GÜVENLİK

Günümüzde "Siber" kelimesi çok kullanılsa da aslında bu kelimenin dilimizde kullanımı ilk olarak 1970'li yılların sonunda Prof.Dr. Ayhan SONGAR'ın "Sibernetik" adlı kitabında yer almaktadır.

Kitabın genel bilgiler bölümünden, kısaca tarihe bir göz atıldığı takdirde, bugün kullanılan bir çok terimin kökeni görülebilmektedir.

1948 yılında yayınladığı ilk eserine "Cybernetics or Communication in the Animal and the machine" (Sibernetik veya hayvan ve makinede kontrol ve haberleşme) adını vererek Sibernetik'in aşağı yukarı tam ve en veciz bir tarifini yapan Sibernetik'in babası sayılan Nobert Wiene'dir. Sibernetik'in Türkçe olarak anlamını hayvan ve makinenin ki insanda bir hayvan olarak ele alındığından yani canlı ve cansız sistemlerin aynı başlık altında incelendiğini, bir bakıma müşterek taraflarının bulunduğunu, bütün "organize sistemlerin" haberleşme ve kontrol prensip ve mekanizmalarını, yani işleyiş tarzı olduğu anlaşılmaktadır. Kökünü eski Yunanca "Kübernetes" ve Latince "Gobernare"den aldığı, her ikisi de "sevk ve idare" anlamında kelimelerdir. (Songar, 1979)

Siber Güvenlik son dönemlerde üretilen bir kelime gibi olsa da aslında yıllardır kullanılan bir kelime olduğuna şahit olmaktayız. Günümüzde Siber Güvenliğin tanımı Bilgi varlıklarının ağlar arası, bilgi sistemleri aracılığı ile işlenirken, depolanırken ve iletilirken maruz kalabileceği tüm tehditlerden korunması olarak ele almaktadır. (ISACA, 2017)

Siber Güvenlik bu anlamda tesisler, binalar ve odalar gibi fiziksel erişimden başlayarak dijital ve teknik güvenliğe kadar ulaşan bir yapıyı ele almaktadır.

İnternet tabanlı yazılımın temel olarak güvenliği ele alınacağı zaman bu yazılımın uygulama sunucuları, veri tabanı sunucuları, entegrasyonu olan uygulama ve sunucuları, ağ güvenliği ve internet güvenliği gibi daha da

detaylandırılabilecek katmanlı, mimari ve yapısal bir siber güvenlik analizi yapılması gerekmektedir.

İnternet tabanlı yazılımın katmanlı, mimari ve yapısal olarak ele alındığında ise güvenliğin arttırılması için yazılım geliştirme aşamalarının tamamında siber güvenlik prensipleri ve standartların uygulanması önem kazanmaktadır.

Yazılım yaşam döngüsü içerisinde hata düzeltme, revizyon ve versiyonlama gibi adımların, oturum açma, yetkilendirme, işletim sistemi ve veri tabanı sistemi gibi çok yönlü siber güvenlik ihtiyaçlarının analizi gerekmektedir.

Siber güvenliğin son adımı ise, bir güvenlik kırılmasına müdahale ya da incelemedir. Müdahale ve inceleme işlemleri öncesinde hukuki bir süreç izlenecek ise konu adli bilişim alanına devredilmesi ya da birlikte çalışılması faydalı olacaktır.

4. ISO STANDARTLARININ GELİŞTİRİLMESİ, ÜYELİK VE ÜYE ÜLKELER

ISO standartları dünyada yapılan iş ve işlemlerin, ürünlerin aynı standartlara sahip olmalarını hedeflemektedir. Birçok uzmanı bir araya getirerek bu standartların oluşturulması sağlanmaktadır. Bu sayede globalleşme adımında bu standartlarla uyumlu olan kurum ve kuruluşlar global pazarda yerlerini alabilmektedir.

Bir kuruluş ilgili standartları etkin bir şekilde uygulayarak, ölçerek ve sürekli olarak iyileştirerek sürdürüğü takdirde büyümeme olasılığı çok düşüktür. Ülkemizde ISO standartlarıyla ilgili olarak en bilineni ISO 9001 Kalite Yönetim Sistemi'dir.

Kalite Yönetim Sistemi, bir ürünün kaliteli olduğunu değil, ürün ya da hizmetin üretilişinden, ürün ya da hizmetin son tüketimine kadar ki olan süreçlerinin ele alınmasını ve yönetilmesini ele almaktadır.

Dünyada da en popüler standartlar sıralamasında ISO 9000 Ailesi ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi en popülerleridir. (ISO.ORG, Popular Standards, 2020)

4.1. ISO Standartlarının Geliştirilmesi

Standartlar oluşturulurken üye olan ülkelerdeki uzmanlar bir araya getirilerek standarta uyacak tüm tipte kuruluşlar göz önüne alınarak hareket edilmektedir.

ISO standartların geliştirilmesini genellikle 3 yıl içerisinde gerçekleştirmektedir. Sürece, belirli bir alandaki pazar ihtiyacını karşılayan bir taslak geliştirilmesi ile başlarlar. Bu daha sonra yorum ve daha fazla tartışma için paylaşılır. (ISO.ORG, Developing Standards, 2020)

Oylama süreci fikir birliğinin anahtarıdır. Bu başarılırsa, taslak bir ISO standardı olma yolunda ilerliyor. Anlaşmaya varılamazsa, taslak daha fazla değiştirilecek ve yeniden oylanacak. (ISO.ORG, Developing Standards, 2020)

İlk tekliften nihai yayına kadar, bir standart geliştirmek genellikle yaklaşık 3 yıl sürer. (ISO.ORG, Developing Standards, 2020)

ISO standartlarda dahil olmak üzere 6 farklı yayını bulunmaktadır. (ISO.ORG, Yayınlar, 2020)

Uluslararası Standartlar;
Uluslararası Standart, belirli bir bağlamda optimum düzen derecesine ulaşmayı amaçlayan faaliyetler veya sonuçları için kurallar, yönergeler veya özellikler sağlar. Birçok şekilde olabilir. Ürün standartlarının yanı sıra diğer örnekler şunları içerir: test yöntemleri, uygulama kodları, kılavuz standartlar ve yönetim sistemleri standartları.

Teknik Özellik (TS);
Teknik Şartname, halen teknik gelişme altındaki veya Uluslararası Standartta gelecekteki, ancak hemen değil, bir anlaşma olasılığının olacağına inandığı yerlere yöneliktir. Hemen kullanmak üzere bir Teknik Şartname yayınlanır, ancak geri bildirim almak için de bir araç sağlar. Amaç, sonunda Uluslararası Standart olarak dönüştürülüp yeniden yayınlanmasıdır.

Teknik Rapor (TR);
Teknik Rapor, önceki iki yayından farklı türde bilgiler içerir. Örneğin, bir anketten veya bilgilendirici bir rapordan elde edilen verileri veya algılanan “son teknoloji” bilgisini içerebilir.

Halka Açık Şartname (PAS);
Halka açık bir Spesifikasyon, bir çalışma grubundaki uzmanların fikir birliğini veya ISO dışındaki bir kuruluştaki bir fikir birliğini temsil eden

acil bir pazar ihtiyacına yanıt vermek için yayınlanır. Teknik Spesifikasyonlarda olduğu gibi, Kamuya Açık Spesifikasyonlar, derhal kullanılmak üzere yayınlanır ve ayrıca bir Uluslararası Standarda dönüşümü için geri bildirim almanın bir yolu olarak hizmet eder. Kamuya Açık Belirtimler maksimum altı yıl ömrüne sahiptir, bundan sonra Uluslararası bir standarda dönüştürülebilir veya geri çekilebilir.

Uluslararası Çalıştay Anlaşmaları;
Uluslararası Atölye Anlaşması, piyasa oyuncularının "açık atölye" ortamında müzakere etmesini sağlamak için normal ISO komite sistemi dışında geliştirilen bir belgedir. Uluslararası Çalıştay Anlaşmaları tipik olarak idari olarak bir üye organ tarafından desteklenmektedir. Yayınlanan anlaşma, gelişimine katılan katılımcı kuruluşların bir göstergesini içermektedir. Uluslararası bir Atölye Anlaşması maksimum altı yıl ömre sahiptir, bundan sonra başka bir ISO'ya dönüştürülebilir veya otomatik olarak geri çekilebilir.

Kılavuzlar;
Rehberler sadece budur. Okuyucuların standartların değer kattığı ana alanlar hakkında daha fazla anlamalarına yardımcı olurlar. Bazı Kılavuzlar, ISO standartlarının nasıl ve neden daha iyi, daha güvenli ve daha verimli çalışmasını sağlayabileceği hakkında bilgi veriyor.

4.2. Üyelik ve Üye Ülkeler

Bireyler veya şirketler ISO üyesi olamaz. Ülkeler üye olabilmektedir.

Üç üye kategorisi vardır. Her biri ISO sistemi üzerinde farklı bir erişim ve etkiye sahiptir. Bu, her bir ulusal standartlar organının farklı ihtiyaç ve kapasitelerini tanıyarak kapsayıcı olmamıza yardımcı olur. (ISO.ORG, Members, 2020)

Tam üyeler (veya üye organlar) ISO teknik ve politika toplantılarına katılarak ve oy vererek ISO standartlarının geliştirilmesini ve stratejisini etkiler. Tam üyeler ISO Uluslararası Standartlarını ulusal olarak satar ve benimser. (ISO.ORG, Members, 2020)

Muhabir üyeler, ISO teknik ve politika toplantılarına gözlemci olarak katılarak ISO standartları ve stratejisinin gelişimini gözlemlemektedir. Muhabir üyeler ISO Uluslararası Standartlarını ulusal olarak satabilir ve benimseyebilir. (ISO.ORG, Members, 2020)

Abone üyeleri ISO'nun çalışmalarından haberdar olurlar ancak işlerine katılamazlar. Ulusal olarak ISO Uluslararası Standartlarını satmaz veya kabul etmez. (ISO.ORG, Members, 2020)

5. ISO/IEC JTC 1/SC 27 "BT GÜVENLİK TEKNİKLERİ" KOMİTESİ

Tüm dünyanın konuştuğu “Bilgi Güvenliği, Siber Güvenlik ve Mahremiyetin Korunması” alanları ISO içerisinde ISO/IEC JTC 1/SC 27 Komitesi tarafından yönetilmektedir.

Komite üyeliği, katılımcı üyeler ve gözlemci üyeler olarak ayrılmaktadır. ISO Katılımcı üye ülkeler ve kurumları Çizelge 1.1.’ de ve ISO gözlemci üye ülkeler ve kurumları Çizelge 1.2.’ de yer verilmiştir. Türkiye Cumhuriyeti gözlemci üyeler içerisindedir.

Çizelge 1.1. ISO/IEC JTC 1/SC 27 Komitesi Katılımcı Üyeler

Ülkeler	**Kurum Kısaltması**
Brazil	ABNT
France	AFNOR
United States	ANSI
Austria	ASI
India	BIS
Philippines	BPS
United Kingdom	BSI
Indonesia	BSN
Panama	COPANIT
Cyprus	CYS
Mexico	DGN
Germany	DIN
Denmark	DS
Malaysia	DSM
Ukraine	DSTU
United Arab Emirates	ESMA
Russian Federation	GOST R
Algeria	IANOR
Bolivia, Plurinational State of	IBNORCA
Luxembourg	ILNAS
Peru	INACAL
Costa Rica	INTECO
Argentina	IRAM
Iran, Islamic Republic of	ISIRI
Japan	JISC
Korea, Republic of	KATS

Kazakhstan	KAZMEMST
Lebanon	LIBNOR
Mauritius	MSB
Belgium	NBN
Netherlands	NEN
Ireland	NSAI
New Zealand	NZSO
Poland	PKN
Rwanda	RSB
Australia	SA
South Africa	SABS
China	SAC
Canada	SCC
Finland	SFS
Israel	SII
Sweden	SIS
Slovenia	SIST
Saint Kitts and Nevis	SKNBS
Norway	SN
Switzerland	SNV
Singapore	SSC
Spain	UNE
Italy	UNI
Uruguay	UNIT
Slovakia	UNMS SR

Çizelge 1.2. ISO/IEC JTC 1/SC 27 Komitesi Gözlemci Üyeler

Ülkeler	**Kurum Kısaltması**
Belarus	BELST
Bosnia and Herzegovina	ISBIH
Bulgaria	BDS
Chile	INN
Côte d'Ivoire	CODINORM
Czech Republic	UNMZ
El Salvador	OSN
Estonia	EVS
Eswatini	SWASA
Ghana	GSA
Hong Kong	ITCHKSAR
Hungary	MSZT
Iceland	IST
Kenya	KEBS
Lithuania	LST

Morocco	IMANOR
North Macedonia	ISRSM
Pakistan	PSQCA
Palestine, State of	PSI
Portugal	IPQ
Romania	ASRO
Saudi Arabia	SASO
Senegal	ASN
Serbia	ISS
Sri Lanka	SLSI
Thailand	TISI
Trinidad and Tobago	TTBS
Turkey	TSE

Komitede 191 adet yayınlanmış standart bulunmakta olup çalışmaları devam eden 70 adet standart bulunmaktadır. Bu standartların geliştirilmesinde üye ülkeler görüş ve uygunluk vermektedir. Üye ülkelerin de kendi ayna komiteleri (Mirror Committee) bulunmaktadır. Türkiye Cumhuriyeti'ni ISO'da TSE (Türk Standartları Enstitüsü) temsil etmektedir. (ISO.ORG, Committee, 2020)

Komite tarafından yayınlanmış olan standartlar Çizelge 1.3.'te yer verilmiştir.

Çizelge 1.3. ISO/IEC JTC 1/SC 27 Komitesi Tarafından Yayınlanan Standartlar

Standart Numarası	**İngilizce Adı**
ISO/IEC 7064:2003	Check character systems
ISO/IEC 9796-2:2010	Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2006	Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:2011	Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2011	Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9797-3:2011/AMD 1:2020	Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function
ISO/IEC 9798-1:2010	Entity authentication — Part 1: General

ISO/IEC 9798-2:2019	Entity authentication — Part 2: Mechanisms using authenticated encryption
ISO/IEC 9798-3:2019	Entity authentication — Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999/COR 2:2012	Entity authentication — Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:2009	Entity authentication — Part 5: Mechanisms using zero-knowledge techniques
ISO/IEC 9798-6:2010	Entity authentication — Part 6: Mechanisms using manual data transfer
ISO/IEC 10116:2017	Modes of operation for an n-bit block cipher
ISO/IEC 10118-1:2016	Hash-functions — Part 1: General
ISO/IEC 10118-2:2010/COR 1:2011	Hash-functions — Part 2: Hash-functions using an n-bit
ISO/IEC 10118-3:2018	Hash-functions — Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998/COR 1:2014	Hash-functions — Part 4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:2010	Key management — Part 1: Framework
ISO/IEC 11770-2:2018	Key management — Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:2015/AMD 1:2017	Key management — Part 3: Mechanisms using asymmetric techniques
ISO/IEC 11770-4:2017	Key management — Part 4: Mechanisms based on weak secrets
ISO/IEC 11770-4:2017/AMD 1:2019	Key management — Part 4: Mechanisms based on weak secrets — Amendment 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)
ISO/IEC 11770-5:2011	Key management — Part 5: Group key management
ISO/IEC 11770-6:2016	Key management — Part 6: Key derivation
ISO/IEC 13888-1:2009	Non-repudiation — Part 1: General
ISO/IEC 13888-2:2010/COR 1:2012	Non-repudiation — Part 2: Mechanisms using symmetric techniques
ISO/IEC 13888-3:2009	Non-repudiation — Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 14516:2002	Guidelines for the use and management of Trusted Third Party services
ISO/IEC 14888-1:2008	Digital signatures with appendix — Part 1: General
ISO/IEC 14888-2:2008/COR 1:2015	Digital signatures with appendix — Part 2: Integer factorization based mechanisms

ISO/IEC 14888-3:2018	Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms
ISO/IEC 15408-1:2009	Evaluation criteria for IT security — Part 1: Introduction and general model
ISO/IEC 15408-2:2008	Evaluation criteria for IT security — Part 2: Security functional components
ISO/IEC 15408-3:2008	Evaluation criteria for IT security — Part 3: Security assurance components
ISO/IEC TR 15443-1:2012	Security assurance framework — Part 1: Introduction and concepts
ISO/IEC TR 15443-2:2012	Security assurance framework — Part 2: Analysis
ISO/IEC TR 15446:2017	Guidance for the production of protection profiles and security targets
ISO/IEC 15816:2002	Security information objects for access control
ISO/IEC 15945:2002	Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:2016	Cryptographic techniques based on elliptic curves — Part 1: General
ISO/IEC 15946-5:2017	Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation
ISO/IEC 17825:2016	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
ISO/IEC 17922:2017	Telebiometric authentication framework using biometric hardware security module
SO/IEC 18014-1:2008	Time-stamping services — Part 1: Framework
ISO/IEC 18014-2:2009	Time-stamping services — Part 2: Mechanisms producing independent tokens
ISO/IEC 18014-3:2009	Time-stamping services — Part 3: Mechanisms producing linked tokens
ISO/IEC 18014-4:2015	Time-stamping services — Part 4: Traceability of time sources
ISO/IEC 18031:2011/AMD 1:2017	Deterministic random bit generation
ISO/IEC 18032:2005	Prime number generation
ISO/IEC 18033-1:2015	Encryption algorithms — Part 1: General
ISO/IEC 18033-2:2006/AMD 1:2017	Encryption algorithms — Part 2: Asymmetric ciphers
ISO/IEC 18033-3:2010	Encryption algorithms — Part 3: Block ciphers
ISO/IEC 18033-4:2011	Encryption algorithms — Part 4: Stream ciphers
ISO/IEC 18033-5:2015	Encryption algorithms — Part 5: Identity-based ciphers

ISO/IEC 18033-6:2019	Encryption algorithms — Part 6: Homomorphic encryption
ISO/IEC 18045:2008	Methodology for IT security evaluation
ISO/IEC 18367:2016	Cryptographic algorithms and security mechanisms conformance testing
ISO/IEC 18370-1:2016	Blind digital signatures — Part 1: General
ISO/IEC 18370-2:2016	Blind digital signatures — Part 2: Discrete logarithm based mechanisms
ISO/IEC 19086-4:2019	Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII
ISO/IEC TS 19249:2017	Catalogue of architectural and design principles for secure products, systems and applications
ISO/IEC 19592-1:2016	Secret sharing — Part 1: General
ISO/IEC 19592-2:2017	Secret sharing — Part 2: Fundamental mechanisms
ISO/IEC TS 19608:2018	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
ISO/IEC 19772:2009/COR 1:2014	Authenticated encryption
ISO/IEC 19790:2012	Security requirements for cryptographic modules
ISO/IEC TR 19791:2010	Security assessment of operational systems
ISO/IEC 19792:2009	Security evaluation of biometrics
ISO/IEC 19896-1:2018	Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements
ISO/IEC 19896-2:2018	IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
ISO/IEC 19896-3:2018	Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
ISO/IEC TR 20004:2015	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC 20008-1:2013	Anonymous digital signatures — Part 1: General
ISO/IEC 20008-2:2013	Anonymous digital signatures — Part 2: Mechanisms using a group public key
ISO/IEC 20009-1:2013	Anonymous entity authentication — Part 1: General

ISO/IEC 20009-2:2013	Anonymous entity authentication — Part 2: Mechanisms based on signatures using a group public key
ISO/IEC 20009-4:2017	Anonymous entity authentication — Part 4: Mechanisms based on weak secrets
ISO/IEC 20085-1:2019	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques
ISO/IEC 20085-2:2020	Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus
ISO/IEC TS 20540:2018	Testing cryptographic modules in their operational environment
ISO/IEC 20543:2019	Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
ISO/IEC 20889:2018	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC 21827:2008	Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)
ISO/IEC 21878:2018	Security guidelines for design and implementation of virtualized servers
ISO/IEC 24745:2011	Biometric information protection
ISO/IEC 24759:2017	Test requirements for cryptographic modules
ISO/IEC 24760-1:2019	A framework for identity management — Part 1: Terminology and concepts
ISO/IEC 24760-2:2015	A framework for identity management — Part 2: Reference architecture and requirements
ISO/IEC 24760-3:2016	A framework for identity management — Part 3: Practice
ISO/IEC 24761:2019	Authentication context for biometrics
ISO/IEC 27000:2018	Information security management systems — Overview and vocabulary
ISO/IEC 27001:2013/COR 2:2015	Information security management systems — Requirements
ISO/IEC 27002:2013/COR 2:2015	Code of practice for information security controls
ISO/IEC 27003:2017	Information security management systems — Guidance
ISO/IEC 27004:2016	Information security management — Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2018	Information security risk management
ISO/IEC 27006:2015/AMD 1:2020	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2020	Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
ISO/IEC TS 27008:2019	Guidelines for the assessment of information security controls
ISO/IEC 27009:2020	Sector-specific application of ISO/IEC 27001 — Requirements
ISO/IEC 27010:2015	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2016/COR 1:2018	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 27013:2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Governance of information security
ISO/IEC TR 27016:2014	Information security management — Organizational economics
ISO/IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2019	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019:2017	Information security controls for the energy utility industry
ISO/IEC 27021:2017	Competence requirements for information security management systems professionals
ISO/IEC TR 27023:2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032:2012	Guidelines for cybersecurity
ISO/IEC 27033-1:2015	Network security — Part 1: Overview and concepts
ISO/IEC 27033-2:2012	Network security — Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3:2010	Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

ISO/IEC 27033-4:2014	Network security — Part 4: Securing communications between networks using security gateways
ISO/IEC 27033-5:2013	Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27033-6:2016	Network security — Part 6: Securing wireless IP network access
ISO/IEC 27034-1:2011/COR 1:2014	Application security — Part 1: Overview and concepts
ISO/IEC 27034-2:2015	Application security — Part 2: Organization normative framework
ISO/IEC 27034-3:2018	Application security — Part 3: Application security management process
ISO/IEC 27034-5:2017	Application security — Part 5: Protocols and application security controls data structure
ISO/IEC 27034-6:2016	Application security — Part 6: Case studies
ISO/IEC 27034-7:2018	Application security — Part 7: Assurance prediction framework
ISO/IEC TS 27034-5-1:2018	Application security — Part 5-1: Protocols and application security controls data structure, XML schemas
ISO/IEC 27035-1:2016	Information security incident management — Part 1: Principles of incident management
ISO/IEC 27035-2:2016	Information security incident management — Part 2: Guidelines to plan and prepare for incident response
ISO/IEC 27036-1:2014	Information security for supplier relationships — Part 1: Overview and concepts
ISO/IEC 27036-2:2014	Information security for supplier relationships — Part 2: Requirements
ISO/IEC 27036-3:2013	Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-4:2016	Information security for supplier relationships — Part 4: Guidelines for security of cloud services
ISO/IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038:2014	Specification for digital redaction
ISO/IEC 27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

ISO/IEC 27040:2015	Storage security
ISO/IEC 27041:2015	Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042:2015	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015	Incident investigation principles and processes
ISO/IEC 27050-1:2019	Electronic discovery — Part 1: Overview and concepts
ISO/IEC 27050-2:2018	Electronic discovery — Part 2: Guidance for governance and management of electronic discovery
ISO/IEC 27050-3:2020	Electronic discovery — Part 3: Code of practice for electronic discovery
ISO/IEC 27102:2019	Guidelines for cyber-insurance
ISO/IEC TR 27103:2018	Cybersecurity and ISO and IEC Standards
ISO/IEC TR 27550:2019	Privacy engineering for system life cycle processes
ISO/IEC 27701:2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC TS 29003:2018	Identity proofing
ISO/IEC 29100:2011/AMD 1:2018	Privacy framework
ISO/IEC 29101:2018	Privacy architecture framework
ISO/IEC 29115:2013	Entity authentication assurance framework
ISO/IEC 29128:2011	Verification of cryptographic protocols
ISO/IEC 29134:2017	Guidelines for privacy impact assessment
ISO/IEC 29146:2016	A framework for access management
ISO/IEC 29147:2018	A framework for identity management — Part 1: Terminology and concepts
ISO/IEC 24760-2:2015	A framework for identity management — Part 2: Reference architecture and requirements
ISO/IEC 24760-3:2016	A framework for identity management — Part 3: Practice
ISO/IEC 24761:2019	Authentication context for biometrics
ISO/IEC 27000:2018	Information security management systems — Overview and vocabulary
ISO/IEC TR 29149:2012	Best practices for the provision and use of time-stamping services
ISO/IEC 29150:2011/COR 1:2014	Signcryption
ISO/IEC 29151:2017	Code of practice for personally identifiable information protection
ISO/IEC 29190:2015	Privacy capability assessment model

ISO/IEC 29191:2012	Requirements for partially anonymous, partially unlinkable authentication.
ISO/IEC 29192-1:2012	Lightweight cryptography — Part 1: General
ISO/IEC 29192-2:2019	Lightweight cryptography — Part 2: Block ciphers
ISO/IEC 29192-3:2012	Lightweight cryptography — Part 3: Stream ciphers
ISO/IEC 29192-4:2013/AMD 1:2016	Lightweight cryptography — Part 4: Mechanisms using asymmetric techniques
ISO/IEC 29192-5:2016	Lightweight cryptography — Part 5: Hash-functions
ISO/IEC 29192-6:2019	Lightweight cryptography — Part 6: Message authentication codes (MACs)
ISO/IEC 29192-7:2019	Lightweight cryptography — Part 7: Broadcast authentication protocols
ISO/IEC TS 30104:2015	Physical Security Attacks, Mitigation Techniques and Security Requirements
ISO/IEC 30111:2019	Vulnerability handling processes

6. TÜRKİYE CUMHURİYETİ'NDE ISO 27001 STANDARDI İLE İLGİLİ YASALAR

Ülkemizde Bilgi Güvenliği Yönetim Sistemiyle ilgili olarak yayınlanmış olan kanun, yönetmelik ve mevzuatlar bulunmaktadır. Bunlar kurumların kendi iş ve işlemleri için ISO 27001 sertifikasını almalarının zorunlu hale gelmesini sağlamaktadır.

Yasalar dışında ülkemizde gerçekleştirilen çoğu ihalede bir gereklilik olarak ISO 27001 sertifikası istenmektedir. E-KAP (Elektronik Kamu Alımları Platformu) incelendiği takdirde birçok ihalede ISO 27001 Sertifikasının gereklilik olduğu görülecektir. (E-KAP, 2020)

Gelir İdaresi Başkanlığı tarafından yetki verilen E-Fatura özel entegratörlüğü başvurusu için ISO 27001 Sertifikası bir zorunluluk olarak istenmektedir. (GİB, 2020)

Bilgi Teknolojileri ve İletişim Kurumu tarafından Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği içerisinde ISO 27001 sertifikası istenmektedir. (BTK, 2014)

Enerji Piyasası Düzenleme Kurumu yönetmeliğinde ISO 27001 sertifikası zorunluluğunu istenmektedir (EPDK, Enerji Piyasası Düzenleme Kurumu, 2013).

Daha sonra yayınlamış olduğu diğer yönetmeliklerle de petrol piyasasına da ISO 27001 sertifikası zorunlu hale getirmişti. Aynı zamanda EPDK birçok yönetmeliğin ISO 27019 Endüstriyel Kontrol Sitemleri standardını da rehber alınmasını istemektedir (EPDK, Enerji Piyasası Düzenleme Kurumu, 2017).

Gümrük ve Ticaret Bakanlığı, gümrük işlemlerinin kolaylaştırılması kapsamında bu faaliyetleri gerçekleştirmek isteyen kuruluşların başvuru aşamasında ISO 27001 sertifikasına sahip olmalırını istemektedir (Ticaret, 2013).

7. ISO 27001 STANDARDININ YAPISI

ISO 27001 standardının uygulanması 4. Madde Kuruluşun Bağlamı ile başlamakta olup, 10. Madde İyileştirme ile tamamlanmaktadır. Çizelge 2.1 ISO 27001 Standardı Maddeleri çizelgesindedir. Bu maddelere ek olarak standardın EK-A bölümünde A.5 Bilgi Güvenliği Politikaları ile A.18 Uyum maddeleri arasında toplam 114 adet kontrolden oluşmaktadır. (ISO/IEC 27001, 2013) Çizelge 2.2 ISO 27001 Standardı EK-A Maddeleri çizelgesindedir

Çizelge 2.1. ISO 27001 Standardı Maddeleri

ISO 27001 Ana Maddeleri
4. Madde Kuruluşun Bağlamı
5. Madde Liderlik
6. Madde Planlama
7. Madde Destek
8. Madde İşletim
9. Madde Performans Değerlendirme
10. Madde İyileştirme

Çizelge 2.2. ISO 27001 Standardı EK-A Maddeleri

ISO 27001 EK-A Maddeleri
A.5 Bilgi güvenliği politikaları
A.6 Bilgi güvenliği organizasyonu
A.7 İnsan kaynakları güvenliği
A.8 Varlık yönetimi
A.9 Erişim kontrolü
A.10 Kriptografi
A.11 Fiziksel ve çevresel güvenlik
A.12 İşletim güvenliği
A.13 Haberleşme güvenliği
A.14 Sistem temini, geliştirme ve bakımı
A.15 Tedarikçi ilişkileri
A.16 Bilgi güvenliği ihlal olayı yönetimi
A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları
A.18 Uyum

EK-A maddeleri ISO 27001 standardına ait olmayıp ISO 27002 standardı içerisinden alınmaktadır. Bu sebep ISO 27001 standardı içerisinde Çizelge A.1 de listelenen kontrol amaçları ve kontroller, Madde 6.1.3 bağlamında kullanılmak üzere, doğrudan ISO/IEC 27002:2013 [1] madde 5'ten madde 18'e kadar listelenenlerden çıkarılmış ve sıraya konulmuştur şeklinde ifade geçmektedir. (ISO/IEC 27002, 2013)

ISO 27001 standardının içerisinde bir diğer standart olarak ISO 27002 birlikte kullanılmaktadır. Bu nedenle standart içerisinde bire bir olarak ilişkilendirilmese de komitenin yayınlamış olduğu diğer standartlar birlikte kullanıldığında bilgi ile sistem kurmak yerine standartlarla ilişkilendirilmiş bir şekilde kurulması Siber Güvenliğe katkı sağlayacaktır.

8. ISO 27001:2013 VE KOMİTENİN YAYINLADIĞI DİĞER STANDARTLARIN İLİŞKİLENDİRİLMESİ

Komitenin yayınlamış olduğu tüm standartlar birbiriyle ilişkilendirilmektedir. ISO 27001 standardı ile diğer standartların ilişkilendirilmesi yapısı ve açıklamaları incelenmektedir.

8.1. ISO 27001 Standardının Ana Maddelerinin Uygulanması (ISO 27003)

Birçok kuruluş yönetim sisteminin kurulması için danışmanlık almayı tercih etmektedir. ISO 27001 ile ilgili olarak EKAP üzerinde de birçok hizmet alım ihalesi görülmektedir. (E-KAP, 2020)

Bu kapsamda komite standardın uygulanması için ana madde olarak ifade ettiğimiz (4-5-6-7-8-9-10) maddelerinin nasıl uygulanacağına dair ISO 27003 standardını yayınlamıştır.

Ana maddelerin nasıl uygulanması gerektiğini ifade eden standart ISO 27003 standardıdır.

8.2. ISO 27001 Standardının EK-A Maddelerinin Uygulanması (ISO 27002)

Bir çok kuruluş standardın EK-A bölümündeki kontrollerin nasıl uygulanacağına dair sorgulamaları vardır. Ancak EK-A bölümü ISO 27001 standardı içerisinden, kontrol amaçları ve kontroller olarak doğrudan ISO/IEC 27002 standardından çıkarılmış ve sıraya konulmuştur.

Bu sebeple bu kontrollerin nasıl uygulanacağına dair kılavuz ISO 27002 standardıdır.

8.3. ISO 27001 Standart 6.1 Planlama Maddesi (ISO 27005)

Risk ve fırsatları ele alan faaliyetler ve Bilgi güvenliği amaçları ve bu amaçları başarmak için planlamayı ifade etmektedir. Komitenin yayınlamış olduğu ISO 27005 standardı ise buna ilişkin riskleri nasıl ele alacağını bu standart içerisinde ifade etmektedir. Aynı zamanda ISO 31000 standardınında kullanılabileceği ilgili bölümde atıf yapılarak bahsedilmiştir.

ISO 27005 standardının özetinde;

Bu belge, bilgi güvenliği risk yönetimi için yönergeler sağlar.

Bu belge, ISO / IEC 27001'de belirtilen genel kavramları desteklemektedir ve bir risk yönetimi yaklaşımına dayalı bilgi güvenliğinin tatmin edici bir şekilde uygulanmasına yardımcı olmak için tasarlanmıştır.

ISO / IEC 27001 ve ISO / IEC 27002'de açıklanan kavramlar, modeller, süreçler ve terminolojiler hakkında bilgi sahibi olmak, bu belgenin tam olarak anlaşılması için önemlidir.

Bu belge, kuruluşun bilgi güvenliğini tehlikeye atabilecek riskleri yönetmeyi amaçlayan her türlü kuruluş (ör. Ticari kuruluşlar, devlet kurumları, kar amacı gütmeyen kuruluşlar) için geçerlidir. (ISO/IEC 27005, 2018)

8.4. ISO 27001 Standart 9.1 İzleme, Ölçme, Analiz Ve Değerlendirme (ISO 27004)

Standart içerisinde Kuruluş, bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelidir şeklinde ifade etmektedir.

Komitenin yayınlamış olduğu ISO 27004 standardı ise buna ilişkin İzleme, ölçme, analiz ve değerlendirme faaliyetlerinin nasıl ele alacağını bu standart içerisinde ifade etmektedir.

ISO 27004 standardının özetinde;

ISO / IEC 27004: 2016, kuruluşların ISO / IEC 27001: 2013, 9.1 gerekliliklerini yerine getirmek için bilgi güvenliği performansını ve bir bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelerine yardımcı olmayı amaçlayan yönergeler sunmaktadır. (ISO/IEC 27004, 2016)

a) Bilgi güvenliği performansının izlenmesi ve ölçülmesi;

b) Süreçleri ve kontrolleri de dahil olmak üzere bir bilgi güvenliği yönetim sisteminin (ISMS) etkinliğinin izlenmesi ve ölçülmesi;

c) İzleme ve ölçme sonuçlarının analizi ve değerlendirilmesi.

ISO / IEC 27004: 2016 her tür ve büyüklükteki kuruluş için geçerlidir.

8.5. ISO 27001 Standart 9.2 İç Tetkik (ISO 27007)

Bir standart gereği her yıl yapılması gerekli olan iç tetkiklerin nasıl yapılması gerektiğine dair kılavuz ISO 27007 standardıdır.

ISO 27009 standardının özetinde;

Bu belge, ISO 19011'de yer alan rehbere ek olarak, bir bilgi güvenliği yönetim sistemi (ISMS) denetim programının yönetilmesi, denetimlerin yapılması ve ISMS denetçilerinin yeterliliği hakkında rehberlik sağlar. (ISO/IEC 27007, 2020)

Bu belge, bir ISMS'nin iç veya dış denetimlerini anlamak veya yürütmek veya bir ISMS denetim programını yönetmek isteyenler için geçerlidir.

8.6. ISO 27001 Standart EK A.18.2 Bilgi Güvenliği Gözden Geçirmeleri (ISO 27008)

Standardın EK A.18 bölümünde bilgi güvenliği gözden geçirmeleri maddesinin alt maddelerinde Bilgi güvenliğinin bağımsız gözden geçirmesi, Güvenlik politikaları ve standartları ile uyum ve Teknik uyum gözden geçirmesi istenmektedir.

ISO 27008 standardının özetinde;

Bu belge Bilgi güvenliği kontrollerinin uygulanması ve işleyişinin gözden geçirilmesi ve değerlendirilmesi konusunda rehberlik sağlar, bilgi sistemi kontrollerinin teknik değerlendirmesini de içeren, kuruluşun oluşturduğu bilgi güvenliği gereksinimlerine dayalı değerlendirme kriterlerine karşı teknik uygunluğu da içeren kuruluşun oluşturduğu bilgi güvenliği gereksinimlerine uygun olarak. (ISO/IEC 27008, 2019)

Bu belge, ISO / IEC 27001 tarafından belirlenen bir Bilgi Güvenliği Yönetim Sistemi aracılığıyla yönetilen bilgi güvenliği kontrollerinin nasıl gözden geçirileceği ve değerlendirileceği konusunda rehberlik sunmaktadır.

Kamu ve özel şirketler, devlet kurumları ve bilgi güvenliği incelemeleri ve teknik uygunluk kontrolleri yapan kar amacı gütmeyen kuruluşlar da dahil olmak üzere her tür ve büyüklükteki kuruluş için geçerlidir.

8.7. Spesifik Sektörler İçin ISO 27009 Standardı (27009)

Standartlar Kamu ve özel şirketler, devlet kurum ve kuruuşlar ve bilgi güvenliği incelemeleri ve teknik uygunluk kontrolleri yapan kar amacı gütmeyen kuruluşlar da dahil olmak üzere her tür ve büyüklükteki kuruluş için geçerlidir.
Bu kapsamda ele alındığı takdirde oluşturulan standart genel çerçevesi olan bir standarttır. Bu nedenle de spesifik işler yapan kuruluşları tümüyle kapsayamamaktadır.

Komite bununla ilgili olarak sektör spesifik olarak yapılması gerekenleri ISO 27009 standardında ele almıştır.

ISO 27009 standardının özetinde;

Bu belge, ISO / IEC 27001'i genişleten ve belirli bir sektörü (etki alanı, uygulama alanı veya pazar) desteklemek için ISO / IEC 27002'yi tamamlayan veya değiştiren sektöre özgü standartlar oluşturma gereksinimlerini belirtir. (ISO/IEC 27009, 2020)

Bu belgede aşağıdakilerin nasıl yapılacağı açıklanmaktadır:

- ISO 27001 gerekliliklerine ilave gereklilikleri içerir,

- ISO gerekliliklerinden herhangi birini hassaslaştırmak veya yorumlamak,

- ISO / IEC 27001: 2013, Ek A ve ISO / IEC 27002'ninkilere ek olarak kontrolleri içerir,

- ISO / IEC 27001: 2013, Ek A ve ISO / IEC 27002 kontrollerinden herhangi birini değiştirmek,

- ISO / IEC 27002'ye kılavuzluk eklemek veya bu kılavuzda değişiklik yapmak.

Bu belge, ek veya rafine edilmiş gereksinimlerin ISO / IEC 27001'deki gereksinimleri geçersiz kılmadığını belirtir.

Bu belge, sektöre özgü standartlar üretmekle ilgilenenler için geçerlidir.

8.8. Kuruluşlar Ve Sektörler Arası Bilgi Güvenliği için ISO 27010 Standardı (27010)

Ülkemizde de sektörler arası veri alış verişi yani entegrasyonlar yapılmaktadır. E-Devlet uygulamaları özel ve kamu kuruluşlar arasında veri transferini sağlamaktadır. ISO 27010 standardı kuruluşlar ve sektörler arası bilgi güvenliğine kılavuzluk etmektedir.

Örneğin, sağlık sistemimizde doktor randevusu almak için kullandığımız uygulama ile bilgilerimizin girildiği sistem ve verilen e-reçetenin eczane tarafından görülerek işleme alınması dolayısıyla eczanenin devletten geri ödeme alması gibi karmaşık entegre sistemlerde bilgi güvenliğinin nasıl ele alınması gerektiğine kılavuzluk etmektedir.

ISO 27009 standardının özetinde;

ISO / IEC 27010: 2015, bilgi paylaşım topluluklarında bilgi güvenliği yönetimini uygulamak için ISO / IEC 27000 standartlar ailesinde verilen rehbere ek olarak kılavuz ilkeler sunmaktadır.

Bu Uluslararası Standart özellikle kuruluşlar arası ve sektörler arası iletişimde bilgi güvenliğinin başlatılması, uygulanması, sürdürülmesi ve iyileştirilmesi ile ilgili kontroller ve rehberlik sağlar. Yerleşik mesajlaşma ve diğer teknik yöntemler kullanılarak belirtilen gereksinimlerin nasıl karşılanabileceğine ilişkin yönergeler ve genel ilkeler sağlar.

Bu Uluslararası Standart, aynı endüstri veya pazar sektörü içinde veya sektörler arasında, hem kamu hem de özel, ulusal ve uluslararası hassas bilgilerin paylaşılması ve paylaşılması için geçerlidir. Özellikle, bir kuruluşun veya ulus devletin kritik altyapısının sağlanması, bakımı ve korunması ile ilgili bilgi alışverişi ve paylaşımına uygulanabilir. Hassas bilgi alışverişi ve paylaşımı sırasında güven yaratılmasını desteklemek, böylece bilgi paylaşım

topluluklarının uluslararası büyümesini teşvik etmek için tasarlanmıştır. (ISO/IEC 27010, 2015)

8.9. Telekominikasyon Kurumları için ISO 27002 (27011)

ISO 27009 dışında belirli özel sektörler için EK-A kontrollerini içeren ISO 27002 standardı oluştulabilmektedir. Telekominikasyon sektörünün tavsiyesi üzerine telekominikasyon sektörüne özel sistemler ve donanımlar kullanması nedeniyle ISO 27011 olarak ayrı bir standart olarak ele alınmaktadır.

ISO 27011 standardının özetinde;

Bu Tavsiye Kararının kapsamı ISO/IEC 27011: 2016, telekomünikasyon organizasyonlarında bilgi güvenliği kontrollerinin uygulanmasını destekleyen kılavuzlar tanımlamaktır.

Bu Tavsiye Kararının kabulü ISO/IEC 27011: 2016, telekomünikasyon kuruluşlarının gizlilik, bütünlük, kullanılabilirlik ve diğer ilgili güvenlik mülklerinin temel bilgi güvenliği yönetimi gereksinimlerini karşılamasına izin verecektir. (ISO/IEC 27011, 2011)

8.10. ISO 27001 ve ISO 20000 Standartlarının Entegre Uygulanması (27013)

ISO standartları Annex SL yapısı ile birlikte her standart ile aynı maddeleri ortak yönetmek amaçlı olarak oluşturulmuştur.

Bu kapsamda ISO 20000 Bilgi Teknolojileri Hizmet Yönetimi standardı ile ISO 27001 standardı benzer maddeleri tek çatı altında kullanılması hedeflenmektedir.

ISO 27013 standardının özetinde;

ISO / IEC 27013: 2015, aşağıdakilerden birini yapmak isteyen kuruluşlar için ISO / IEC 27001 ve ISO / IEC 20000-1'in entegre uygulaması hakkında rehberlik sağlar. (ISO/IEC 27013, 2015)

a) ISO / IEC 20000-1 önceden uygulandığında ISO / IEC 27001'i uygulayın, veya tam tersi,

b) ISO / IEC 27001 ve ISO / IEC 20000-1'in birlikte uygulanması veya

c) ISO / IEC 27001 ve ISO / IEC 20000-1'e dayalı mevcut yönetim sistemlerini entegre etmek.

ISO / IEC 27013: 2015 sadece ISO / IEC 27001'de belirtildiği gibi bir bilgi güvenliği yönetim sisteminin (ISMS) ve ISO / IEC 20000-1'de belirtildiği gibi bir hizmet yönetim sisteminin (ITSM) entegre uygulamasına odaklanmaktadır.

Uygulamada, ISO / IEC 27001 ve ISO / IEC 20000-1, ISO 9001 ve ISO 14001 gibi diğer yönetim sistemi standartlarına da entegre edilebilir.

8.11. Bilgi Güvenliği Yönetişimi (27014)

Bilgi Güvenliğinin yönetilmesi, izlemesi ve değerlendirilebilmesiyle ilgili olan ISO 27014 standardı tüm kurum ve kuruluşlara uygulanabilmektedir.

ISO 27014 standardının özetinde;

ISO / IEC 27014: 2013, kuruluşların kuruluş içindeki bilgi güvenliği ile ilgili faaliyetleri değerlendirebilmeleri, yönetebilmeleri, izleyebilmeleri ve iletebilmeleri için bilgi güvenliğinin yönetimi ile ilgili kavramlar ve ilkeler konusunda rehberlik sağlar. (ISO/IEC 27014, 2013)

ISO / IEC 27014: 2013 her tür ve büyüklükteki kuruluş için geçerlidir.

8.12. Organizasyonel Ekonomi (27016)

Bilgi Güvenliği sağlamak günümüzde ciddi maliyetler gerektirebilmektedir. Üst yönetimler bu maliyetlerin ne kadar gerekli olduğuna dair değerlendirme ve karar vermeyle ilgili olarak ekiplerine güvenmek durumunda kalmaktadır. ISO 27016 standardı üst yönetimlerin ekonomik kararlar almasında yardımcı olmaktadır.

ISO 27016 standardının özetinde;

ISO / IEC TR 27016: 2014, bir kuruluşun kaynakları korumak için rakip gereklilikler bağlamında bilgiyi korumak ve bu kararların ekonomik sonuçlarını anlamak için nasıl karar verebileceğine dair yönergeler sunar.

ISO / IEC TR 27016: 2014 her tür ve büyüklükteki kuruluş için geçerlidir ve bilgi güvenliği kararlarından sorumlu üst yönetim tarafından bilgi güvenliği yönetiminde ekonomik kararlar alınmasını sağlayacak bilgiler sağlar. (ISO/IEC 27016, 2014)

8.13. Bulut Hizmetler için ISO 27002 (27017)

Bulut (Cloud) teknolojisi ile birlikte bulut hizmet sağlayıcıları bilgi güvenliğini bulut gereklilikleri ile karşılayabilmeleri açısından oluşturulmuş standarddır.

ISO 27017 standardının özetinde;

ISO / IEC 27017: 2015, bulut hizmetlerinin sağlanması ve kullanımı için geçerli olan bilgi güvenliği denetimleri için aşağıdakileri sağlayarak yönergeler sağlar:

- ISO / IEC 27002'de belirtilen ilgili kontroller için ek uygulama kılavuzu;

- Özellikle bulut hizmetleriyle ilgili uygulama kılavuzlu ek kontroller.

Uluslararası Standart, hem bulut hizmeti sağlayıcıları hem de bulut hizmeti müşterileri için denetimler ve uygulama kılavuzu sağlar. (ISO/IEC 27017, 2015)

8.14. Kamuya Açık Bulut Hizmetlerinde, Kişi Bilgileri İşleyenler için Kişi Tanımlama Bilgisinin Korunması (27018)

Kişisel verilerin korunması tüm dünyada hükümetler tarafından koruma altına alınımaya çalışılıyor. Bunlarla ilgili olarak cezai yaptırımlar uygulanmaktadır. Ülkemizde de kişisel verilerin korunması kanunu ile koruma altına alınmaktadır.

Bulut teknolojisinde kişi bilgileri barındıran ve bunları işleyen kuruluşlar için bu bilgileri nasıl koruyacaklarına dair standarttır.

ISO 27018 standardının özetinde;

Bu belge, Genel Olarak Bulut Bilişim Ortamı için ISO / IEC 29100'deki gizlilik ilkeleri doğrultusunda Kişisel Olarak Tanımlanabilir Bilgileri (PII) korumak için önlemlerin uygulanması için yaygın olarak kabul edilen kontrol hedefleri, kontroller ve yönergeler oluşturur.

Özellikle, bu belge, genel bulut hizmetleri sağlayıcısının bilgi güvenliği risk ortamları kapsamında uygulanabilecek olan PII'nin korunmasına ilişkin düzenleyici gereklilikleri göz önünde bulundurarak ISO / IEC 27002'yi temel alan yönergeleri belirtir.

Bu belge, kamu ve özel şirketler, devlet kurumları ve kar amacı gütmeyen kuruluşlar da dahil olmak üzere, diğer kuruluşlarla sözleşme kapsamında bulut bilişim yoluyla PII işlemcileri olarak bilgi işleme hizmetleri sağlayan her türlü ve büyüklükteki kuruluş için geçerlidir. (ISO/IEC 27018, 2019)

Bu belgedeki yönergeler, PII denetleyicisi olarak görev yapan kuruluşlarla da ilgili olabilir. Ancak, PII kontrolörleri, PII işlemcileri için geçerli olmayan ek PII

koruma mevzuatına, düzenlemelerine ve yükümlülüklerine tabi olabilir. Bu belgenin bu tür ek yükümlülükleri kapsaması amaçlanmamıştır.

8.15. Enerji Hizmet Sektörü için Bilgi Güvenliği Kontrolleri (27019)

Standartlar her büyüklükteki kuruluşlar için tasarlandığından spesifik işler yapan kuruluşları tümüyle kapsayamamaktadır. ISO 27009 dışında belirli özel sektörler için EK-A kontrollerini içeren ISO 27002 standardı oluştulabilmektedir.

Enerji sektörünün tavsiyesi üzerine enerji sektörüne özel sistemler ve donanımlar kullanması nedeniyle ISO 27019 olarak ayrı bir standart olarak ele alınmaktadır.

Enerji üretim sistemlerinde kullanılan endüstriyel kontrol sistemleri (EKS) ve SCADA (Supervisory Control And Data Acquisition) sistemlerini baz almaktadır.

ISO 27019 standardının özetinde;

ISO / IEC 27019: 2017, enerji hizmeti endüstrisi tarafından elektrik enerjisi, gaz, petrol ve ısı üretimini veya üretimini, iletimini, depolanmasını ve dağıtımını kontrol etmek ve izlemek için kullanılan proses kontrol sistemlerine uygulanan ISO / IEC 27002: 2013'e göre rehberlik sağlar ve ilişkili destekleyici işlemlerin kontrolü içindir. (ISO/IEC 27019, 2017)

- Merkezi ve dağıtılmış proses kontrol, izleme ve otomasyon teknolojisi ile bunların çalışması için kullanılan programlama ve parametre belirleme cihazları gibi bilgi sistemleri;

- Dijital sensör ve aktüatör elemanları dahil olmak üzere kontrol ve saha cihazları veya Programlanabilir Mantık Kontrolörleri (PLC'ler) gibi dijital kontrolörler ve otomasyon bileşenleri;

- Proses kontrol alanında kullanılan diğer tüm destekleyici bilgi sistemleri, ör. ek veri görselleştirme görevleri ve kontrol, izleme, veri arşivleme, tarih kaydı, raporlama ve dokümantasyon amaçları için;

- Proses kontrol alanında kullanılan iletişim teknolojisi, ör. ağlar, telemetri, telekontrol uygulamaları ve uzaktan kontrol teknolojisi;

- Gelişmiş Ölçüm Altyapısı (AMI) bileşenleri, ör. Akıllı sayaçlar;

- Ölçüm cihazları, ör. emisyon değerleri için;

- Dijital koruma ve güvenlik sistemleri, ör. koruma röleleri, emniyet PLC'leri, acil durum vali mekanizmaları;

- Enerji yönetim sistemleri, ör. Özel hanelerde, konutlarda veya endüstriyel müşteri tesislerinde Dağıtılmış Enerji Kaynakları (DER), elektrikli şarj altyapılarının;

- Akıllı şebeke ortamlarının dağıtılmış bileşenleri, ör. enerji şebekelerinde, özel evlerde, konutlarda veya endüstriyel müşteri tesislerinde;

- Yukarıda belirtilen sistemlere yüklenen tüm yazılım, bellenim ve uygulamalar, ör. DMS (Dağıtım Yönetim Sistemi) uygulamaları veya OMS (Kesinti Yönetim Sistemi);

- Yukarıda belirtilen ekipman ve sistemleri barındıran tesisler;

- Yukarıda belirtilen sistemler için uzaktan bakım sistemleri.

ISO / IEC 27019: 2017 nükleer tesislerin proses kontrol alanı için geçerli değildir. Bu alan adı IEC 62645 kapsamındadır.

ISO / IEC 27019: 2017 ayrıca ISO / IEC 27001: 2013'te açıklanan risk değerlendirme ve tedavi süreçlerini bu belgede sağlanan enerji hizmeti sektörüne özel rehberliğe uyarlama gereksinimini de içerir.

8.16. Bilgi Güvenliği Yönetim Sistemi Profesyönelleri İçin Yeterlilik (27021)

Yönetim sistemlerinin çoğunda 7.2 Yeterlilik maddesi bulunmaktadır. Bilgi güvenliği yönetim sistemi profesyönellerinin yeterlilikleriyle ilgili olarak nelerin gerektiğine dair kılavuz bilgileri içerir.

ISO 27021 standardının özetinde;

ISO / IEC 27021: 2017, ISO / IEC 27001'e uygun bir veya daha fazla bilgi güvenliği yönetim sistemi sürecinin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesine katılan ya da iştirak eden ISMS uzmanları için yeterlilik gereksinimlerini belirtir. (ISO/IEC 27021, 2017)

8.17. Bilgi Ve İletişim Teknolojilerinin İş Sürekliliği (27031)

İş sürekliliği yaşanan COVID-19 pandemi döneminde de önemini bir kez daha gözler önüne serdi. ISO 27001 standardının EK A.17 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları olarak ele almaktadır. 27031 standardı ise kılavuz bilgiler içermektedir.

ISO 27031 standardının özetinde;

ISO / IEC 27031: 2011, iş sürekliliği için bilgi ve iletişim teknolojisine (BİT) hazır olma kavramlarını ve ilkelerini açıklar ve iş sürekliliğini sağlamak için bir kuruluşun BİT hazırlığını geliştirmek. Bu, iş sürekliliği programı (IRBC) için BİT hazırlığını geliştiren ve BİT hizmetlerinin / altyapılarının ortaya çıkması durumunda ticari operasyonları desteklemeye hazır olmasını gerektiren herhangi bir kuruluş (özel, resmi ve hükümet dışı, büyüklükten bağımsız) için

geçerlidir kritik iş işlevlerinin sürekliliğini (güvenlik dahil) etkileyebilecek olaylar, olaylar ve bunlarla ilgili aksaklıklar. Ayrıca bir kuruluşun IRBC'si ile ilişkili performans parametrelerini tutarlı ve tanınmış bir şekilde ölçmesini sağlar. (ISO/IEC 27031, 2011)

ISO / IEC 27031: 2011 kapsamı, ICT altyapısı ve sistemleri üzerinde etkisi olabilecek tüm olayları ve (güvenlikle ilgili olanlar) olayları kapsar. Bilgi güvenliği olay yönetimi ve yönetimi ile ICT hazır bulunuşluk planlaması ve hizmetleri uygulamalarını içerir ve genişletir.

8.18. Tedarikçi Yönetiminde Bilgi Güvenliği (27036)

ISO 27001 standardı içerisinde ve neredeyse her yönetim sisteminde tedarikçi yönetimiyle ilgili olarak belirli kontroller bulunmaktadır. ISO 27001 standardı A.15 maddesi de tedarikçi ilişkileri ile ilgili kılavuz bilgiler sağlamaktadır. Ayrıca 27036-1, 27036-2 olarak devam eden bir seri halindedir.

ISO 27036-1 standardının özetinde;

ISO / IEC 27036-1: 2014, ISO / IEC 27036'nın tanıtıcı bir parçasıdır. Kuruluşlara bilgi ve bilgi sistemlerini tedarikçi ilişkileri bağlamında güvence altına almada yardımcı olmaya yönelik rehberliğe genel bir bakış sağlar. Ayrıca, ISO / IEC 27036'nın diğer bölümlerinde ayrıntılı olarak açıklanan kavramları da tanıtmaktadır. ISO / IEC 27036-1: 2014, hem edinenlerin hem de tedarikçilerin bakış açılarını ele almaktadır. (ISO/IEC 27036, 2014)

ISO 27036-2 standardının özetinde;

ISO / IEC 27036-2: 2014, tedarikçi ve edinen ilişkilerinin tanımlanması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve geliştirilmesi için temel bilgi güvenliği gereksinimlerini belirtir.

Bu gereksinimler, imalat veya montaj, iş süreci tedariki, yazılım ve donanım bileşenleri, bilgi süreci tedariki, Yap-İşlet-Devret ve bulut bilişim hizmetleri gibi ürün ve hizmetlerin tedariki ve tedarikini kapsar.

Bu gereksinimlerin türü, boyutu ve niteliğine bakılmaksızın tüm kuruluşlar için geçerli olması amaçlanmıştır.
Bu gereklilikleri karşılamak için, bir kuruluş halihazırda dahili olarak bir dizi temel süreç uygulamış olmalı veya aktif olarak yapmayı planlamalıdır. Bu süreçler aşağıdakileri içerir, ancak bunlarla sınırlı değildir: yönetişim, iş yönetimi, risk yönetimi, operasyonel ve insan kaynakları yönetimi ve bilgi güvenliği.

ISO 27036-3 standardının özetinde;

ISO / IEC 27036-3: 2013, bilgi ve iletişim teknolojisi (BİT) tedarik zincirindeki ürün ve hizmet alıcılarına ve tedarikçilere aşağıdaki konularda rehberlik sağlar:

Fiziksel olarak dağınık ve çok katmanlı BİT tedarik zincirlerinin neden olduğu bilgi güvenliği risklerinin görünürlüğü ve yönetimi;

Küresel BİT tedarik zincirinden bu ürün ve hizmetleri kullanan kuruluşlar üzerinde bilgi güvenliği etkisi olabilecek BİT ürün ve hizmetlerine yönelik risklere yanıt vermek. Bu riskler, kurumsal ve teknik yönlerle ilişkili olabilir (örneğin, kötü amaçlı kodun takılması veya sahte bilgi teknolojisi (IT) ürünlerinin varlığı);

Bilgi güvenliği süreçlerini ve uygulamalarını ISO / IEC 15288 ve ISO / IEC 12207'de açıklanan sistem ve yazılım yaşam döngüsü süreçlerine entegre ederken, ISO / IEC 27002'de açıklanan bilgi güvenliği kontrollerini destekler.

ISO / IEC 27036-3: 2013, ICT tedarik zinciriyle ilgili iş sürekliliği yönetimi / esneklik konularını içermez. ISO / IEC 27031, iş sürekliliğini giderir.

ISO 27036-4 standardının özetinde;

ISO / IEC 27036-4: 2016, bulut hizmeti müşterilerine ve bulut hizmeti sağlayıcılarına aşağıdaki konularda rehberlik sağlar:

a) Bulut hizmetlerinin kullanımıyla ilişkili bilgi güvenliği riskleri hakkında görünürlük kazanmak ve bu riskleri etkin bir şekilde yönetmek ve

b) Bu hizmetleri kullanan kuruluşlar üzerinde bilgi güvenliği etkisi olabilecek bulut hizmetlerinin edinilmesi veya sağlanmasına özgü risklere yanıt vermek.

ISO / IEC 27036-4: 2016, bulut hizmetiyle ilgili iş sürekliliği yönetimi / esneklik sorunlarını içermez. ISO / IEC 27031, iş sürekliliğini giderir.

ISO / IEC 27036-4: 2016, bir bulut hizmet sağlayıcısının bilgi güvenliğini nasıl uygulaması, yönetmesi ve işletmesi konusunda rehberlik sağlamamaktadır. Bunlar hakkında rehberlik ISO / IEC 27002 ve ISO / IEC 27017'de bulunabilir.

ISO / IEC 27036-4: 2016'nın kapsamı, bulut hizmetlerinin kullanımı için bilgi güvenliği yönetiminin uygulanmasını destekleyen yönergeler tanımlamaktır.

8.19. ISO 27001 ve ISO 27002 Genişletilerek Mahremiyet Bilgisi Yönetimi (27701)

Kişisel verilerin korunmasıyla ilgili olarak yayınlanan kanunla birlikte ülkemizde de kişisel verilerin korunması yasalarla zorunlu hale gelmiştir. Avrupa birliğinde GDPR, Kaliforniya'da CCPA gibi tüm dünyada kişisel bilgilerin korunması için kanunlar yürürlüğe girmektedir. Bilgi güvenliği belgelendirmesinin genişletilmesi de bu kapsamda ISO 27701 ile kişisel verilerin diğer bir deyişle mahremiyet bilgisinin korunması için ciddi anlamda katkı sağlamaktadır.

ISO 27701 standardının özetinde;

Bu belge, kuruluş kapsamında gizlilik yönetimi için ISO / IEC 27001 ve ISO / IEC 27002'nin bir uzantısı şeklinde bir Gizlilik Bilgi Yönetim Sistemi (PIMS) oluşturulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için gereklilikleri belirtir ve kılavuzluk sağlar. (ISO/IEC 27701, 2019)

Bu belge, PIMS ile ilgili gereksinimleri belirtir ve PII işlemcileri için sorumluluk ve hesap verebilirliğe sahip PII kontrolörleri ve PII işlemcileri için rehberlik sağlar.

Bu belge, kamu ve özel şirketler, devlet kurumları ve kar amacı gütmeyen kuruluşlar da dahil olmak üzere, bir ISMS içinde PII'yi işleyen PII kontrolörleri ve / veya PII işlemcileri de dahil olmak üzere her tür ve büyüklükteki kuruluş için geçerlidir.

8.20. Güvenlik Açığı Yönetim Süreçleri (30111)

Güvenlik açıklıkları her donanım, yazılım ve süreçte bulunabilmesi muhtemel konulardan biridir. Siber güvenliğin kalbinde de güvenlik açıklıklarının yönetimi bulunmaktadır. Komite bu konuda ISO 30111 standardını yayınlamıştır.

ISO 30111 standardının özetinde;

Bu belge, bir ürün veya hizmetteki bildirilen olası güvenlik açıklarının nasıl işleneceği ve düzeltilebileceği ile ilgili gereksinimleri ve önerileri sağlar.
(ISO/IEC 30111, 2019)

Bu belge, güvenlik açıklarını ele alan üreticiler için geçerlidir.

9. TARTIŞMA VE DEĞERLENDİRMELER

Komitenin yayınlamış olduğu ve Dünyada en popüler sertifikalar içerisinde sayılan ISO 27001 sertifikası aslında Siber Güvenlik için temel oluşturmaktadır. Siber güvenlik sadece tek bir yönetim sistemi ile yönetilmesi maalesef mümkün olmayacaktır.

Bilgi Güvenliği Yönetim Sistemi ile birlikte yayınlanan diğer standart kılavuzlar etkin bir şekilde uygunlanması gerekmektedir. Günümüzde her ne kadar siber güvenlik Bilgi ve İletişim Teknolojileri departmanlarının sorumluluğunda gibi görünse de ya da sorumluluk bu departmanlara verilse de siber güvenlik uçtan uca yani tüm şirketin birlikte hareket etmesiyle mümkün olacaktır. Bunu sağlamanın yöntemi ise farkındalık eğitimleri verilerek gerçekleştirilmesidir.

Farkındalık eğitimleri her yönetim sistemi içerisinde bulunmaktadır. Her yıl bir kez tüm ilgili çalışanlara ve tedarikçilere farkındalık eğitimlerinin verilmesi gerekmektedir. Şirketler genellikle tek bir farkındalık eğitimi hazırlayarak her yıl aynı eğitimi vermektedir. Hatta birçok kuruluş internetten elde ettiği farkındalık eğitimlerinden derlemeler yaparak oluşturmaktadır.

Farkındalık eğitimleri şirkete özel hazırlanması gerekir. Şirkete özel hazırlanmasının sebebi ise şirketin kendi prosedür, politika ve talimatlarını anlatmaları ve doğru şekilde uygulanıp uygulanmadığını ölçmeleri için önemlidir.

Farkındalık eğitimlerinin doğru hazırlanarak verilmesi siber güvenlik için en temel konu olarak ele alınmalıdır. Siber güvenlikle ilgili olarak temel bilgileri içeren kılavuz olan ISO 27032 Siber Güvenlik Kılavuzu da ciddi anlamda katkı sağlayacaktır.

Temel bilgi ve farkındalık sağlandıktan sonra ise yapılması gereken en önemli konu komitenin yayınladığı en popüler standart olan ISO 27001 doğru şekilde planlanması, uygulanması ve iyileştirilmesidir.

ISO 27001 standardının doğru şekilde planlanması, uygulanması ve iyileştirilmesi de komitenin yayınlamış olduğu diğer standarların kullanılması ve teknik olarak irdelenmesi ile mümkün olacaktır.

ISO 27001 standardının maddeleri ve diğer standartların bu maddeler de nelerin yapılabileceğini ise ana maddeler ve EK-A olarak ele alınabilir.

9.1. ISO 27001 Standardının Ana Maddeleri ve Komitenin Diğer Standartlarının Uygulanması

Ana maddeler içerisinde bulunan 4. madde kuruluşu tanıtacak, ilgili tarafları , iç dış hususları ve kapsamı ifade edeceği için aslında bilgi güvenliğinin temelini ve sınırlarını belirleyecektir.

5. Madde olan liderlikte ise üst yönetim siber güvenlik ve bilgi güvenliğine bakışını ve desteğini içermesi gerekmektedir. Ayrılan bütçelerden, güvenlik hedeflerine kadar birçok konuyu üst yönetimin sorumluluğunda olması gerekmektedir. Bu sebeple ISO 27016 standardının kurum kültür ve yapısına uygun şekilde ele alınması ve uygulanması katkı sağlayacaktır.

6. Madde olan planlama da ise risk ve fırsatlar ele alınmaktadır. Risk ve fırsatların ele alınabilmesi için öncelikle 4. Maddede ilgili taraflar gibi konuların ve sonra EK A.8 maddesindeki varlık envanterinin oluşturulması gerekmektedir.

Varlık Envanteri ve ilgili taraflar gibi konular oluşturulduktan sonra risk envanteri oluşturularak eşleştirilmeleri gerekmektedir. Burada da ISO 31000 Kurumsal Risk Yönetimi kullanılabilecektir.

Ardından bilgi güvenliği ile ilgili olarak risk analizi için ISO 27005 standardı kullanılabilecektir. Eğer kuruluş içerisinde risk departmanı bulunuyor ve entegre biz özet risk raporu hazırlanması gerekli ise bunun hazırlanması için gerekli olarak risk hesaplama yöntemlerinin anlatıldığı ISO 31010 standardı kullanılabilecektir.

7. Madde olan destek maddesinde ise kaynaklar, yeterlilik ve farkındalık konuları ele alınmaktadır. Kaynak üst yönetimin 5. madde liderlikten temeli hazırlanmış olacaktır. Yeterlilik konusunda ise ISO 27021 standardı ile sağlabilecektir. Farkındalık konusu zaten kurumun kendi siber güvenlik ve bilgi güvenliği yöntemleri ile ele alınması gereklidir.

8. Madde olan işletim de ise 6. Maddede oluşturulan ve değerlendirilen risklerin düşürülmesi, kaçınılması ve kabul edilmesi gibi risk yönetim süreçlerini içermesi sebebiyle kuruluş büyüklüğü ile doğru orantılı tüm paydaşlarla gerçekleştirilmesi gerekmektedir. Eğer kuruluş diğer kuruluşlar ve sektörlerle entegre çalışmalar içerisinde ise ISO 27010 standardı kullanılabilecektir.

9. Madde olan performans değerlendirmede ise izleme, ölçme, analiz ve değerlendirme, iç tetkik ve yönetim gözden geçirme konuları ele alınmaktadır. İzleme, ölçme, analiz ve değerlendirme için ISO 27004 standardı, iç tetkik için 27007 standardı kullanılabilecektir.

10. Madde olan İyileştirme ise iç denetim ve dış denetimlerden ya da ihlal olaylarından elde edilen uygunsuzluk, düzeltici faaliyetleri ve sürekli iyileştirmeyi ele almaktadır.

9.2. ISO 27001 Standardının EK-A Kontrolleri ve Komitenin Diğer Standartlarının Uygulanması

A.5 Maddesi Bilgi güvenliği politikalarını ele almaktadır. Bilgi güvenliği için oluşturulan tüm politikaların (Uzaktan Çalışma Politikası, Temiz masa Temiz Ekran Politikası vd.) listelenmesi ve gözden geçirme sıklığını ele almaktadır.

A.6 Maddesi bilgi güvenliği organizasyonunu ele almakta ve ilgili takip edilen otorite, özel ilgili gruplarının tanımlanmasını istemektedir. Son olarak ise proje yönetimi içerisinde bilgi güvenliğinin ele alınmasını istemektedir. Burada proje yönetiminde proje türüne bakılmaksızın ele alınması gereklidir. Örnek olarak tesis içerisine ya da dışarısına otopark yapılacaksa eğer bilgi güvenliği

rollerindeki kişiler bu proje içerisinde olması gerekmektedir. Çünkü otopark giriş çıkışı, kamera sistemleri, araç altı sistemleri gibi bir çok sistem kullanılacağından ya da bir diğer proje olarak yeni bir satış kampanyasıyla ilgili çalışma yapılacaksa yazılımlardan alınacak veriler kampanya ile ilgili geliştirilecek uygulama gibi bir çok şey değişebileceğinden envanterin güncellenmesi, risklerinin ele alınması ve diğer bir çok konu olması sebebiyle proje türünün ne olduğuna bakılmaksızın bilgi güvenliği rollerine sahip kişiler projeye dahil olmaları gerekmektedir.

A.7 Maddesi insan kaynakları güvenliğini ele almaktadır. İşe girişten iş akdinin sonlanması ya da görev değişikliğine ve yönetim sorumluluklarına kadar bir çok konuyu ele almaktadır. Burada kritik olan konulardan biri ise disiplin prosesidir. Bilgi güvenliği ya da siber güvenlik ihlal olayına karışan çalışanlar için bir süreç tanımlanması gerekmektedir.

A.8 Maddesi varlık yönetimini ele almaktadır. Risk analizinde önemli rol oynayan varlıkların envanterinin oluşturulması, bilgi sınıflandırması ve ortam işleme konularını ele almaktadır.

A.9 Maddesi erişim kontrollerini ele almaktadır. Erişim kontorollerini iş gerekliliklerine göre belirlemek, kullanıcı erişim ve sorumlulukları, sistem ve uygulamalara erişim konularını ele almaktadır.

Kullanıcı erişimi ve kontrolü siber güvenlikte en önemli konulardan biridir. Günümüzde birçok siber saldırı kullanıcı hesaplarının ele geçirilmesine yönelik olarak yapılmaktadır. Hatta kullanıcı haklarının yükseltilmesi yöntemi (Privilege Escalation) en çok kullanılan yöntemlerden biridir. Tüm bu sebeplerden ötürü kullanıcıların sistemlere kontrollü ve güvenilir şekilde erişmelere çok önemlidir.

Kullanıcıların kontrollü ve güvenlilir erişimi için çoklu oturum açma yöntemleri artık vazgeçilmez bir hal almaktadır. Microsoft, Google gibi birçok şirket ve

verdikleri bulut hizmetlerde artık tek kullanımlık şifre yöntemi ücretsiz olarak kullandırılan servislerde de mevcuttur.

Tek kullanımlık şifre üretiminin daha güvenli hale getirilmesi ve kişiselleştirilmesi gittikçe önem kazanmaktadır. Bunun neden eğer tek kullanımlık şifre üretim sistemi bir şekilde ele geçirilirse tüm kullanıcıların erişimleri kullanılabilecektir. Bu nedenle üretilen tek kullanımlık şifreler kişiselleştirilmesi gerekmektedir.

Dijital hesapların güvenliği artık vazgeçilmez bir hal almaktadır. Bu hesaplara erişim güvenliği ise bir çok farklı yöntem ile sağlanmaya çalışılıyor. Dünya da uluslararası standartlar ile dijital hesapların güvenliği bir temele oturtulmaya çalışılırken çoklu doğrulama yöntemleri ve tek kullanımlı şifreler vaz geçilmez hale geliyor.

Tek kullanımlık şifreler ise zaman bazlı, lokasyon bazlı ve farklı algoritmalar ile üretilebiliyor. Çalışmamızda kullanılan tüm çözümlerin kolaylıkla suiistimal edilebileceği ve tahmin edilebileceğini değerlendirdik. Kişiselleştirilmiş tek kullanımlık şifrenin üretilebilemesi için kişinin mobil cihaz bilgileri kullanılarak IMEI ve SIM kart seri numarası AES ve TOTP algoritmalarından geçirilerek üretilen OTP şifreleri ile dijital hesaplar çok daha güvenli hale getirilmektedir.

A.10 maddesi kriptolojiyi ele almaktadır. Kriptoloji konusu çok fazla anlaşılamadığından etkin bir yönetim sağlanamamaktadır. Microsoft firmasının bitlocker uygulaması, kablosuz ağların güvenliği için WPA kullanılması yada internet siteleri için kullanılan SSL sertifikası gibi tüm yapılan işlemler kriptoloji olarak ele alınması gerekmektedir.

Ayrıca eğer kurum kendi yazılımları ve uygulamarını geliştiriyorsa burada kriptoloji kullanmak istiyorsa ISO 19772 standardı ile oturum açma şifrelemesi, ISO 20009 gibi bir çok standardı kullanabilecektir.

A.11 maddesi fiziksel ve çevresel güvenlik konularını ele almaktadır. Bunlar güvenli alanlar ve teçhizatların fiziksel güvenliği olarak ele alınmaktadır. Siber güvenlik için önemli konulardan biri tesislere yetkisiz fiziksel erişimin sağlanmaması ve güvenli alanlara kontrollü şekilde erişimin sağlanmasıdır. ISO 30104 standardı bu konularda fiziksel güvenliği arttırmada katkı sağlayacaktır.

A.12 maddesi işletim güvenliğini ele almaktadır. İşletim güvenliği; işletim prosedürleri ve sorumlulukları, kötücül yazılımlardan koruma, yedekleme, kaydetme ve izleme, işletimsel yazılım kontrolü, teknik açıklık yönetimi ve bilgi sistemleri tetkik hususlarını ele almaktadır.

İşletim prosedür ve sorumlulukları işletilen her sistem için hazırlanması gerekmektedir. Sunucular dışında işletilen her sistem için gereklidir. Turnike ve kapı sistemleri, enerji yönetim sistemleri gibi bilgi teknolojileri tarafından yönetilmemesine karşın siber güvenlik ve bilgi güvenliği ile ilgili tüm işletilen sistemleri kapsamaktadır.

Kötücül yazılımlardan koruma sadece anti-virüs gibi değerlendirilmemesi gerekmektedir. Malware, Adware, spyware ve diğer kötücül tüm yazılımlar dikkate alınmalıdır. Siber güvenliğin temelini de bu tarz yazılımlardan korunmak oluşturmaktadır.

Yedekleme işletilen tüm sistemler için öncelikli sistemler dahilinde alınması gerekmektedir. Yedeklilik aynı zamanda iş sürekliliğine de katkı sağlayacağından ISO 27031 kılavuz olarak kullanılabilir.

Kaydetme ve izleme günümüzde log yönetimi olarak ele alınmakta olup Security Information and Event Management (SIEM) olarak siber güvenliğe ciddi anlamda katkı sağlamaktadır.

İşletimsel yazılım kontrolü işletilen tüm sistemler sunucu ve bilgisayarlardaki yazılımların kontrollü bir şekilde kullanılmasını sağlamayı amaçlamaktadır. Her

yazılımda güvenlik açığı olabileceğinden yazılımları sınırlandırmak siber güvenliğe katkı sağlayacaktır.

Teknik açıklıkların yöntemi yazılımlar üzerindeki açıklıkların güncellenerek kapatılmasını hedeflemekte olup, aynı zamanda kullanıcıların bilgisayarlara yazılım yüklemelerinin önüne geçmesini istemektedir. Bu kontrol siber güvenliğin temellerindendir.

Bilgi sistemlerinin tetkik kontrollerinde güvenlik işlemlerinin doğrulanmasını amaçlamaktadır ve burada ISO 27008 standardı kılavuz olarak kullanılabilecektir.

A.13 maddesi haberleşme güvenliğini ele almaktadır. Haberleşme sağlanabilmesi için ağa (network) bağı olmak gerekmektedir. Komite ağ güvenliği ile ilgili olarak birçok standart kılavuz yayınlamaktadır. ISO 27033 standardı 6 bölümden oluşmaktadır. Siber dünyaya açıldığımız güvenlik duvarları ile ilgili olarak ise ISO 27039 standardını kullanmak temel siber güvenliğe en büyük katkılardan birini sağlayacaktır.

A.14 maddesi sistem temini, geliştirme ve bakımını ele almaktadır. Genellikle yazılım geliştirme olarak değerlendirilse de bütüne baktığımız takdirde sistemler, ağ ve yazılımlar açısından değerlendirmek gerekmektedir. Sistemlerin, ağ ve yazılımların güvenliklerinden, geliştirilmesine, testlerinden ve test verisi oluşturup korumaya kadar geniş bir konuyu ele almaktadır.

Komite bununla ilgili olarak birçok standart yayınlamaktadır. ISO 27034 serisi, ISO 15945 ve ISO TS 19249 gibi standartlar ciddi anlamda katkı sağlayacaktır.

Ancak tüm bunların dışında işletimsek sistemlerle ilgili olarak siber güvenlik için en önemli alan olan açıklıkların ve sıfırıncı gün açıklıkları gibi konuların değerlendirileceği ISO 30111 standardı önemli bir rehber olacaktır.

A.15 maddesi tedarikçi ilişkilerini ele almaktadır. Kurumlar genellikle tedarikçi ilişilerinde ISO 9001 yönetim sistemindeki bilgileri kullanmaya çalışsa da standardın gerekliliğini karşılamamaktadır. Standart tedarikçi ilişkilerinde güvenliğin ele alınmasını beklemektedir.

Tedarikçi ilişkileri siber güvenlikle ilgili olarak tedarik edilecek her hangi bir ürün için büyük önem taşımaktadır. Bu sebeple komite ISO 27036 serisi ile 4 bölüm olarak ele almaktadır.

A.16 Maddesi bilgi güvenliği ihlal olayları yönetimini ele almaktadır. Bir bilgi güvenliği ihlali dolaylı olarak siber güvenlik ihlali olarak ele alınması gerekmektedir. Bu nedenle de buna sebep olan bir çalışansa A.7 insan kaynakları güvenliğinde bulunan disiplin prosesi önem kazanıyor. Eğer ihlal hukuki bir süreç gerektirecekse delil toplama gibi birçok süreci de değerlendirmmek standart içerisinde bir gerekliliktir. Standart sonra olarak ise bu ihlallerin tekrar edilmemesi için ihalden öğrenilmiş olan derslerin neler olduğunun ele alınmasını beklemektedir. Öğrenilen dersler daha sonrasında farkındalık eğitimlerine ciddi anlamda fayda sağlayacaktır.

Komite ihlal olaylarıyla ilgili olarak ISO 27035 standardı bölüm 1 ve bölüm 2 olarak iki ayrı kılavuzla ele almaktadır.

A.17 Maddesi iş sürekliliği yönetiminin bilgi güvenliği hususlarını ele almaktadır. Burada iş sürekliliğini değil, bilgi güvenliği yani siber güvenlik ile ilgili olarak bilgi güvenliğinin sürekliliğini ele almaktadır.

İş sürekliliği ISO içerisinde 22301 İş Sürekliliği Yönetim Sistemi standardı ile yönetilmektedir. Bu nedenle bilgi güvenliğine ISO 27031 standardının rehber olarak alınması gerekmektedir.

A.18 Maddesi uyumu ele almaktadır. Uyum bir şirketin kendi politika, prosedür ve talimat gibi tüm kurallarına, kanun ve sözleşmeye tabi gereksinimlere olan uyumu ele almaktadır.

İçerisinde fikri mülkiyet hakları, kişi tespit bilgisinin korunması, kriptografik kontroller ve kayıtların korunması gibi hukuki ve şirket uyum konularını ele almaktadır.

Kriptografik kontroller yasalarla kriptografik olarak uygulanması gerekli olan konuları kapsamaktadır. Dijital imza kullanımı, kayıtların (log) imzalanması, askeri kriptolojik ürünler vd. gibi bir çok konuyu kapsamaktadır.

10. SONUÇ VE ÖNERİLER

Siber güvenlik gelişmiş sürekli tehdit (APT) alanlarına maruz kalmaktadır. Bunun yanı sıra yeni olası tehdit ve sıfıncı gün tehditlerinin ele alınması gerekmektedir. Tüm bunlar siber güvenliğin temel taşları olmaktadır.

Siber güvenliğin sağlanabilmesi için kullanılan platformlar ve araçlar, ağ bağlantıları, kullanıcıların farkındalıklarının arttırılması, yeni güncelleştirilmelerin takip edilmesi gerekmektedir.

Bunların yanı sıra bilgilerin gizlilik, bütünlük, erişebilirlik ve inkar edilememezliğinin sağlanması da siber güvenliğin temel yapı taşlarıdır.

Komitenin yayınlamış olduğu bilgi güvenliği yönetim sistemi bu temel siber güvenlik yapı taşlarının tamamını kapsamaktadır. Bu nedenle de dünyada önemli bir yere sahip olmaktadır.

Komitenin siber güvenlik kılavuzuyla birlikte etkin bir yönetim sistemi kurmak, Siber güvenliğin birçok alanındaki güvenlik önlemlerini almanızı ve etkin bir siber güvenlik yönetimine katkı sağlayacaktır.

Etkin bir yönetim sistemini kurmanın ilk aşaması yetkinlik profesyoneller ve danışmanlarla çalışmaktan geçmektedir. Ancak bu profesyonellerin ve danışmanların yetkinlik değerlendirmesini yapmak etkin bir sistem kurmanın başlangıcıdır. Bu nedenle komitenin yayınlamış olduğu ilgili standartları kullanmak katkı sağlayacaktır.

Dökümantasyon ne kadar önemli ise teknik olarak siber güvenlik kavramlarına ve kullanılan teknolojilere hakim olmakta bir o kadar önemlidir. Oluşturulacak olan bilgi güvenliği yönetim sisteminin kapsamı ile siber güvenlik kapsamanın bir birini kapsaması ise riskleri minimize edebilmek için çok önemlidir. Bu nedenle doğru bir envanter çıkarmak ve bu envanterlerle ilgili etkin bir risk analizi yapmak çok önemlidir.

Risk analizinde ise kurumun büyüklüğüyle doğru orantılı standartlar ve yöntemler kullanılması gerekmektedir. Risk yönetim sonuçlarına göre strateji ve yatırımlar yapılacağından bir diğer hayati konu olarak risk analizini ele alabiliriz.

Risk analizinde varlıkların gizlilik, bütünlük ve erişebilirlikle değerlendirilmesi ve artık bunlara ek olarak inkar edilememezlik ihtiyacını da ele almak ciddi faydalar sağlayacaktır. Nitekim her bir varlığını etkilenebileceği gizlilik, bütünlük, erişebilirlik ve inkar edilememezlik önem derecesi farklılık gösterebilcektir. Örneğin UPS (Kesintisiz Güç Kaynağı) bütünlük derecesi ve gizlilik derecesi, erişebilirlik derecesinden çok daha düşük olacaktır. Eğer UPS'e erişim olmaz ise elektrik kesintisi gerçekleşeceğinden tüm sistemlerin erişilebilirliği etkilenecektir. Her bir varlığın değerlendirilmesinde olası tüm problemlerin değerlendirilmesi ve etkisinin ele alınması fayda sağlayacaktır.

Risklerin gerçekleşmesi durumunda olası etkilerin değerlendirmesi de çok önemlidir. Örneğin bir deprem riskini ele alan kurum rakipleri ve müşterileri aynı bölgede bulunuyorsa bu riski düşük risk olarak değerlendirebilir. Çünkü bölgede bir depremin olması ve zarar vermesi aynı bölgedeki tüm rakipleri ve müşterileri etkileyebilecektir. Gerçekçi bir risk analizi ve etki analizi yapılması siber güvenlik için nerelere yatırım yapılması ve güçlendirilmesi gerektiğiyle ilgili fikir verecektir.

Kullanılan bilişim sistemlerinin ve geliştirilen tüm yazılım ve uygulamaların siber güvenlik gereksinimmleri ve temel bilgi güvenliği ihtiyaçlarının yerine getirildiğinden emin olunması gerekmektedir. Bunu en kolay yöntemi ise tüm dünyanın uygulamış olduğu standartlar ile gerçekleştirilebilir. Bu nedenle komitenin yayınlamış olduğu standartlar temel konuları sağlamakta olup, kullanılan siber güvenlik ürünlerinin beyaz sayfaları, kılavuzları ve güncelleştirmelerini çok sıkı bir şekilde takip etmeleri gerekmektedir.

Geliştirilen yazılım ve uygulamaları içinde komitenin standartlarınnı dışında ilgili yazılım platformları ve veri tabanı platformarının beyaz sayfaları

kılavuzlarını kullanmak ve yaşam döngüsü platformlarına uygun hareket edilmesi siber güvenliğe katkı sağlayacaktır.

Güvenlik mimarisi içerisinde kullanılan bilişim sistemleri, geliştirilen yazılım ve uygulamalar, ağ teknolojieri ve farkındalık ile katmanlı bir mimari yapı kurulması vaz geçilmezdir. Bu mimari oluşturulurken dikkat edilmesi gereken en önemli husus ise birbirleriyle olan entegrasyonlarıdır. Mimari içerisinde biz güvenlik kırılması durumunda etkisini minimuma düşürebilmek için mimarinin doğru şekilde çıkarılması ve güncelliğinin sürdürülmesi çok önemlidir.

Tüm bunların sağlanabilmesi için üreticiler, distribütörler, bayiler ve hizmet sağlayacıların tümüne tedarikçi olarak adlandırabiliriz. Tedarikçilerin değerlendirilmesi ve tetkik edilmeside bir o kadar önemlidir. Alınan ürün ya da hizmet üzerindeki yetkinliği, yeterliliği ve tecrübesi siber güvenlik ve bilgi güvenliği için hayati önem taşımaktadır. Bir çok kuruluş artık bir çok hizmeti dış kaynaklı olarak almakta, ilgili dış kaynak hizmeti yetkin ve yeterli kuruluşlardan almadığı takdirde yaşanabilecek güvenlik kırılmalarından kuruluş zarar görecektir.

Bu tarz kötü tecrübelerin yaşanmaması adına tedarikçilerin ilgili hizmetlerinin ve tedarikçinin tetkik edilmesi hatta yerinde tetkik edilmesi önemlidir. Tedarikçinin iş kabiliyetini sürdürebilmesi, personel değiştirme sıklığı ve kendi ürün ve hizmetlerindeki yetkinliği ve yeterliliği çok önemlidir.

Tüm bunlara karşın bir güvenlik kırılması yaşanması mümkündür. Yüzde yüz güvenlikten bahsetmek mümkün olmayacaktır. Sıfırıncı gün açıklıkları olması nedeniyle bu oran her zaman yüz bareminin altında kalacaktır. Sıfırıncı gün açığı tespit edilse dahi tespitten sonra ilgili açıklığın kapatılması da ayrıca bir süreç gerektirecektir. Bu nedenle ihlal olaylarının takibi ayrıca önem kazanmaktadır.

İhlal olaylarının yönetimi dünyada ve ülkemizde belirli sektörler için kanunlarla belirlenmiştir. Ülkemizde siber olaylara müdahale ekiplerinin oluşturulması ve bu ekiplerin yetkinlikleri belirlenmiştir.

Bilgi güvenliği yönetim sistemi içerisinde ve siber güvenlik içerisinde de ihlal olaylarının yönetilmesi bir gerekliliktir. Bu nedenle komitenin ihlal olaylarının yönetilmesi ile ilgili ilk müdahale, raporlama, kanıt toplama ve ihlal olaylarından öğrenme yani ders çıkarma önemlidir.

Bu sayede yaşanan tüm olaylar karşısında nasıl hareket edileceği, yapılması gereken aksiyonların neler olduğu gibi gerek dökümantasyon gerekse teknik konulara hazırlıklı olunacaktır. İhlaller esnasında zarar gören bölümün bir yedeğinin ya da sürekliliğinin sağlanması için gerekli planlamanın olup olmadığı da çok önemlidir.

Bu nedenle siber güvenlikle ilgili ürünler yeterli fazlalıkla çalıştırılmalıdır. Sektör, risk ve ihtiyaçlarla doğru orantılı olarak felaketten kurtarma merkezlerinin hazır bulunması ve devreye alınması önemlidir. Bu nedenle bilgi güvenliği ve siber güvenliğin sürdürebilmesi için komitenin kılavuzları, ilgili ürün ve hizmetlerin teknik kabiliyetleri ve eş zamanlı çalışabilmeleri önemlidir.
Tüm bunlar sağlandığı takdirde kuruluş politika, prosedür, ilgili kılavuz, standart ve yasa koyucullara uyumun incelenmesi gerekmektedir. Bu nedenle bağımsız gözetim ve denetim şirketleri tarafından siber güvenlik ve bilgi güvenliğine uyumun raporlandırılması ilgili rapor bulgularının ivedilikle değerlendirilerek sonuçlandırılması gerekmektedir.

Etkili bir siber güvenlik, sürüdülebilir ve iyieştirilebilir standart ve kılavuzlarla sağlanabilecektir.

KAYNAKLAR

Altınpulluk, Ö., 2016. ISO 27001: 2013, Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi, İstanbul.

BTK, 2014. Bilgi Teknolojileri Kurumu, Erişim Tarihi: 06.01.2020, https://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm.

E-KAP, 2020. Kamu İhale Kurumu, Erişim Tarihi: 06.01.2020, https://ekap.kik.gov.tr/.

EPDK, 2013. Enerji Piyasası Düzenleme Kurumu, Erişim Tarihi: 06.01.2020, https://www.resmigazete.gov.tr/eskiler/2013/03/20130329-5.htm.

EPDK, 2017). Enerji Piyasası Düzenleme Kurumu, Erişim Tarihi: 06.01.2020, https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-6.htm.

Erdoğan, Ş., 2020. Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ ISO 27001 Standartının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi. İstanbul.

Ganbat, O., 2013. Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetim ISO/IEC 27005 Standartlarının Uygulanması, İzmir.

Gencer, K., 2015. ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım, Afyon.

GİB, 2020. Gelir İdaresi Başkanlığı, Erişim Tarihi: 06.01.2020, https://ebelge.gib.gov.tr/efaturaozelentegratorlukbasvurusu.html

Gürcan, İ., 2014. Assessing Information Security Management Requirements For Finance Sector Using An ISO 27001 Based Approach, İstanbul.

ISACA, 2017. CSX Cybersecurity Fundamentals Study Guide, ISACA.

ISO.ORG, 2020. Committee, Erişim Tarihi: 06.01.2020, https://www.iso.org/committee/45306.html.

ISO.ORG, 2020. Developing Standards, Erişim Tarihi: 06.01.2020, https://www.iso.org/developing-standards.html.

ISO.ORG, 2020. Members, Erişim Tarihi: 06.01.2020, https://www.iso.org/members.html?m=MC.

ISO.ORG, 2020. Popular Standards, Erişim Tarihi: 06.01.2020, https://www.iso.org/popular-standards.html.

ISO.ORG, 2020. Yayınlar, Erişim Tarihi: 06.01.2020, https://www.iso.org/deliverables-all.html.

ISO/IEC 27001, 2013. Bilgi Güvenliği Yönetim Sistemi, Ankara.

ISO/IEC 27002, 2013. Code of practice for information security controls, Switzerland.

ISO/IEC 27003, 2017. Information security management systems — Guidance, Switzerland.

ISO/IEC 27004, 2016. Information security management — Monitoring, measurement, analysis and evaluation, Switzerland.

ISO/IEC 27005, 2018. Information security risk management, Switzerland.

ISO/IEC 27007, 2020. Guidelines for information security management systems auditing, Switzerland.

ISO/IEC 27008, 2019. Guidelines for the assessment of information security controls, Switzerland.

ISO/IEC 27009, 2020. Sector-specific application of ISO/IEC 27001 — Requirements, Switzerland.

ISO/IEC 27010, 2015. Information security management for inter-sector and inter-organizational communications, Switzerland.

ISO/IEC 27011, 2011. Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations, Switzerland.

ISO/IEC 27013, 2015. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, Switzerland.

ISO/IEC 27014. 2013. Governance of information security. Switzerland.

ISO/IEC 27016, 2014. Organizational economics, Switzerland.

ISO/IEC 27017, 2015. Code of practice for information security controls based on ISO/IEC 27002 for cloud services, Switzerland.

ISO/IEC 27018, 2019. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, Switzerland.

ISO/IEC 27019, 2017. Information security controls for the energy utility industry, Switzerland.

ISO/IEC 27021, 2017. Competence requirements for information security management systems professionals, Switzerland.

ISO/IEC 27031, 2011. Guidelines for information and communication technology readiness for business continuity, Switzerland.

ISO/IEC 27036, 2014. Information security for supplier relationships — Part 1: Overview and concepts, Switzerland.

ISO/IEC 27701, 2019. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, Switzerland.

ISO/IEC 30111, 2019. Vulnerability handling processes, Switzerland.

Kandemirli, B., 2012. Bilgi Teknolojileri Güvenliği Ve Sigorta Şirketinde Iso/Iec 27001 Standartları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uygulaması, İstanbul.

Kılıç, B., 2019. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' De Hukuk Bürolarında Bilgi Güvenliği Yönetimi, Ankara.

Mete, H., 2010. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezlerinde Uygulanması, Sakarya.

Songar, A., 1979. Sibernetik, İstanbul.

Ticaret, B., 2013. Ticaret Bakanlığı, Erişim Tarihi: 06.01.2020, https://www.resmigazete.gov.tr/eskiler/2013/03/20130329-5.htm.

ÖZGEÇMİŞ

Adı Soyadı : İsmail Sinan TATLIGİL

Doğum Yeri ve Yılı : İSTANBUL, 10/11/1984

Medeni Hali :Evli

Yabancı Dili : İngilizce

E-posta : sinan.tatligil@volfram.com.tr

Eğitim Durumu

Lise : Ataşehir Lisesi,
Fen – Matematik, 2001

Ön Lisans : Kahramanmaraş Sütçü İmam Üniversitesi,
Kahramanmaraş MYO, Bilgisayar Programcılığı, 2003

Lisans : Anadolu Üniversitesi,
Açıköğretim Fakültesi, İşletme Bölümü, 2014

Yüksek Lisans : Ankara Yıldırım Beyazıt Üniversitesi,
Fen Bilimleri Enstitüsü, Adli Bilişim Mühendisliği Anabilim Dalı, 2018

Yüksek Lisans : İstanbul Ticaret Üniversitesi,
Fen Bilimleri Enstitüsü, Siber Güvenlik Anabilim Dalı, 2020

Mesleki Deneyim

Superonline, Teknik Uzman	2003-2004
Bilge Adam Akademi, Eğitmen	2005-2010
Yapı Kredi Sigorta, Takım Lideri	2006-2008
SGS Süpervise Gözetme Etüd Şirketi Baş Denetçi	2015- Devam Ediyor
Volfram Bilgi Teknolojileri Yönetici	2011- Devam Ediyor

Yayınları

ISACA, 2015. Cybersecurity Fundamentals Study Guide. Çev. Tatlıgil, İ.S., ISACA, 189, USA.