MUHASEBE VE DENETİM DÜNYASI

BİLGİ SİSTEMLERİ DENETİMİNDE ISO/IEC 27001 VE ISO/IEC 27002 STANDARTLARININ YERİ

Burcu GÜNDOĞAN - Uzman Yrd.

ÖZET

Çağımızda bilgi en değerli varlık olarak kabul edilmektedir. Bilgiden ve bilgi birikimlerinden en üst seviyede fayda sağlayabilmek adına bilgi teknolojileri ve bilgi sistemleri kullanımı karar alma süreçlerinde büyük rol oynamaktadır.

Bilgi sistemleri kullanımı, bilginin yaşam döngüsü sürecinde karşılaşılabileceği riskler ve sistemler aracılığı ile üretilen bilginin gizliliği, bütünlüğü ve erişilebilirliği konusunda güvenlik zafiyetleri oluşturabilmektedir. Bu nedenle, ilgili teknolojilerin ve sistemlerin kullanımı bilgi sistemleri denetim faaliyetlerinin ortaya çıkmasını sağlamıştır.

Bilgi sistemleri denetimi, amaçlar ve hedefler doğrultusunda bağımsız bir denetim alanı olarak yürütülebileceği gibi diğer denetim alanları ile bütünleşik olarak da icra edilebilmektedir. Bu hususta uluslararası kabul görmüş standartlar, çerçeve dokümanlar ve ulusal mevzuattan kaynaklanan hükümler başvurulması gereken kaynaklardır.

Bu çalışmada, uluslararası alanda ve ülkemizde kabul görmüş olan ISO/IEC 27001 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler Standardı ve ISO/IEC 27002 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri Standardı kapsamında bilgi sistemleri denetim faaliyetleri yürütülürken uygulanması gereken kontroller incelenmiş, ilgili standartlar kapsamında yürütülecek denetim faaliyetlerinin, bilgi sistemlerini özellikle bilgi güvenliği konusunda ele aldığı gözlemlenmiştir.

Anahtar Kelimeler: Bilgi Sistemleri Denetimi, Bilgi Sistemleri Denetim Kontrolleri, Uluslararası Bilgi Sistemleri Denetim Standartları, ISO/IEC 27001, ISO/IEC 27002.

ABSTRACT

Information is considered as the most valuable asset in our era. Usage of information technologies and information systems plays a great role in decision-making processes in order to utilize preeminently the information and funds of knowledge.

Usage of information systems may generate security gaps in respect of the risks which may be encountered in the process of the life cycle of the information and of confidentiality, integrity and accessibility of the information produced through the systems.

Information systems audit, as can be conducted as an independent audit field in line with the purposes and objectives, it also can be performed integratedly with the other audit fields. In this respect, the provisions stemming from internationally approved standards, framework documents and national legislation are the resources that should be consulted.

In this study, while the information systems audit standards are conducted in scope of ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements Standard and ISO/IEC 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls Standard that are approved in the interna-

tional field and in our country; the controls that should be implemented are examined and it is observed that the audit activities which will be conducted in scope of the related standards has handled the information systems especially in the field of information security.

Keywords: Information Systems Audit, Information Systems Audit Controls, International Information Systems Standarts, ISO/IEC 27001, ISO/IEC 27002.

GİRİŞ

Bilgi ve iletişim teknolojileri alanında yaşanan gelişmeler ve buna bağlı olarak değişim gösteren iş ve rekabet ortamı, kamu kurumlarını ve özel sektörü önemli ölçüde etkileyerek, söz konusu kurum ve kuruluşları iş süreçlerini gerçekleştirirken, büyük ölçüde bilgi teknolojilerine dayalı kaynakları kullanmaya sürüklemiştir. Bu çerçevede; iş süreçleri, iş hacmi ve sistemlerin karmaşıklığı arttıkça sistemlerin doğasından ve etkileşim içinde olduğu yapılardan kaynaklanan risklerin ortadan kaldırılmasına veya seviyelerinin makul düzeye indirilmesine yönelik olarak bilgi sistemleri denetimleri çözüm olarak karşımıza çıkmaktadır.

Finans, bankacılık, enerji, sağlık, ulaştırma, telekomünikasyon, elektronik devlet hizmetleri, elektronik ticaret gibi birçok sektör bilgi sistemlerinden faydalanmakta ve ilgili sektörlerin bilgi sistemlerinde karşılaşılan olumsuzlukların sebep olduğu çeşitli tehditler ve yol açtığı riskler, düzenli aralıklarla ve sistematik bir şekilde bir dizi teknik kontrolün yapılmasını gerekli kılmaktadır. Bilişim suçlarının ve bilgi sistemlerinden kaynaklanabilecek tehditlerin önüne geçmek amacıyla yasal düzenlemeler ve bu hususta en iyiye yakın yapının nasıl olması gerektiği konusunda ulusal ve uluslararası standartlar, çerçeve dokümanlar ve rehberler geliştirilmiştir.

1. BİLGİ SİSTEMLERİ

1.1. Kavramsal Çerçeve

Küreselleşmenin ve teknolojik gelişmelerin hızla gerçekleştiği çağımız bilgi çağı olarak nitelendirilebilir. Bu bağlamda bilgi çağı, bilginin amacına uygun olarak kullanılması ihtiyacını doğurmaktadır, bilgiyi iyi tanımlamak, kavramak bilgi toplumlarının ileriye yönelik hedeflerini gerçekleştirmelerinin ve gelişimlerini şekillendirmelerinin en önemli anahtarıdır.

Tarih boyunca bilginin korunmasına ihtiyaç duyulmuş ve bilgilerin korunması ilk olarak sır kavramı ile ortaya çıkmıştır. Uzunca bir zaman diliminde bilginin yazılı ortama aktarılması, saklanması, arşivlenmesi ve imha edilmesi işlemleri manuel olarak gerçekleştirilerek bilgi işleme yaşam döngüsü devam etmiştir, teknolojik gelişmeler ile bilgi ve iletişim teknolojilerinde büyük bir gelişim kaydedilmiş ve bu gelişime bağlı olarak bilgi yaşam döngüsü boyut değiştirmiştir. Bilgi yaşam döngüsü:

- Bilginin bulunması veya keşfedilmesi,
- Bilginin saklanması,
- Bilginin işlenerek kullanılması,
- Bilginin geliştirilmesi,
- Bilginin iletimi
- Bilginin arşivlenmesi
- Bilginin gerek duyulduğu takdirde imha edilmesi aşamalarından oluşur.

Manuel olarak devam eden bilgi yaşam döngüsü süreçleri elektronik ortama taşınarak, bilgi yaşam döngüsünün düzgün işleyebilmesi amacıyla sistemler oluşturulmuş ve bu sistemler bilginin boyutu, karmaşıklığı ve miktarıyla orantılı olarak karmaşık bir hal almaya başlamıştır. İlgili sistemler bilgi teknolojileri kullanılarak oluşturulan bilgi sistemleri kavramını ortaya çıkarmıştır.

Bilgi sistemleri kavramının anlaşılabilmesi için öncelikle bilgi ve iletişim teknolojilerinin temel kavramı olan bilginin tanımlanması gereklidir. Bilgi aşamalar halinde şekillenirken farklı terimlerle literatürde yer alır bunlar; veri, bilgi, özbilgi, malumat olarak

isimlendirilir. Bu terimlerin, aşağıda açıklanan tanımları aralarındaki farkı ortaya koymaktadır.

Veri: Bilgi teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

Bilgi: Bilgi, zihnin öğrenme ve öğrenilenden yararlanabilme yetisi ile verinin kişisel deneyimlere, algılara, sezgilere göre şekil almış halidir. Bir başka deyişle, verinin anlamlı hale getirilerek iletişim amacıyla kullanılabilir duruma dönüştürülmesi olarak ifade edilebilir.

Özbilgi: Bilginin tecrübe etme, gözlemleme, farkındalığını kavrama gibi süreçlerden geçerek, bilginin ne olduğuna (know-what), niçin ortaya çıktığına (know-why), nasıl oluştuğuna (know-how) ve kim tarafından kullanılması gerektiğine (know-who) dair niteliklerinin bir araya gelerek oluşturduğu yapı olarak ifade edilebilir.

Hikmet: Hikmet, belirli bir alana özgü özbilginin, kişisel deneyimler ve birikimler sonucunda nasıl kullanılacağının kavranması olarak tanımlanabilir.

Şekil 1. Bilgi Piramidi

1.2. Bilgi Sistemleri

Bilgi sistemleri; planlama, kontrol ve karar verme süreçlerinde gerekli olan bilginin toplanması, işlenmesi, erişilmesi, saklanması ve aktarılmasında kolaylık ve etkililik sağlanması amacıyla bilgi teknolojileri kullanılarak oluşturulan ve kullanıcılar ile etkileşim içerisinde bulunan sistemler bütünüdür.

En yaygın anlamıyla bilgi sistemleri, enformasyonun çeşitli ihtiyaçları gidermek üzere düzenlenmesi, işlenmesi, depolanması ve istenildiği zaman iletilmesi için organize edilmiş bir kurallar bütünüdür.

Bilgi sistemlerinin tarihçesi 1960'lı yıllara dayanmaktadır. 1960'lı yıllarda bilgi sistemleri basit düzeyde ve çok temel işlemleri gerçekleştirirken, 1970'li yıllarda karar destek sistemleri olarak kullanılmaya başlandı. 1980'li ve 1990'lı yıllarda teknolojinin hızla gelişmesi sonucunda, stratejik bilgi sistemleri ve kurumsal kaynak planlama sistemlerinin (ERP) ortaya çıkması ile bilgi sistemlerinde önemli gelişmeler yaşanıldı.

Günümüzde ise bilgi sistemleri kullanımı kuruluşlar için nerdeyse kaçınılmaz duruma gelmiştir. Bilgi sistemleri kullanımı, kuruluşlara yeni müşteriler bulma, yeni pazarlara açılma, paydaşları ile kolay çalışma ortamı yaratma, rakipleri arasında fark yaratma vb. pek çok konuda avantaj sağlamaktadır. Bu nedenle kuruluşlar büyük bütçeler ayırarak bilgi sistemlerinin faaliyet alanlarına ve amaçlarına uygun olarak kullanılmasını sağlamaya yönelik yatırımlar yapmaktadır. Bilgi sistemleri, kuruluşun yönetimi, kuruluş organizasyonunu oluşturan çalışanlar ve bilgi teknolojileri ile sürekli etkileşim içerisinde bulunmaktadır.

Şekil 2. Bilgi Sistemleri Etkileşim Alanı

1.3. Bilgi Sistemleri Kullanılmasına Duyulan İhtiyaç

Gelişen teknoloji ve buna bağlı olarak değişen iş ve rekabet ortamında, kuruluşlar

varlıklarını sürdürmek amacıyla gelişime ve değişime hazırlıklı olmalıdırlar. Bu nedenle bilgi sistemlerinin kullanımı kuruluşlar açısından büyük önem arz etmektedir. Günümüzde bir kuruluşun varlığını sürdürebilmesinin bilgi teknolojilerinden büyük oranda yararlanmasına bağlı olduğu bir gerçektir. Drucker (1993)'ın ifade ettiği gibi, bugün temel ekonomik kaynaklar artık ne sermaye ne doğal kaynaklar ne de işgücüdür, en önemlisi bilgidir. İş süreçlerinin manuel olarak yürütülmesi; zaman, verimlilik ve kullanılan insan gücü kriterleri açısından, bu süreçlerin bilgi sistemleri kullanılarak yürütülmesi ile karşılaştırıldığında genellikle düşük performans sergilediğinden, bilgi sistemleri kullanmak bilgiden en hızlı ve etkin şekilde verim elde etmeyi sağlar.

Bilgi sistemleri kullanmanın kuruluşlara sağladığı faydalar genel olarak:

- Kuruluşların ihtiyaç duyduğu bilgilerin toplanması, işlenmesi, erişilmesi, saklanması ve aktarılması süreçlerinde kuruluşlara zaman kazandırması,
- Kuruluştaki operasyonel verimliliği arttırması,
- Bilgiye dayalı yeni ürünlerin geliştirilmesini sağlayarak rekabet gücünü arttırması,
- Kuruluşun bulunduğu konumun bir önemi olmadan bilgisayar ağları üzerinden aynı kuruluşa ait farklı konumda bulunan şubeler, proje grupları, paydaşlar veya farklı kuruluşlar ile iletişimi sağlayarak maliyet ve zaman kazandırması,
- Yönetilebilir kontrol mekanizmaları oluşturarak kuruluşun ihtiyaç duyduğu bilgiye ve dosyalara erişiminde kolaylık sağlaması,
- Küreselleşen dünyada kuruluşların yeni pazarlara girmesi, ürünlerini ve hizmetlerini sunması ve yeni müşteriler kazanması konularında fırsatlar sunması,
- Kuruluşların çalışanları üzerinde oluşturduğu pozitif etkiler ve bilgi sistemlerine yapılan yatırımların zaman içerisinde kuruluşların performanslarını arttırması, şeklinde ifade edilebilir.

2. BİLGİ SİSTEMLERİ DENETİMİ

Bilgi sistemleri denetimi, bilgi sistemleri denetim standartları ve çerçeve dokümanlar kapsamında sistemler üzerinde; bilgi varlıklarının korunmasına, bütünlüğünün, erişilebilirliğinin, güvenilirliğinin sağlanmasına ve bilgi sistemlerinin kuruluşun hedeflerine ve faaliyet alanına yönelik etkin ve verimli bir hizmet sağladığına yönelik makul güvence vermek üzere yapılan incelemedir.

Bilgi sistemleri denetimlerinin niteliği, kapsamı ve yürütülme biçimi denetimin hedefine göre değişmektedir. Denetim hedefi finansal süreçleri etkileyen bilgi sistemleri süreçlerinin denetlenmesi, belirli bir faaliyet alanına hizmet veren bilgi sistemlerinin işleyişinin yasal mevzuata uygunluğunun tespiti, bilgi sistemlerinin bilgi güvenliği konusunda değerlendirilmesi, bilgi sistemlerinin performans ve etkinliğinin değerlendirilmesi veya farklı özel hususların değerlendirilmesi doğrultusunda olabilir. Bu nedenle belirlenen hedefler doğrultusunda, bilgi sistemleri denetimi bağımsız bir denetim olarak icra edilebileceği gibi mali denetim, uygunluk denetimi, performans denetimi, güvenlik denetimi gibi diğer denetim alanları ile bütünleşik/entegre denetim olarak da yürütülebilir.

Mali denetim ile birlikte yürütülen bilgi sistemleri denetiminde; denetçilerin görüş verdiği mali tablolar bilgi sistemlerinin ürettiği verilerle oluşturuluyor ise denetlenen kuruluşta bilgi sistemleri kullanımının, mali tablolara ve mali süreçlere yaptığı etki ile ortaya çıkardığı riskler incelenir. Bu tür bir denetimde, mali verilerin bilgi sistemleri kullanılarak işlenmesi, saklanması ve iletilmesinin, iç kontrol sistemlerine olan etkisi ile yapısal risklere veya kontrol risklerine ilişkin denetçi kanaatine ne ölçüde tesir ettiği değerlendirilir. Sonuç olarak ise mali bilgiler

üzerinde doğrudan ve önemli etkiye sahip bilgi sistemleri kontrolleri hakkında bir görüş oluşturulur. (Asya Ülkeleri Sayıştaylar Birliği - ASOSAI, 2003)

Uygunluk denetimi kapsamında yürütülen bilgi sistemleri denetiminde, yasal mevzuatın belirttiği hususlar bilgi sistemleri kullanılarak gerçekleştiriliyor veya bilgi sistemleri kullanımından kaynaklanan yasal mevzuat yükümlülükleri bulunuyor ise bu hususlara ait süreçlerin sistemler üzerindeki işleyişe doğru olarak uygulanıp uygulanmadığına ve gerekli kontrol mekanizmalarının var olup olmadığına yönelik incelemeler yapılarak, bilgi sistemlerinin ilgili yükümlülükleri karşılayıp karşılamadığı konusunda görüş oluşturulur.

Performans denetimi kapsamında gerçekleştirilen bilgi sistemleri denetiminde, ilgili faaliyet alanına yönelik bilgi sistemleri üzerinden yürütülen iş süreçlerinin denetlenin amaç ve hedeflerini gerçekleştirmesi konusunda, ne kadar etkin ve verimli çalıştığı değerlendirilerek ilgili bilgi sistemleri hakkında görüş oluşturulur.

Güvenlik denetimi kapsamında gerçekleştirilen bilgi sistemleri denetiminde, bilgi güvenliği politikaları, erişim ve yetkilendirme yönetimi, insan kaynakları güvenliği, denetim izlerinin tutulması, fiziksel ve çevresel güvenlik, kriptografi vb. alanlarda kontroller yürütülür. Güvenlik denetimleri mali, uygunluk, performans denetimlerinin kapsamı içerisinde de yürütülebilmektedir.

2.1. Bilgi Sistemleri Denetimi Neden Gereklidir?

Bilgi sistemlerinin yaygın olarak hemen her sektörde kullanımı, birçok iş sürecine yeni ve hızlı çözümler sunmakla birlikte yeni iş risklerinin ortaya çıkmasına sebep olmuştur. Kuruluşlar bu sistemleri kullanarak iş hedeflerini yerine getirmenin yanında, oluşabilecek risklere karşı mücadele etmek zorunda kalmıştır. Bilgi sistemlerinin güvenli bir ortamda çalışıp çalışmadığından, bu sistemlerin doğru veriler üretip üretmediğine kadar bir dizi kontrol yapılarak bu sistemlerin düzenli aralıklarla değerlendirilmesi risklerin ortadan kaldırılması veya asgari seviyeye indirilebilmesi, kuruluşun sektördeki güvenilirliği açısından önem arz etmektedir. Etkileşim içerisinde olan tüm iş süreçlerinden kaynaklanacak risklere karşı, kuruluşlar olası risklerin önüne geçmek için hem iç denetim faaliyetlerini yürütmekte hem de dış kaynakların değerlendirmeleri sonucunda risklere karşı önlemler almakta, önleyici faaliyetleri hayata geçirmekte ve bu denetim faaliyetlerini düzenli aralıklarla tekrarlamaktadırlar. Yapılan denetimler sayesinde, kuruluşların iş hedeflerinde daha kararlı sonuçlara ulaşması bu kuruluşları sektörde daha güvenilir bir noktaya taşımaktadır. Bilgi sistemleri denetimini gerekli ve zorunlu kılan durumları sıralayacak olursak:

- Teknolojik gelişmelere bağlı olarak manuel olarak gerçekleştirilen kurumsal faaliyetlerin büyük ölçüde bilgi sistemleri üzerinden yürütülmesi sonucunda kritik verilerin izlenmesinin ve kontrol altına alınmasının güçleşmesi,
- Bilgi sistemlerinin gün geçtikçe daha karmaşık bir yapıya dönüşmesi,
- Kurumsal yönetişim için bilgi sistemlerinin güvenliğinin artan önemi,
- Bilgi sistemlerinden kaynaklanan risklerin, kuruluşların diğer faaliyet süreçlerinde yeni risk faktörleri oluşmasına zemin hazırlaması,
- Kuruluşların bilgi sistemlerini kontrolleri kabul görmüş bir standart ve çerçeve doküman kapsamında değerlendirerek, bu sistemlerin doğru ve güvenilir işlediklerinden emin olma istekleri,
- Bilgi sistemleri üzerinde iş sürekliliğini sağlamaya yönelik güvence sağlanması isteği,
- Kuruluşların faaliyet alanları doğrultusunda hizmet veren bilgi sistemlerinin kullandığı teknolojilerin kuruluşun amaç ve ihtiyaçlarına uy-

gunluğunun belirlenmesi,

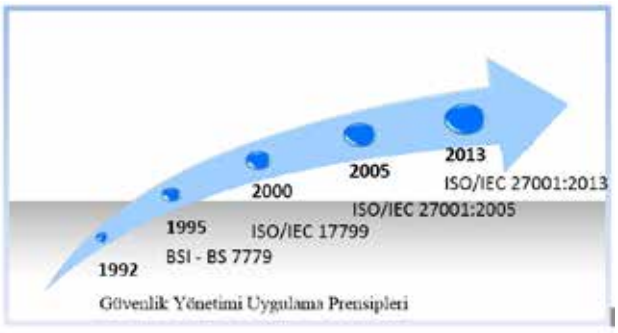
- Bilgi sistemlerinden kaynaklanan risklere karşı kuruluşların önlem almak istemesi,
- Bilgi sistemleri altyapısı için optimum çözüm sağlanmak istenmesi,
- Bilgi sistemleri alanında yasal mevzuattan kaynaklanan yaptırımlara uyum sağlayabilmek şeklinde ifade edilebilir.

3. TS ISO/IEC 27001, TS ISO/IEC 27002 STANDARDI VE BİLGİ SİSTEMLERİ DENETİMİNDEKİ YERİ

3.1. TS ISO/IEC 27001 Standardı

TS ISO/IEC 27001 standardının tarihi gelişimi, 1992 yılında İngiltere'de kamu ve özel sektörde yer alan birçok kuruluşun bilgi güvenliği standardı oluşturulmasına yönelik isteği dikkate alınarak İngiliz Standartları Enstitüsü (BSI) desteği ile oluşturulan çalışma grubu tarafından BS (British Standart) 7779 adında bir rehber oluşturulması ve söz konusu rehberin İngiliz Standartları Enstitüsü tarafından BS 7779 İngiliz Standardı olarak kabul edilmesi ile başlamıştır. İlgili standart BS 7779 – 1 ve BS 7779 – 2 olarak iki kısımdan oluşmuştur. İngiliz Standartları Enstitüsü tarafından 1999 yılında BS 7779 – 2 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri adı altında yayımlanmış ve ISO (International Organization for Standardization – Uluslararası Standardizasyon Kuruluşu) tarafından 2000 yılında ISO/IEC 17799 standardı olarak kabul görmesi ile ilgili standart ülkemizde de 2002 yılında TSE tarafından kabul görmüştür. Daha sonra ISO tarafından 2005 yılında ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereklilikleri adı altında yayımlanmıştır. 2006 yılında ISO/IEC 27001:2005 sürümü ve 2014 yılında ISO/IEC 27001:2013 sürümü TSE tarafından Türkçe olarak yayımlanmıştır.

Şekil 3. ISO/IEC 27001 Tarihi Gelişimi



TS ISO/IEC 27001 standardı Information Technology – Security Techniques – Information Security Management Systems – Requirements olarak adlandırılmış, ülkemizde TSE tarafından Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler olarak kabul görmüştür.

Bu standart, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır. İç ve dış taraflar tarafından, kuruluşun kendi bilgi güvenliği gereksinimlerini karşılayıp karşılamadığına ilişkin kabiliyetinin değerlendirilmesi amacıyla kullanılabilir. Bu standartta ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm kuruluşlara uygulanabilir olması hedeflenmiştir. (TS ISO/IEC 27001, 2013) Teknik ve teknoloji bağımlı bir standart değildir. Belli bir ürün veya bilgi teknolojisi ile ilgilenmez. Hatta bilgi teknolojileri güvenliği dahi standart içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir. Teknik detaylara inmeden kuruluşların bilgi güvenliği hususunda neler yapması gerektiğini açıklar. Standart, aşağıda belirtilen 7 bölüm başlığından ve bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrolleri içeren EK A Referans Kontrol Amaçları ve Kontroller çizelgesinden oluşmaktadır.

- Kuruluşun Bağlamı
- Liderlik
- Planlama
- Destek

- İşletim
- Performans Değerlendirme
- İyileştirme

Standardın 2005 yılına ait sürümünde sürekli vurgulanan Planla – Uygula – Kontrol Et – Önlem Al (PUKÖ) döngüsüne olan bağlılık 2013 yılında yayımlanan sürümünde görülmemekte bunun yerine düzenli aralıklarla iyileştirme ve geliştirme yapılmasının önemi vurgulanmaktadır. Bu durum, PUKÖ döngüsünün istenilirse sürekli iyileşmeyi sağlamak adına güncel sürümde de kullanılabileceğini göstermektedir.

Güncel sürümde yer alan bölüm başlıkları PUKÖ döngüsünün fazlarıyla aşağıdaki gibi eşleştirilebilir.

Tablo 1. PUKÖ Döngüsü ile ISO 27001:2013 Maddelerinin Eşleştirilmesi

PUKÖ	27001:2013 Bölüm Başlıkları	
Planla	4. Kuruluşun Bağlamı 6. Planlama	5. Liderlik
Uygula	7. Destek 8. İşletim	
Kontrol Et	9.Performans Değerlendirme	
Önlem Al	10. İyileştirme	

Standart, kamu ve özel sektörde bilgi güvenliğinin sağlanmasını ve bu konudaki denetimlerin yapılmasını kolaylaştıran bir çerçeve özelliği taşımakta ve bilgi sistemleri denetimi kapsamında kullanıldığında standartta yer alan bütün kontrollerin kuruluş üzerinde uygulanması gerekmektedir.

3.1.1. Bilgi Güvenliği

Günümüzde bilgi teknolojilerinde, iş süreçlerinde hızlı yaşanan gelişmelere ve değişimlere, bilgi toplumu olma sürecinin getirdiği yükümlülüklere paralel olarak kişilerin ve kuruluşların sahip oldukları bilginin önemi giderek artmaktadır. Bilginin öneminin ve bilgiye olan bağımlılığın giderek artması bilginin korunması ihtiyacını doğurarak, bilgi güvenliği kavramının ortaya çıkmasına sebep olmuştur.

Bilgi güvenliği, bilginin yetkisiz kullanıma, erişime, ifşa edilmeye, değiştirilmeye, hasara veya yok edilmeye karşı korunması ve bu eylemlere ilişkin önlemlerin alınması olarak tanımlanabilir. Bir başka ifadeyle bilgi güvenliği, bilginin korunmasına yönelik geçerli üç unsur olan bilginin gizliliği, bütünlüğü ve erişilebilirliği konusunda olası riskleri göz önünde bulundurarak bunlar için gerekli önlemlerin alınmasıdır.

Bilgi güvenliğinin temel unsurları, Gizlilik (Confidentiality), Bütünlük (Integrity), Erişilebilirlik/Kullanılabilirlik (Availability) kavramlarıdır. Temel unsurların yanında güvenilirlik, erişim denetimi, hesap verebilirlik, inkar edilemezlik, emniyet unsurları bilgi güvenliğini destekleyen unsurlardır. Temel unsurları açıklayacak olursak:

Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesi veya yetkisiz kişilerin bilgiyi açığa çıkarması ihtimaline karşı erişiminin engellenmesidir.

Bütünlük: Bilginin yetkisiz veya yetki dahilinde, kasıtlı veya kasıtsız olarak değiştirilmesinin, silinmesinin vb. eylemlere karşı bilginin içeriğinin korunmasıdır.

Erişilebilirlik/Kullanılabilirlik: Bilginin ihtiyaç duyulduğu her an yetkili kişinin kullanımına hazır olmasıdır.

Bilgi teknolojileri ve bilgi sistemleri alanında, bilgi güvenliğinin amacı kişi veya kuruluşların söz konusu teknolojileri veya sistemleri kullanırken karşılaşabilecekleri tehdit, tehlike ve olası risklere karşı analizlerin yapılarak gerekli önlemlerin alınmasını sağlamaktır. Bu bağlamda kuruluşlara yönelik alınacak önlemler bilgi güvenliği yönetim sistemi kurularak gerçekleştirilebilmektedir.

3.1.2. Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi kavramı ilk

kez İngiliz Standartları Enstitüsü (British Standards Institute) tarafından yayımlanan BS 7799 – 2 standardında kullanılmıştır. Günümüzde ise TS ISO/IEC 27001 standardı kapsamında; "Bilgi güvenliği yönetim sistemi, bilginin gizliliği, bütünlüğü ve erişilebilirliğini risk yönetimi prosesini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir." şeklinde tanımlanmaktadır.

Kuruluşlarda, bilgi güvenliğini sağlamaya yönelik alınan teknik önlemler tek başına yeterli olmadığından, bilgi güvenliğinin ve denetiminin sağlanması konusunda uluslararası kabul görmüş standartlar ve çerçeve dokümanlar kapsamında, kuruluşların ihtiyaçları doğrultusunda ölçeklenen bilgi güvenliği yönetim sisteminin oluşturulması büyük önem arz etmektedir.

Bilgi güvenliği yönetim sistemi, kuruluşun amaçlarının, hedeflerinin, faaliyet alanının ve iş kültürünün ayrılmaz bir parçası olarak görülmeli ve kuruluş organizasyonunu, politikalarını ve prosedürlerini kapsamalıdır. Bilgi güvenliği yönetim sisteminin kurumsal prosesler ve genel yönetim yapısının bir parçası olması ve bunlar ile entegre olması ve bilgi güvenliği süreçlerinin, bilgi sistemlerinin ve kontrollerin tasarımında dikkate alınması önemlidir. (TS ISO/IEC 27001, 2013)

Bilgi güvenliği yönetim sistemi kurulumu, kuruluşun faaliyetlerini gerçekleştirme tarzını etkileyen geniş çaplı bir sistemdir. Kuruluşun bilgi güvenliği yönetim sistemi, sadece bilgi sistemleri ya da bilgi teknolojileri birimlerini etkileyen bir yapı değildir. Kuruluşun en üst kademelerinde yer alan yöneticiler de dahil olmak üzere kuruluşun tüm çalışanlarının sorumluluk alarak, sistemin getirdiği bilgi güvenliği prensiplerine uygun davranmalarını ve desteklerini gerektirir.

Bilgi güvenliği yönetim sistemi kurmanın, kuruluşlara sağladığı faydalar;

- Bilgi varlıkları hakkında ve bilgi güvenliği konularında farkındalık sağlama,
- Bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması,
- İş sürekliliğinin sağlanmasına yardımcı olması,
- Kuruluşta risk farkındalığının yaratılması,
- Kuruluş içerisinde veya dışarıdan tedarik yöntemi ile çalışanların, bilgi varlıklarına yönelik yetkisiz veya kötü niyetli kullanımının önüne geçilmesi,
- Rekabet ortamında, müşteri bilgileri güvenliğine gösterilen özeni avantaj haline getirmesi,
- Kuruluşa yönelik piyasa güvenini arttırması,
- Kuruluşun güvenlik ihlallerinden kaynaklanan maliyetlerini düşürmesi,
- Kuruluşun, bilgi güvenliği konusunda yasal mevzuat ve düzenlemelere uyum sağlamasını kolaylaştırması,
- Kuruluşun bilgi sistemlerinin, bilgi güvenliği yönetim sisteminin kurulmasında yol gösterici olan uluslararası standart veya çerçeve dokümanlar ile uyumunun sağlanması şeklinde özetlenebilir.

3.2. TS ISO/IEC 27002 Standardı

TS ISO/IEC 27002 standardının tarihi gelişimi, 1992 yılında İngiltere'de kamu ve özel sektörde yer alan birçok kuruluşun bilgi güvenliği standardı oluşturulmasına yönelik isteği dikkate alınarak, İngiliz Standartları Enstitüsü (BSI) desteği ile oluşturulan çalışma grubu tarafından BS 7779 adında bir rehber oluşturulması ve söz konusu rehberin İngiliz Standartları Enstitüsü tarafından BS 7779 İngiliz Standardı olarak kabul edilmesi ile başlamıştır. İlgili standart BS 7779 – 1 ve BS 7779 – 2 olarak iki kısımdan oluşmuştur. BSI tarafından yayımlanan BS 7779 – 1 bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu standart ISO tarafından kabul edilmiş ve

ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılmıştır. 2014 yılında güncel hali olan ISO/IEC 27002:2013 sürümü TSE tarafından Türkçe olarak yayımlanmıştır.

Söz konusu standart, ISO/IEC 27001 standardına dayalı bilgi güvenliği yönetim sistemi uygulanması sürecinde, gerekli kontrolleri seçmek için kuruluşların bir referans model olarak kullanmaları ya da yaygın olarak kabul edilen bilgi güvenliği kontrolleri için kılavuz doküman olması amacıyla hazırlanmıştır. Aynı zamanda sanayi ve kurumlara özgü bilgi güvenliği yönetim sistemi kılavuzlarının, söz konusu sektöre özgü bilgi güvenliği risk çevrelerinin de dikkate alınarak geliştirilmesi amacıyla hazırlanmıştır. Daha genel bir anlamda, etkin bilgi güvenliği; işi mümkün kılan bir faktör olarak, yönetim ve diğer paydaşları kuruluşun varlıklarının oldukça güvenli ve zararlara karşı korumalı olmasını temin etmektedir. (TS ISO/IEC 27002, 2013)

TS ISO/IEC 27001 standardı gibi bu standartta teknik ve teknoloji bağımlı bir standart değildir. Teknik detaylara inmeden, kuruluşların bilgi güvenliği hususunda gerekli kontrolleri uygulaması için uygulama prensipleri sunar.

Standart, 14 ana güvenlik kontrol maddesi altında toplamda 35 ana güvenlik kategorisi ve 114 kontrol içermektedir. Ana güvenlik kategorileri şu şekildedir:

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliğinin Organizasyonu
- İnsan Kaynakları Güvenliği
- Varlık Yönetimi
- Erişim Kontrolü
- Kriptografi
- Fiziksel ve Çevresel Güvenlik
- İşletim Güvenliği
- Haberleşme Güvenliği
- Sistem Edinimi, Geliştirme ve Bakımı
- Tedarikçi İlişkileri
- Bilgi Güvenliği İhlal Olayı Yönetimi
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları
- Uyum

3.3. TS ISO/IEC 27001 ve TS ISO/IEC 27002 Standartları Kapsamında Bilgi Sistemleri Denetimi

TS ISO/IEC 27001, bilgi güvenliği yönetim sistemi gereksinimlerini tanımlayarak, bu hususdaki bilgi güvenliği denetim kontrollerinin listesini tanımlar. Bu standart, TS ISO/IEC 27002 standardı ile şartlar ve kontroller yönü ile birbirine sıkı bir şekilde bağlıdır. TS ISO/IEC 27002 standardında da bu ilişkiyi destekleyen, "TS ISO/IEC 27001 standardına dayalı bilgi güvenliği yönetim sistemi uygulanması sürecinde kontrolleri seçmek için kuruluşların bir referans model olarak kullanmaları ya da yaygın olarak kabul edilen bilgi güvenliği kontrolleri için kılavuz doküman olması amacıyla bu uluslararası standart hazırlanmıştır." ifadesi yer almaktadır. Bu nedenle ilgili iki standart, bilgi güvenliği konusunda gerçekleştirilen bilgi sistemleri denetimlerinde birlikte kullanıldığı takdirde daha faydalı olacaktır.

TS ISO/IEC 27001 standardı, bilgi güvenliği yönetim sistemi kurmak isteyen kuruluşların, risk analizi çalışması yaparak ilgili kontrolleri devreye almasını ve mevcut risklerin ortadan kaldırılmasını veya kabul edilebilir risk seviyesinin altına düşürülmesini şart koşmaktadır. Bu kontroller TS ISO/IEC 27001 standardı için önem taşıyan TS ISO/IEC 27002 standardında detaylı olarak açıklanmaktadır.

TS ISO/IEC 27002 standardı 14 ana güvenlik kontrol maddesi, bu kontrollerin altında tanımlı 35 ana güvenlik kategorisi ve 114 kontrol içermekte ve kuruluşun bilgi sistemleri

yapısına bağlı olarak herhangi bir güvenlik kontrolü bir değerine göre önem arz edebilmektedir. TS ISO/IEC 27001 standardı kapsamında yapılacak bilgi sistemleri denetimlerinde, standardın sunmuş olduğu EK A - Referans Kontrol Amaçları ve Kontroller adında çizelge bulunmaktadır. Bu çizelge TS ISO/IEC 27002 standardının 5. ana güvenlik kontrol maddesinden 18. ana güvenlik kontrol maddesine kadar listelenen ve bunlara bağlı kontrol hedeflerinden oluşmaktadır. Çizelge, ilgili standartlar kapsamında denetim yapacaklara veya kuruluşlar için bilgi güvenliği yönetim sistemi kurulmasında yol gösterici olacaktır.

Bilgi sistemleri denetiminde veya bilgi güvenliği yönetimi için kontrollerin seçimi; kuruluş kararlarında temel alınan risk kabulüne, risk işleme seçeneklerine ve kuruluşta uygulanan genel risk yönetimi yaklaşımına bağlıdır. Ayrıca kontrol seçimi, savunma derinliği sağlamak için kontrollerin birbirleriyle olan etkileşim tarzına bağlıdır. Kontrollerin uygulanmasında kullanılan kaynaklar, bu kontrollerin yokluğunda güvenlik sorunlarının neden olacağı muhtemel iş zararlarına karşı dengelenmelidir. (TS ISO/IEC 27002, 2013)

İlgili iki standart kapsamında, bilgi güvenliği alanında yapılacak bilgi sistemleri denetimlerinde veya bilgi güvenliği yönetim sistemi kurulması sürecinde uygulanması gereken kontrolleri ve kontrol amaçlarını açıklayacak olursak:

- **Bilgi Güvenliği Politikaları**

Bilgi güvenliğini sağlamak için, kuruluşun iş gereksinimlerine, ilgili yasalara ve düzenlemelere göre yönetim tarafından onaylanan bilgi güvenliği politikası oluşturulmalıdır. Söz konusu politika iş stratejisinden, düzenlemelerden, yasalardan ve sözleşmelerden, mevcut ve öngörülen tehdit ortamından kaynaklanan gereksinimleri karşılamalıdır. Bilgi güvenliği politikası kuruluş çalışanları, ticari ortaklar, yükleniciler ve hizmet sağlayıcılar ile paylaşılmalıdır. İlgili politika kuruluş dışındakilerinin erişimine açılırsa, gizli bilgilerin ifşa edilmemesine dikkat edilmelidir.

- **Bilgi Güvenliğinin Organizasyonu**

Bilgi güvenliğinin organizasyonuna ilişkin kontroller, kuruluş içerisinde bilgi güvenliğini sağlamaya yönelik organizasyonel bir yapının oluşturulmasını ve kurum dışından ya da mobil cihazlardan bilgi varlıklarına yapılan erişimin güvenliğini sağlamayı hedeflemektedir.

- **İnsan Kaynakları Güvenliği**

İnsan kaynakları güvenliğine ilişkin kontrollerin amacı kuruluş bünyesinde veya dışarıdan tedarik yolu ile çalışanların, sorumluluklarına ilişkin görevler için yetkinliğini, uygunluğunu belirlemek, yasal mevzuattan kaynaklanan gereklilikleri sağladıkları konusunda emin olmak, ilgili kişilerin istihdamının son bulması halinde bilgi güvenliği ile alakalı uygulanacak politika ve prosedürlerin oluşturulmasını sağlamaktır.

- **Varlık Yönetimi**

Varlık yönetimi kontrollerinin temel amacı kuruluşun bilgi varlıklarının tespit edilerek, ilgili varlıkların bilgi güvenliği kapsamında korunmasını sağlamaktır. Varlık yönetimi kontrolleri; varlıkların sorumluluğu, bilgi sınıflandırma ve ortam işleme kontrollerinden oluşur.

- **Erişim Kontrolü**

Erişim kontrollerinin amacı; kuruluşun bilgi varlıkları üzerinde gerçekleştirilen fiziksel ve mantıksal erişimin, bilgi güvenliği şartları temelinde oluşturulmuş, erişim talebi, erişim yetkilendirmesi, erişim haklarının periyodik olarak gözden geçirilmesi, ayrıcalıklı erişim rolleri, erişim haklarının kaldırılması vb. unsurları içeren bir erişim kontrol politikası çerçevesinde yürütülmesini sağlamaktır.

- **Kriptografi**

Kriptografi kavramı, belirli bir anahtar şifreleme yöntemi ile bilginin kodlanmış bir hale getirilerek, bilgi güvenliği kapsamında bilginin gizlilik, bütünlük/doğruluk, inkar

edilemezlik ve kimlik doğrulama unsurlarını sağlamayı hedefler.

Kriptografik kontroller kapsamında, kriptografik kontrollerin kullanımına, anahtarların kullanımına ve yaşam süresine dair politika geliştirildiğine ve tüm sistem yaşam döngüsü içerisinde ilgili politikaların kullanılmasına yönelik kontroller yapılır. Kuruluş kriptografik kontrollerin kullanımına yönelik politika oluştururken, dünya genelinde kullanılan kriptografi tekniklerinin kullanımı hususunda yasal düzenlemelere ve ulusal kısıtlamalara dikkat etmelidir.

- **Fiziksel ve Çevresel Güvenlik**

Fiziksel ve çevresel güvenlik kontrolleri, kuruluşun kaynaklarına yetkisiz fiziksel erişimi, hasar verilmesini, işlerliğine müdahale edilmesini, çalınmasını ve kuruluşun faaliyetlerinin durmasını ve kesintiye uğramasını engellemeyi amaçlar. Bu kapsamda bilgi sistemlerini koruma amacıyla güvenlik sınırlarının tanımlanmasına ve kullanılmasına, bu alanlara sadece yetkili personelin uygun giriş kontrolleri ile erişiminin sağlanmasına, doğal felaketler, saldırılar ve kazalara karşı fiziksel önlemlerin alınmasına, bilgi sistemleri teçhizatlarını etkileyecek çevresel tehditlerden ve tehlikelerden kaynaklanan riskleri azaltmaya yönelik önlemlerin alınmasına, teçhizatın enerji kesintileri ve diğer kesintilerden korunmasına, bilgi iletiminde kullanılan enerji ve telekomünikasyon kablolarının dinleme ve oluşabilecek hasarlara karşı korunmasına, teçhizat bakımlarının düzenli yapılmasına, teçhizatın yetki dâhilinde olmadan kuruluş dışına çıkarılmamasına yönelik kontroller yapılır.

- **İşletim Güvenliği**

İşletim güvenliğinin temel amacı; kuruluşun bilgi işleme tesislerinin güvenli bir şekilde işletimlerini sağlamaktır. İşletim güvenliği kontrolleri detayda, işletim prosedürleri ve sorumlulukları, kötücül yazılımlardan koruma, yedekleme, kaydetme ve izleme, işletimsel yazılımın kontrolü, teknik açıklıkların yönetilmesi, bilgi sistemleri tetkik hususları kontrollerini içermektedir.

- **Haberleşme Güvenliği**

Haberleşme güvenliğinin amacı, kuruluşun ağ güvenliğini ve kuruluşun gerçekleştirdiği bilgi transferine yönelik güvenliği sağlamaktır. Ağ güvenliği sağlanırken, ağ kontrolleri, ağ hizmetlerinin güvenliği ve ağlarda ayrım olmak üzere üç temel başlık altında kontroller gerçekleştirilir. Bilgi transferinde ise; bilgi transfer politikaları ve prosedürleri, bilgi transferindeki anlaşmalar, elektronik mesajlaşma, gizlilik ya da ifşa etmeme anlaşmaları başlıkları altında kontroller gerçekleştirilir.

- **Sistem Edinimi, Geliştirme ve Bakımı**

Sistem edinimi, geliştirme ve bakıma yönelik yapılan kontrollerin amacı; bilgi sistemlerinin tüm yaşam döngüsünde bilgi güvenliğinin daimi olmasını, halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilginin, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan korunmasını sağlamak, uygulamalar üzerindeki bilginin eksik iletimini, yanlış yönlendirilmesini ve yetkisiz ifşasını önlemektir.

- **Tedarikçi İlişkileri**

Tedarikçi ilişkileri kontrollerinin amacı; kuruluşun tedarikçi ilişkilerini bilgi güvenliği gereksinimlerini karşılamak adına, tedarikçi ilişkileri için hazırlanan bilgi güvenliği politikası çerçevesinde yürütmesini ve tedarikçi hizmetlerini sağlamaya yönelik yapmış olduğu anlaşmalar kapsamında izleme ve ilgili hizmetlerdeki değişiklikleri yönetme faaliyetlerini gerçekleştirmesini sağlamaktır.

- **Bilgi Güvenliği İhlal Olayı Yönetimi**

Bilgi güvenliği ihlal olayı yönetimi kapsamında yapılacak kontrollerin amacı; bilgi güvenliği olaylarının değerlendirilerek, bilgi güvenliği ihlal olayı kapsamında sınıflandırılıp sınıflandırılmayacağına karar vermek, ilgili ihlal olaylarına hızlı ve etkili yanıtların verilmesini sağlamak, ihlal olaylarının kanıtlara dayandırılması için kanıt elde etmek ve bu kanıtların korunmasını sağlamak için prosedürler tanımlamak, yazılı politika ve prosedürler kapsamında uygun yönetim kanalları

aracılığı ile ihlal olaylarının hızlı bir şekilde yetkili kişi veya mercilere raporlanmasını sağlamak, söz konusu olayların çözümlenmesinden kazanılan tecrübelerin gelecekte oluşabilecek ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmasını sağlamaktır.

- **İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları**

İş sürekliliği yönetiminin bilgi güvenliği hususları kapsamında değerlendirilmesi gerçekleştirilirken; kuruluşun olası bir kriz veya felaket durumunda bilgi güvenliği yönetimi sürekliliğini sağlamak adına ilgili gereksinimleri belirleyerek, bilgi güvenliği süreklilik gereksinimleri ile uyumlu aşağıda belirtilen hususları yazılı hale getirmesi, uygulaması ve sürdürmesi hedeflenir:

a) İş sürekliliği ya da felaket kurtarma prosesleri, prosedürleri ve destekleyici sistemler ve araçlarda yer alan bilgi güvenliği kontrolleri,

b) Olumsuz bir durum sırasında mevcut bilgi güvenliği kontrollerini sürdürmek için prosesler, prosedürler ve uygulama değişiklikleri,

c) Olumsuz bir durum sırasında sürdürülemeyen bilgi güvenliği kontrolleri için telafi edici kontroller. (TS ISO/IEC 27002, 2013)

- **Uyum**

Uyum kapsamında yapılacak kontrollerin amacı; yasal mevzuata, düzenleyici hükümlere ve sözleşmelerden doğan yükümlülüklere ilişkin ihlalleri önlemek adına kuruluşun bilgi sistemlerinin ihtiyaç duyduğu gereksinimlerin açıkça tanımlanarak yazılı hale getirilmesini, fikri mülkiyet hakları ve patentli yazılım ürünlerinin kullanımına yönelik uygun prosedürlerin ilgili yükümlülük gereksinimleri çerçevesinde oluşturulmasını, bilgi sistemleri üzerinde var olan kayıtların kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı korunmasını, kişi tespit bilgisinin mahremiyetinin korunmasını, kriptografik kontrollerin ilgili yükümlülüklere uyumlu olarak yürütülmesini sağlamaktır.

4. SONUÇ VE DEĞERLENDİRME

Bilgi toplumu olmak ve bilgi çağında yaşamak bilgiye ulaşımı kolay hale getirirken, bilginin amacına uygun olarak korunmasını bir o kadar zorlaştırmaktadır. Bilgiye duyulan ihtiyacın ve verilen önemin artması, bilgi teknolojilerinin gelişimini desteklerken, ilgili teknolojilerin ve bilgi sistemlerinin güvenilirliğini tartışma konusu haline getirmektedir.

Kuruluşlar, kurumsal iş süreçlerini gerçekleştirirken, rekabet ortamına ayak uydurmak ve faaliyet gösterdikleri sektörde farkındalık yaratmak için bilgi teknolojilerini kullanarak kurumsal bilgi varlıklarını korumayı hedeflemektedir. Bu noktada kurumsal iş süreçlerine ve hacmine bağlı olarak, bilgi işleme faaliyetleri artmakta dolayısı ile kullanılan bilgi sistemleri de karmaşık bir hal almaktadır. Söz konusu sistemlerin karmaşıklığı arttıkça, kuruluşlar kullandıkları bilgi sistemlerinin ne kadar güvenilir olduğu konusunda tereddüt yaşamakta ve kullanılan sistemlerin kuruluşun diğer iş süreçlerinde yeni risk faktörleri oluşturmasını engellemek, sistemlerin güvenilirliğinden emin olmak ve sistemlerinin güvenilirliğini kontrolleri kabul görmüş bir standarda dayandırmak istemektedirler. Bu çerçevede bilgi sistemleri denetimi kaçınılmaz bir ihtiyaç olarak karşımıza çıkmaktadır.

Bilgi sistemleri denetimi, uluslararası kabul görmüş standartlar, çerçeve dokümanlar ve rehberler aracılığı ile gerçekleştirildiği takdirde verdiği güvence kabul edilebilir olmaktadır. Bu çalışma kapsamında, uluslararası alanda kabul görmüş belirli bilgi sistemleri denetim standartları ve çerçeve dokümanları incelenerek, ilgili standartlardan TS ISO/IEC 27001 ve TS ISO/IEC 27002 standartları çerçevesinde yapılacak bilgi sistemleri denetiminin niteliği ve söz konusu standartların kapsamları, içerikleri ve kontrolleri incelenmiştir.

Söz konusu standartlar üzerinde yapılan incelemeler sonucunda; TS ISO/IEC 27001 standardı kapsamında, bilgi güvenliği yö-

netim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi faaliyetlerinin gerçekleştirilebileceği, risk yönetimi süreçleri uygulanarak bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanabileceği ve risklerin doğru yönetildiği hususunda güvence verilebileceği aynı zamanda iç ve dış kaynaklar tarafından kuruluşların bilgi güvenliği konusunda ne kadar yeterli olduğuna ilişkin değerlendirmenin yapılabileceği görülmektedir. TS ISO/IEC 27002 standardının, TS ISO/IEC 27001 standardı çerçevesinde bilgi güvenliğinin sağlanması amacıyla uygulanması gereken kontrolleri ve uygulama prensiplerini içerdiği gözlemlenmektedir. İlgili standartlar, bilgi teknolojilerinin kuruluşun iş amaçlarına uygun olarak hizmet etmesi, bilgi teknolojileri stratejisi ile iş stratejisinin uyumlu çalışması ve bilgi sistemleri hizmetlerinin planlanması ve uygulanması faaliyetlerinden ziyade, risk yönetim yaklaşımı ile bilgi güvenliği kontrollerinin nasıl yapılacağı üzerinde durmakta ve söz konusu kontrollerin uygulanması konusunda teknik ve teknolojik detaylara inmemektedir.

KAYNAKÇA

ASLAN, B. Biryönetim Fonksiyonu Olarak İç Denetim. Sayıştay Dergisi, 81.

Asya Ülkeleri Sayıştaylar Birliği - ASOSAI. (2003). IT Audit Guidelines.

CANTÜRK, S. kpmg.com.tr. (2016). <kpmg.com.tr>.

COSO. (2011). Internal Control - Integrated Framework. COSO.

COSO. (2013). Internal Control - Integrated Framework Executive Summary. COSO.

ÇALIK, O. ISO 27001:2013. ISO 27001:2013. TÜBİTAK.

Dinçer Önel, A. D. (2007, 08 28). Bilgi Güvenliği Yönetim Sistemi Kurulumu. Bilgi Güvenliği Yönetim Sistemi Kurulumu. Kocaeli, Türkiye: Uekae.

Fatih Güneş, S. K. Bilgi Teknolojileri Denetimi ve COBIT' in Sektörel Uygulanabilirliği. Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği.

Gürol CANBEK, Ş. S. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi .

İDKK. (2014, Ocak). Kamu Bilgi Teknolojileri Denetim Rehberi. Kamu Bilgi Teknolojileri Denetim Rehberi. Ankara: İDKK.

ISACA. (2014, Eylül 1). ITAF. ISACA.

Kamu Bilgi Teknolojileri Denetimi Rehberi. (2014, OCAK). Ankara, Türkiye: İç Denetim Koordinasyon Kurulu.

KAYRAK, M. (2012). IT Denetimi. Sayıştay Dergisi.

Prytherch, R. (2000). HARROD'S LIBRARIONS' Glossary and Reference Book . Gover Publishing Company Limited.

Sayıştay. (2013, Haziran). Bilişim Sistemleri Denetim Rehberi. Ankara, Türkiye: Sayıştay.

Tığdemir, S. (2014). Coso 2013'ün Yol Haritası. KPMG GÜNDEM, 24.

TS ISO/IEC 27001. (2013). TS ISO/IEC 27001. ISO/IEC.

TS ISO/IEC 27002. (2013). Bilgi Güvenliği - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri. ISO/IEC.

TÜBİTAK BİLGEM. Ulusal Bilgi Güvenliği Kapısı. <http://www.bilgiguvenligi.gov.tr>

Türkiye İç Denetim Enstitüsü. < https://www.tide.org.tr/>

Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü. TÜBİTAK BİLGEM. < http://uekae.bilgem.tubitak.gov.tr