Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği

Volkan Evrin [1, 2] Mehmet Demirer [1, 3]

[1] Bilişim Hukuku Tezsiz Yüksek Lisans Programı, Hacettepe Üniversitesi, Ankara
[2] Bilgi Teknolojileri Direktörlüğü, KAREL Elektronik A.Ş., Ankara
[3] Elektrik-Elektronik Mühendisliği Bölümü, Hacettepe Üniversitesi, Ankara

[1] e-posta: volkan@evrin.net [2] e-posta: mehmet@hacettepe.edu.tr

Özetçe

Kurumların faaliyet konularında Bilgi Güvenliği başlığı ile karşılaştıkları sorunlarda süreç yönetimi yapılarından faydalanmaları artık doğal bir sonuç haline gelmiştir. Her kurumun kendi faaliyet alanına ve çalışma kültürüne uygun bir süreci seçmesi ve onun gereklerini yerine getirerek bu çalışmalarını sertifikalandırması mümkündür.

Finans ve savunma sanayisi gibi özel konular dışında kalan sağlık, haberleşme, üretim, Ar-Ge vb. pek çok sektör için ISO/IEC 27000 ailesi, Bilgi Güvenliği Yönetim Sistemi olarak genel kabul gören süreç yönetimidir. Kurumların bu süreç yönetimini bünyelerinde uygulamaları ve ISO/IEC 27001 çalışmalarını tamamlayarak belgelendirmeleri, iyi bir planlama, kapsam belirleme, risk analizi ve varlık değerlendirmesi sonucunda olmaktadır.

Bilgi Güvenliği Yönetim Sistemi, sadece bir belgelendirme değil, aynı zamanda kurumlar için çalışma kültürü haline gelmesi gereken bir süreç yönetimidir.

Anahtar Sözcükler: ISO/IEC 27000 Standart Ailesi, ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemi, BGYS, Süreç Yönetimi, Bilişim Hukuku

1. Giriş

Dünya tarihi büyük devrimlerin, keşiflerin ya da bilimsel olayların açtığı ve kapadığı çağlarla bölümlendirilmektedir. Taş devirlerinden başlayarak gelen bu sınıflandırma, 20. yy. son çeyreğinden itibaren yaşadığımız zamanı "*Bilgi Çağı – Information Age*"[1] olarak adlandırmaya başlamıştır. Bunun temel nedeni de iletişim ve bilişim teknolojilerinin çok hızlı gelişmesi ve hayatımızın her alanına girmiş olmasıdır. Bir bilgi ya da teknolojinin ortaya çıkması ile Dünya üzerinde en uzak köşeye kadar ulaşması ve yayılması için özel bir çabaya gerek kalmamıştır. Sanal dünyada ve İnternet ortamında bilginin dolaşması bağlamında coğrafi uzaklıklar ve fiziksel sınırlar artık bir anlam ifade etmemektedir. *"Bilgi"* artık her yerdedir.

Bilgi'nin değeri arttıkça ona sahip olma motivasyonu ve sahip olduktan sonra sağladığı güç de çok artmıştır. Sadece toplumlar ve devletler değil, tüm kurumlar ve hatta bireyler de bu gücün farkındadır ve "*Bilgi*"ye sahip olmak için günümüz teknolojilerinin araçlarını kullanmak istemekte ve kullanmaktadır[2]. Bu yaygın kullanım ve güce sahip olma güdüsü "*Bilgi Güvenliği*" kavramını da yanında getirmiştir. Bilgiye erişmek ne kadar değerli ise onu korumak ve ifade ettiği değerin sahibi olmak da bir o kadar önemlidir.[3] Kişisel bilgilerin mahremiyetinden kurumların ticari sırlarına kadar uzanan bu geniş bilgi yelpazesi, bireylerin İnternet, sosyal medya, iletişim araçları ve küresel bilgi paylaşım ve erişim ortamlarının değerini yadsınamaz şekilde en üst düzeye çıkarmıştır. Artık bireyler, kurumlar, toplumlar ve tüm devletler, sahip oldukları maddi ve manevi klasik değerlerinin yanına Bilgi Çağı'nın getirdiği yenilikleri ve değerleri de eklemek zorundadır.

21. yüzyılda çok hızlı ilerleyen ve gelişen iletişim teknolojileri ve bilişim altyapıları beraberinde küresel bir bilgi ortamının oluşmasını sağlamıştır. Kimse bu çemberin dışında kalmak istememektedir.[4] Fakat diğer yandan da bu kıymetli veriler ve taşıdığı bilgi değerleri, öncelikli ve hassas koruma gerektiren bir konuma gelmiştir. Bu süreçte Bilgi Güvenliği kavramları da aynı hızla gelişmeye başlamıştır. Bunun bir diğer gerekçesi de suç kavramının evrimleşmesidir. Gerek eski yöntemlerin modern araçlar ile kullanılmaya devam etmesi gerekse yeni suç tanımlarının ortaya çıkması, herkesin bilgiye güvenli erişme ve sahip olduğu bilginin değerini koruma aşamasında daha dikkatli ve donanımlı olmasını gerektirmiştir.[5]

2. Süreç Bazlı Standartlar ve Düzenlemeler

Toplumlardaki bilgi çağı ihtiyaçları İnternet'in ve iletişim araçlarının sağladığı olanaklarla gelişirken, devletler de kendi hukuk ve kamu düzenlerinde bu yeniliklerin gereklerini yapmaktadırlar. Bireyler bu aşamada devletlerin ve toplumların bu yeni çağa ayak uydurmaları için kendi talepleri ile ortaya çıkmakta, ama her zaman istediğini de

[1] Wikipedia. *Information Age. Erişim: 11.09.2011*

[2] Devlet Planlama Teşkilatı Müsteşarlığı (DPT), (2010). *Bilgi Toplumu İstatistikleri.* (s. 4-19)

[3] Pekel, A., (2010). *Bilişim Teknolojilerinde Yönetişim.* (s. 5-7)

[4] "Ürettiği bilgi ve geliştirdiği teknolojileri, ülke ve insanlığın yararına yenilikçi ürün, süreç ve hizmetlere dönüştürebilen Türkiye" vizyonu ile TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010) tarafından yayınlanan "*Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016"* belgesi, ülkemizin bu süreçte aktif olabilmek için yapmak istediklerinin çerçevesini çizmektedir.

[5] Ünver, M., Canbay, C., Mirzaoğlu, A.G., (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* (s. 3-20)

alamamaktadır. Yeni kavramlar, yeni teknolojiler ve yeni yaşam şartlarına uyum sağlayabilen devletler ve toplumlar, Bilgi Çağı'nın nimetlerinden daha verimli ve sağlıklı olarak yararlanabilmektedir. Bu sürece ayak uyduramayan diğer aktörler ise küreselleşmenin dışında kalmamak adına garip bir devinimle kendilerine özel bilgi çağı değerlerini üretmektedir.

Gelişen bu altyapılar ve iletişim gücü, kurumların da yaşam döngülerinde çok önemli noktalara yerleşmeye başlamıştır. Özellikle, bilgi üreten, bilgi ile üretim yapan, hizmet götüren, finansal ve kamusal değerler ile faaliyet gösteren kurumların öncelikli olarak Bilgi Güvenliği kavramlarına uyum sağlaması gerekmektedir.[1, 2] Bilgi güvenliği süreçlerini kendi içinde özümsemeli ve kurumsal kültürünün bir parçası haline getirmelidir. Devletler bazı özel konumdaki kurumlara bunu kanuni bir zorunluluk olarak getirmekle birlikte, kurumlar da kendi değerlerini korumak ve faaliyet alanlarında öne çıkmak adına bu süreçlerden faydalanmaktadır.[3, ,4, 5]

Bilgi Güvenliği çalışmalarına başlamadan önce sorulması gereken en önemli sorulardan biri ne tür bir süreç çalışmasının yapılacağı, hangi standart ailesinin seçileceği ve bu uygulamaların hangi kapsamda ele alınacağıdır.[6] Finans sektöründe BDDK'nin getirdiği yasal mevzuat nedeni ile genel kabul gören sistem COBIT olmuştur.[7] Doğal olarak da onun çevresinde yerleşik durumda olan Risk IT, Val IT, ITAF gibi destekleyici süreç yönetimleri de öncelikli durumdur.[8] Bunların yanında SOX süreçleri de finansal aktörlerin tercihleri arasında yer almaktadır. Bu sektördeki firmaların, kendi tercihleri ile seçecekleri farklı organizasyon yapıları, resmi denetleme mekanizmaları devreye girdiğinde yetersiz ya da zayıf kalabilir.[9]

Müşteri ve son kullanıcılara dönük hizmet götüren firmaların da tercihi genelde ITIL üzerinden gitmektedir.[10] Burada, BT Hizmet Yönetimine dönük çalışmalar doğrudan faaliyet alanına katkı sağladığı için de geri dönüş hızının daha yüksek olması beklenmektedir. Bu yapı, süreç yönetimi talep eden ile hizmet götüren arasındaki uzun ilişki düzeninin temel kurallarını ve detaydaki çalışmalarını düzenlemektedir. Bilgi güvenliği süreçlerini iyi çözmüş bir yapıda eğer müşteri kavramı zayıf işlenirse, hizmet sektörünün süreç yönetiminin temelden aksaması kaçınılmaz olacaktır.

Proje tabanlı çalışan kurumlarda, PMI'nın PMBOK yapısı ve PRINCE2 çerçevesi ya da CMMI seviyesinde süreç çalışmaları ağırlık kazanabilmektedir. Bu yapıların firma kültürü içinde kullanılabilir olması için organizasyon yapısının proje yönetimine yatkın olması beklenmektedir. Zira yatay ya da dikey organizasyon şemalarında, proje yönetimi, kaynak kullanımı, üst - ast ilişkileri ve performans yönetimleri konusunda ciddi sorunlar olacaktır.

Askeri ve savunma sanayisinde çok gizli yapıdaki çalışmalarda zaten yapılacak süreç çalışmaları ve sağlanması gereken belgelendirmeler bellidir. Yapılacak çalışmalar bu süreçleri kurumun yeterliliği haline getirmektir.

Bilgi Güvenliği anlamında finans, savunma ve hizmet sektöründeki özel durumlar dışında, Sağlık, Haberleşme, Bilgi Teknolojileri, Tasarım, Ar-Ge, Üretim, gibi ana faaliyet konularında pek çok firmanın ihtiyacını karşılayacak Bilgi Güvenliği Süreç Yönetimi sistemi ISO/EIC 27000 ailesi olacaktır.[11] Gerek bilgi güvenliği süreçlerini tam karşılaması gerekse destekleyici diğer standartlar ile eksik nokta bırakmaması, bu süreç yönetimini popüler kılmaktadır. Buna ek olarak, kapsam belirlemede bu süreç ailesinin daha esnek olması da karar verme, planlama ve uygulama aşamasında büyük avantajlar sağlamaktadır.[12] Ayrıca, süreç çalışmalarında dış kaynak kullanımı ve danışmanlığın çok önemli olduğu da düşünüldüğünde, kapsamı, uygulama metodolojisi ve referansları olabilecek bir sertifikasyon, süreç çalışmalarını olumlu yönlerden destekleyecektir.[13]

1947 yılında kurulan Uluslararası Standardizasyon Organizasyonu (*International Organisation for Standardisation – ISO*) Uluslararası geçerlilikte standartlar konusunda çalışan bir kurumdur. Ayrıca, Bilgi Güvenliği ve süreçleri konusunda Uluslararası Elektroteknik Komisyonu (*International Electrotechnical Commission - IEC*) ve Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union - ITU*) Bilgi ve İletişim Teknolojileri (*Information and Communications Technology - ICT*) kurumları ile işbirliği yapan hükümetler dışı bir uluslararası organdır. Aşağıda yaygın olarak kullanılan ISO güvenlik standartlarının başlık tanımları vardır:

•ISO/IEC 27000 — Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Tanımlar

•ISO/IEC 27001 — Bilgi Güvenliği Yönetim Sistemleri - Gereklilikler

•ISO/IEC 27002 — Bilgi Güvenliği Yönetim Sistemleri - Uygulama Kuralları

•ISO/IEC 27003 — Bilgi Güvenliği Yönetim Sistemleri - Uygulama Kılavuzu

•ISO/IEC 27004 — Bilgi Güvenliği Yönetim Sistemleri - Ölçme

[1] TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010). *Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016.* (s. 4-6)

[2] Ünver, M., Ketevanlıoğlu, M.S., (2010). *Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı.* (s. 37-40)

[3] Pattinson, F., (2007). *Certifying Information Security Management Systems.* (s. 9-10)

[4] Çetinkaya Kılıç, M., Gökçöl, O., (2010). *Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi.* (s. 1, 5)

[5] Pekel, A., (2010). *Bilişim Teknolojilerinde Yönetişim.* (s. 9, 15-17)

[6] *Aynı makale* (s. 7-10, 15-17)

[7] Bankacılık Düzenleme ve Denetleme Kurumu'nun tüm mevzuat bilgileri için bakınız: *Erişim: 11.09.2011* http://www.bddk.org.tr/websitesi/turkce/Mevzuat/Mevzuat.aspx

[8] ISACA, (2010). *COBIT, Val IT and Risk IT — Synergistic Relationship.*

[9] Türkyılmaz, M., (2010). *COBIT® ve Diğer Standartlar ile Karşılaştırılması.* (s. 13-23)

[10] The IT Service Management Forum (2007). *An Introductory Overview of ITIL® V3.*

[11] Çetinkaya Kılıç, M., Gökçöl, O., (2010). *Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi.* (s. 1-3)

[12] Perendi, Ü., (2008). *BGYS Kapsamı Belirleme Kılavuzu.* (s. 6-7)

[13] Ottekin, F., (2011). *BGYS ve BGYS Kurma Deneyimleri.* (s. 25)

•ISO/IEC 27005 — Bilgi Güvenliği Risk Yönetimi

•ISO/IEC 27006 — Bilgi Güvenliği Yönetim Sistemleri'nin Denetim ve Belgelendirme işlerini sağlayan kuruluşlar için şartlar

•ISO/IEC 27011 — ISO/IEC 27002'ye göre telekomünikasyon kuruluşları için bilgi güvenliği yönetim kuralları

•ISO/IEC 27031 — İş sürekliliği için bilgi ve iletişim teknolojisi hazırlık rehberi

•ISO/IEC 27033-1 — Ağ güvenliği genel bakış ve kavramlar

•ISO 27799 — ISO/IEC 27002 ile Sağlıkta Bilgi Güvenliği Yönetimi

Hazırlık Aşamasında olan belgeler:

•ISO/IEC 27007 — Bilgi Güvenliği Yönetim Sistemleri Denetimi Rehberi (yönetim sistemi odaklı)

•ISO/IEC 27008 — BGYS denetçileri (bilgi güvenliği denetimleri odaklı) için rehber

•ISO/IEC 27013 — ISO/IEC 20000-1 ve ISO/IEC 27001 bütünleştirme çalışmalarına ilişkin kılavuz

•ISO/IEC 27014 — Bilgi Güvenliği Yönetim Çerçevesi

•ISO/IEC 27015 — Finans ve sigorta sektörleri için bilgi güvenliği yönetim kuralları

•ISO/IEC 27032 — Siber Güvenlik (temelde, İnternet'te 'iyi bir komşu olmak' için rehber)

•ISO/IEC 27033 — BT Ağ Güvenliği, ISO/IEC 18028:2006'ya dayalı çok parçalı standart (Sadece Bölüm 1 yayınlandı)

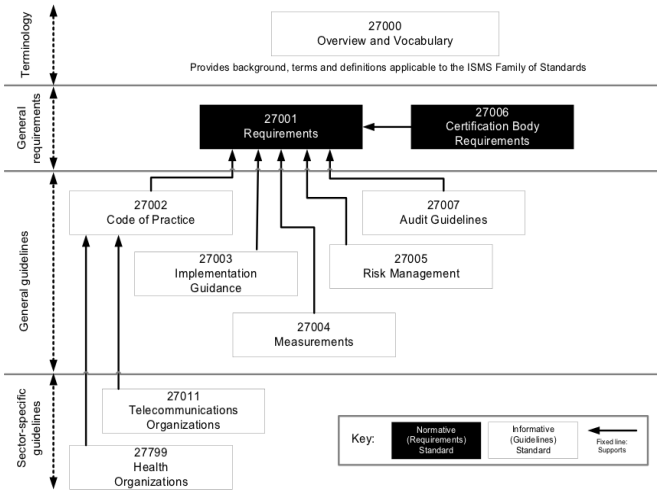
•ISO/IEC 27034 — Uygulama Güvenliği Rehberi

•ISO/IEC 27035 — Güvenlik Olay Yönetimi

•ISO/IEC 27036 — Dış Kaynak kullanımı için güvenlik rehberi

•ISO/IEC 27037 — Tanımlama, toplama ve / veya satın alma ve dijital kanıt korunması rehberi

ISO/IEC 27000:2009 : Information Security Management Systems — Overview and Vocabulary - Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Tanımlar: BGYS Standartlar ailesi, bazıları hali hazırda yayınlanmış veya geliştirme aşamasında olan ve birbiriyle yakın ilişkili standartlardan oluşur (Şekil 1). Bu belgeler süreçlerle ilgili önemli yapısal bileşenleri içerir. Bu bileşenler BGYS gereksinimlerini (ISO/IEC 27001) ve bunları belgelendirecek kuruluşun gerekliliklerini (ISO/IEC 27006) açıklamaya odaklanmış kural koyucu yapılardır. Diğer standartlar da bir BGYS için gerekli olan uygulama yönleri, kontrol ile ilgili kurallar ve sektöre özel rehberlik gibi çeşitli başlıkları açıklar.



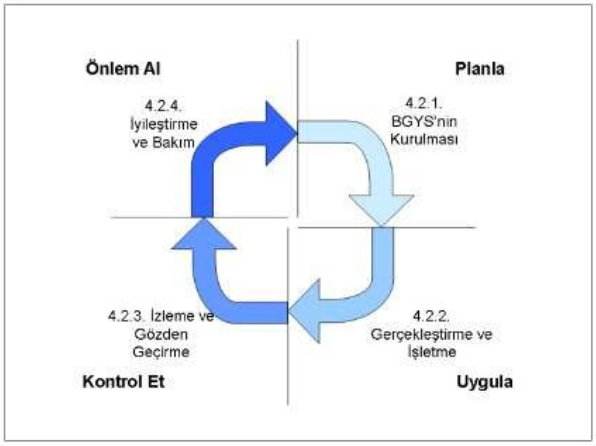
Şekil 1: ISO/IEC 27000 Standartlar Ailesi [1]

ISO/IEC 27001:2005 : Information Security Management System – Requirements - Bilgi Güvenliği Yönetim Sistemleri için Gereklilikler: Uluslararası bir standart olan ISO/IEC 27001:2005, köklerini bir *British Standards Institute* (BSI) standardı olan BS7799 Bölüm 2:2002'den elde edilen teknik içerikten türetilmiştir.[2] Bu standart, bir organizasyon içinde belgelenmiş bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak, uygulamak, işletmek, incelemek, sürdürmek, geliştirmek ve izlemek için gereksinimleri belirtir.[3] Ayrıca, bilgi varlıklarını korumak için yeterli ve uygun güvenlik kontrollerinin seçimini sağlamak için tasarlanmıştır. Bu standart, genellikle her türlü ticari şirketler, kamu kuruluşları, vb. kuruluşlar için uygulanabilir. Standart bir kuruluşun BGYS etkinliğini artırmak amacı ile "Planla – Uygula - Kontrol Et - Önlem al (PUKÖ)" modeli olarak bilinen bir döngüsel model oluşturmaya yardım eder. PUKÖ döngüsünün dört aşaması vardır (Şekil 2):

[1] ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. (s. 12)

[2] ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements. (s. iv – vii, 1)

[3] Taşkın, E., (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. (s. 3-4)



Şekil 2: BGYS için temel PUKÖ döngüsü.[1]

ISO/IEC 27001:2005 çoğu zaman ISO/IEC 27002:2005 ile birlikte yürütülmektedir. ISO/IEC 27001 BGYS bilgi güvenliği gereksinimlerini tanımlar ve BGYS için en uygun bilgi güvenliği denetimleri için de ISO/IEC 27002'deki ana hatları kullanır. ISO/IEC 27002, bir kuruluşun bilgi güvenliği risklerine uyum sağlaması için önerilen ve kontrol sağlayan basamaklardır. Bu kontroller zorunlu değildir. Yine de bir kurum ISO/IEC 27001 ile uyumlu sertifika almak isterse bu belgeden kesinlikle yararlanmalıdır. Belgelendirme işlemleri uluslararası geçerlilikte akredite olmuş belgelendirme kuruluşları aracılığı ile genelde bu yönetim başlıklarındaki kontrollerle yapılmaktadır.[2]

ISO/IEC 27002:2005 : Code of Practice for Information Security Management - Bilgi Güvenliği Yönetim Sistemleri için Uygulama Kuralları: Temeli *British Standards Institute* (BSI) kökenli ilk uluslararası standart olan BS7799-1'e dayanan bir standarttır (Nisan 2007'de ISO/IEC 17799:2005 yerine yayınlandı).[3] ISO/IEC 27002:2005, Bilgi güvenliği yönetimi için uygulanabilir gereklilikler anlamına gelir ve kuruluşlar için güvenlik standartları ve etkin yönetim uygulamaları geliştirmek için ortak bir temel rehber niteliğindedir.[4]

Bu standart, aşağıdaki 10 güvenlik etki alanı için kurallar ve en iyi uygulamalar için öneriler içermektedir: (a) güvenlik politikası; (b) bilgi güvenliği organizasyonu; (c) varlık yönetimi; (d) insan kaynakları güvenliği; (e) fiziksel ve çevresel güvenlik; (f) iletişim ve operasyon yönetimi; (g) erişim kontrolü; (h) bilgi sistemleri satınalma, geliştirme ve bakım; (i) bilgi güvenliği olay yönetimi; (j) iş sürekliliği yönetimi ve (k) uygunluk.

[1] Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. (s. 14)

[2] 28.09.2009 itibariyle ülkemizde 14 adet kuruluş TS ISO/IEC 27001 belgesi almıştır. (Kaynak: Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. (s. 14)). 25 Haziran 2010 tarihi itibari ile de bu sayı 18 olmuştur (Kaynak: Ergin, H., (2010). TSE Bilgi Güvenliği Belgelendirme, s. 26)

[3] ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management. (s. vii)

[4] Ottekin, F., (2011). BGYS ve BGYS Kurma Deneyimleri. (s. 3-4)

Bu 10 güvenlik etki alanı arasında, 39 kontrol hedefi ve en iyi uygulamalar için bilgi güvenliği kontrol önlemlerini içeren yüzlerce denetleme amaçlarını ve gizlilik, bütünlük ve kullanılabilirlik için tehditlere karşı bilgi varlıklarını korumaya yönelik tavsiyeler vardır.

3. ISO/IEC-27001 Süreç Çalışmaları

Bilgi Güvenliği Yönetim Sistemi (BGYS), kuruma ait kritik bilgi varlıklarının güvenliğini sağlamak amacıyla etkin risk yönetimi ile belirlenen güvenlik kontrollerinin uygulanmasına ve bu kontrollerin sürekli iyileştirilmesine dayanan bir yönetim sistemidir. Bir kurumun bilgi güvenliği anlamında bir süreç çalışmasının içine girmesi için mutlaka kötü bir senaryonun yaşanmasını beklememelidir. Faaliyet gösterdiği alanda kendisi için önemli bilgi ve çalışmalar varsa, bir an önce gerekli süreç disiplinini kurmak için çaba harcamalıdır. Bu süreç, haberleşme, sağlık, finans, Ar-Ge, savunma sanayisi gibi bilginin çok değerli olduğu sektörlerde devlet tarafından da mecburi hale getirilebilir. [5], [6] O yüzden de ciddi bir kurum, hukuki mecburiyetlerden önce kendi kararı ve iradesi ile bu çalışmalara başlamalı ve faaliyet konusunda en uygun süreç sertifikasyonlarını tamamlamalıdır.

3.1. Organizasyon ve Başlangıç

BGYS çalışmalarının başlayabilmesi için öncelikle bir kapsam çalışması yapılmalıdır.[7] Burada kurumun hangi faaliyet konularının, hangi yerleşkelerinin, hangi bölümlerinin ve hangi süreçlerinin bu yapıya dahil olacağının belirlenmesi gerekmektedir. Tanımı düzgün yapılmayan bir çalışmanın, ilerleyen süreçlerinde mutlaka eksikler veya zorluklar çıkacaktır. Bu aynı zamanda, süreç çalışmalarının planlamasında, bütçe ve iş gücü hesaplamalarında, çalışma ekiplerinin kurulmasında, belgeleme çalışmalarının ve takvimin belirlenmesinde de çok önemli bir adımdır.[8]

Kapsamı belirlenmiş bir BGYS çalışmasının karar aşamasında olması gereken bir ön şartı da Üst Yönetim'in desteğidir. Kurum yöneticilerinin, bu çalışmaların kurumsal bir ihtiyaç olduğunu, mecburiyetten değil, gereklilikten yapılması gerektiğini kabul etmesi ve alt kadrolarına bu mesajı ve kararlılığını net bir şekilde iletmesi gerekmektedir. Çünkü, sürecin en zorlu aşamalarında, gerek çalışanların motivasyonu gerekse zorlukların aşılmasında bu kararlılık anahtar rol oynayacaktır.[9]

ISO/IEC 27000 ailesi için çalışmaların başlangıcı, bu sürecin uzun soluklu bir çalışma olduğunu kabul etmekle başlayacaktır. Ve daha önemlisi, çalışmalar başarılı bir şekilde sonlandığında, ikinci perde başlayacaktır. O da bu sürecin kurum kültürü olarak sürekli yaşayacağı ve gelişeceği

[5] *Elektronik Haberleşme Kanunu* (2008).

[6] *Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri Ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik* (2010).

[7] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 5, 11)

[8] Taşkın, E., (2010). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi.* (s. 3-4, 9-12)

[9] Ottekin, F., (2011). *BGYS ve BGYS Kurma Deneyimleri.* (s. 19)

aşamadır. O yüzden de gerek politikaların belirlenmesinde gerekse süreç çalışmalarında, bir şekilde bitsin, belge alınsın, süreç tamamlansın psikolojisinin oluşmaması gerekir. Bu yapının, kurum aynı konuda faaliyet gösterdikçe ve yaşadıkça devam edecek bir döngü olduğu bilinmelidir.[1] Bu aşamada belirlenmesi gereken bir diğer başlık da süreç içinde görev alacak ekibin ve rollerinin belirlenmesidir. BT ekibi başta olmak üzere süreç tasarım ve yönetim tecrübesi olan Kalite ve İnsan Kaynakları gibi ekiplerden yürütücü roller için elemanlar seçilmelidir.

Bilgi Güvenliği politikalarının tasarlanması ve belirlenmiş kapsam içinde ortaya konması, BGYS çalışmalarının en büyük adımlarından olacaktır.[2] Bu politikalar, kurumun Bilgi Güvenliği anayasası olacağı için olması ve olmaması gereken temel ilkelerin, faaliyet konularının ve süreçlerinin hangi hedeflere yoğunlaşması gerektiğinin ortaya konacağı belgelerdir. Kapsaması gereken temel konular itibari ile tek bir belge olarak da yazılabilir. Hiyerarşik olarak birbirini destekleyen temel konuları başlık olarak seçen bir belge kümesi de hazırlanabilir.

BGYS için yapılacak çalışmaların kapsam, politika, kaynak planlama, çalışma takvimi ve ekip organizasyonu Üst Yönetim ile paylaşılmalı ve onların da görüşleri alınmalıdır. Temel çerçeve program ortaya çıktıktan sonra mutlaka orta ve üst kademe yöneticilerinin de görüşleri alınmalı ve süreç hakkında onlara da detaylı bilgiler aktarılmalıdır. Zira çalışmaların sağlıklı başlaması ve kurum çalışanları tarafından benimsenmesinin ilk adımı yönetim kadrolarının bu çalışmanın önemini ve gereğini kabul etmesi ile başlayacaktır. Süreç çalışmaların resmi bir açılışı mutlaka yapılmalıdır. Bu hem kurum içinde tüm çalışanların bilgilenmesi hem de çalışma ekibinin motivasyonu açısından önemli bir aşamadır.

3.2. Varlık Envanteri Oluşturma ve Risk Yönetimi

Varlık, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır.[3] İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir.

Bilgi güvenliği açısından bir donanımın bütünlüğünden söz etmek çok zordur. Bu sebeple asıl korunması ve yönetilmesi gereken bilgi veya süreçleri değerlendirmek, ardından bu bilgi ve süreçleri sağlayan veya barındıran donanım ve yazılımı güvenlik açısından incelemek ve sınıflandırmak daha kolay olacaktır. Diğer varlıklar düşünüldüğünde (yazılım, donanım, fiziksel varlıklar ve insan) bilgi ve süreçler en soyut kavramlardır ve güvenliğin üç temel öğesi (gizlik, bütünlük, erişilebilirlik) için derecelendirmenin kolaylıkla yapılabileceği varlık guruplarıdır.[4]

Bir organizasyonda varlıkların belirlenmesi ve varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. BGYS için varlık envanteri hazırlanırken öncelikle, tüm varlıkların kapsandığından emin olmak için gruplandırma yapmak varlıkların tanımlanması işini kolaylaştıracaktır. Bilgi varlıkları, yazılımsal varlıklar, fiziksel varlıklar, servisler vb. bir gruplandırma yapılabilir. Organizasyon içinde bir "varlık yönetim kılavuzu" veya "varlık envanteri yönetim kılavuzu" hazırlanmasında fayda vardır. Bu kılavuzda özellikle envantere yeni bir varlığın eklenmesi, envanterden varlık çıkarılması ve envanter sorumlusu net olarak belirtilmesi gerekir.[5]

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir.[6] Tehdit değerlendirmesi sırasında hiç bir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir. Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir.

Risk, *"zarara yol açan ya da zarar verme kapasitesi olan kişi ya da nesne"* olarak tanımlanmaktadır. Riskin, varlık, açıklık ve tehdit kavramları bağlamındaki bir diğer tanımı da: *"Bir kıymetteki bir açıklığın bir tehdit tarafından kullanılma ihtimalidir."* şeklindedir.[7]

Risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla koruyucu önlemlerin ve maliyetlerinin dengelenmesi ve organizasyonun hedeflerine ulaşması için gerekli kritik sistemlerin korunması gibi konularda BT yöneticilerinin yararlandığı süreçtir. Bu süreç risk analizi, risk işleme ve değerlendirme ve takip alt süreçlerinden oluşur.[8]

3.3. Güvenlik Kontrollerinin Hazırlanması, Uygulanması ve İyileştirme Adımları

BGYS konusunda temel başvuru kaynakları ISO/IEC 27001 ve ISO/IEC 27002 standartlarıdır. BGYS kurulumu öncesinde bu standartların mutlaka dikkatlice okunup anlaşılması gerekmektedir. BGYS kurulumu TS ISO/IEC 27001:2005'teki "4.2.1 BGYS'nin Kurulması" başlıkları altında detaylı olarak açıklanmaktadır.[9]

Risk işleme süreci sonuçlarına göre uygun kontrol ve kontrol hedeflerinin seçilmesi gerekir. TS ISO/IEC 27002:2005'te bu kontrollerden detaylı bir biçimde bahsedilmektedir. Bu kontroller standartta yol gösterici olması amacıyla verilmiştir. Kurum kendisine ek olarak başka kontroller de seçmekte serbesttir. TS ISO/IEC 27002:2005'te bulunan kontroller, sektör tecrübelerinden faydalanmak suretiyle, standart etki

---

[1] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 9-10)

[2] Öztürk, G., (2008). *Bilgi Güvenliği Politikası Oluşturma Kılavuzu* .

[3] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[4] Koç, F., (2008). *BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu.* (s. 6-7)

[5] *Koç, F., (2008). BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu.* (s. 8-9)

[6] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[7] İbrişim, A., (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları.*

[8] Evrin, V., (2011). *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. (s. 38-43)*

[9] *TS ISO/IEC 27001 (Mart 2006). Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler.* (s. 5-7)

alanlarında olabildiğince geniş kapsamlı olarak belirlenmiş olsa da dış kaynaklı kontrollere ihtiyaç olabilmektedir. Sadece TS ISO/IEC 27002:2005'ten değil herhangi bir bilgi güvenliği kaynağından uygun kontrol seçilebileceği gibi kurumun kendine özel geliştirebileceği kontroller de olabilmektedir. Fakat gözden kaçan önemli bir kontrol hedefi veya kontrol olmadığından emin olmak için bu listeyi bir başlangıç noktası olarak kullanmakta fayda görülmektedir.[1]

Bu aşamada yazılı belge hazırlama işleri de tamamlanmalıdır. BGYS'nin kapsadığı alan için gerekli olan politikalar, yönetmelikler, prosedürler, talimatlar ve diğer kayıt amaçlı belgeler gerek kontrol süreçleri içinde gerekse belgelendirme aşamasında kullanılmaya başlanmalıdır.[2]

Son olarak risklere karşı seçilen kontrolleri içeren ve riskin ortadan kaldırılması süreçlerinin sonuçlarına dayanan, denetim hedeflerini ve kuruluşun BGYS'yle ilgili olan ve uygulanabilen denetimleri açıklayan belge olan "*Uygulanabilirlik Bildirgesi*" hazırlanır. Bu belgede seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. Ayrıca, TS ISO/IEC 27001 belgesindeki kontrol listesi olan EK-A'dan seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçeleri de Uygulanabilirlik Bildirgesinde verilmelidir.[3]

Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür. Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir.

Kullanıcılar, bilgi güvenliği bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir.[4] Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir.

Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar. Bilgi güvenliği bilinçlendirme süreci kapsamında ortak sorumlulukları yerine getirmek amacıyla Bilgi Güvenliği Yöneticisi ve Bilgi Güvenliği Bilinçlendirme Süreci Yürütücüsü ile birlikte çalışmaları beklenmelidir.[5]

3.4. Kurum İçi Uyum Çalışmaları

Pek çok firma, BGYS çalışmalarından önce mutlaka farklı başlıklarda ve amaçlarda süreç çalışmalarına kendi bünyesinde yer vermiştir. ISO-9000 Kalite Süreçleri ailesi; Tesis Güvenlik Belgesi; CMMI, PMBOK gibi proje yönetim süreçleri gibi. Bu çalışmalar kurum için başlangıçta ciddi bir avantajdır, zira kurum çalışanlarının yönetmelik, iş akışı, süreç yönetimi, prosedür, talimat gibi kavramlara yakın olması beklenir. Bu başlığın BGYS için ek yükü ise geçmişte hazırlanmış ve halen aktif uygulanan bu tür sertifikasyon sistemlerinin de yeni süreç çalışması içinde gözden geçirilmesi, gerekli bütünleştirme çalışmalarının yapılması ve karşılıklı atıflarda bulunulması gerekliliğidir. Sonuçta, kurum içinde BGYS'nin ISO-9000 süreçlerinden ya da CMMI başlıklarından bağımsız çalışması hem beklenmemesi gereken bir durumdur hem de süreç mantığında olanaksız bir yaklaşımdır. Bu yüzden de kurumun sahip olduğu tüm süreç yönetimleri ve kurumsal uygulamaların BGYS içinde yer bulması ve kapsamı dahilinde karşılıklı atıflarda bulunulması gereklidir.

Bir kurum da zaman içinde gerek yönetimin oluşturduğu gerekse çalışanların yaşama geçirdiği bir firma kültürü vardır. Bu yerleşik kültür, kurumun yeni bir süreç çalışmasında duruma göre olumlu ya da olumsuz etkiler yapabilir. Yeniliğe açık, paylaşımcı ve iş birliği yapmaya yatkın yöneticilerin ve çalışanların olduğu bir kurumda BGYS gibi zorlu süreçlerin hayat bulması nispeten daha kolaydır. Bu yapının kurum için ne kadar önemli ve gerekli olduğu, bu bakış açısındaki insanlara daha çabuk gösterilebilir ve benimsetilebilir. Aksi durumlarda, her çalışan bu süreçleri, yeni bir külfet, çalışma hayatına ek yükler, özgürlüklerin kısıtlanması gibi algılayacaktır. Bu da sürecin toplam başarısında ciddi sorunlara neden olacaktır. Bu nedenle gerek BGYS'nin tanıtım, tasarım ve uygulamalarında ölçülü ve dengeli politikaların yürütülmesi, gerekse hem yönetimin hem de çalışanların tüm süreçlere sahip çıkmasını sağlayacak bilgilendirme ve empatinin sağlanması gereklidir.

BGYS çalışmalarında her bölüm ya da birim sürece katkı yapmaktadır. Fakat en önemli ekipler BT, Kalite ve İnsan Kaynakları gibi süreç yönetimlerine yakın konularda çalışan birimlerin çalışanlarından oluşmaktadır. Onların Bilgi Güvenliği farkındalığı ve bilinci konusunda herkesten bir adım önde olmaları ve süreçlere sürekli sahip çıkmaları beklenmelidir. PUKÖ döngüsü içinde oluşacak aksaklıkların ve alınacak aksiyonların ilk adresi bu ekipler olacaktır. Sürecin sorgulanması, farklı bakış açıları ile iyileştirilmesi ve geliştirilmesi yine bu ekiplerin önceliğinde olmalıdır.

3.5. Bilişim Hukuku'nun Süreçler ile Bütünleştirilmesi

Bilgi Güvenliği doğası gereği, varlıkları ortaya koymak, riskleri ve tehditleri tespit etmek, gerekli önlemleri hem gerçek ortamlarında almak hem de yazılı belgeler ile bunları somutlaştırmak durumundadır. Bilişim sistemlerinin kullanılması, bunların belli kural ve kontrollere tabi tutulması, "*bilgi*"nin korunması süreçlerinde kurumun ve çalışanlarının karşılıklı olarak haklarının korunması, ihlal edilmemesi şarttır. Doğal olarak bu süreçlerin tamamının yürürlükteki hukuk mevzuatı ile de uyumlu olması gereklidir. Bunun sağlanması için de dengeli bir politika hazırlanmalı ve tüm çalışanlar ile paylaşılmalıdır.

Bilişim sistemlerinde ve hizmetlerinde teknik bilgiler, hukuk mevzuatında neyin suç olabileceği ve neyin normal davranış olabileceği, hangi kanunların hangi konularda kurumlara veya çalışanlara haklar ve ödevler verdiğinin tüm yöneticiler ve

[1] Önel, D., Dinçkan, A., (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* (s. 7-11)

[2] Evrin, V., (2011). *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği*. (s. 46-47)

[3] Ottekin, F., (2008). *ISO/IEC 27001 Denetim Listesi.* (s. 6-58)

[4] Önel, D., (2008). *Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu.* (s. 9)

[5] *Aynı makale* (s. 8)

çalışanlar tarafından bilinmesi için Bilgi Güvenliği farkındalık eğitimleri düzenli olarak yapılmalıdır.[1] Bu eğitimlerde kullanıcılara BGYS süreçlerinin hangi amaca hizmet ettiği, hangi değeri ne için ve nasıl koruduğunun aktarılması ana hedef olmalıdır. Zira, bilişim ve iletişim sistemlerinin bu kadar hızlı geliştiği bir dönemde yönetici ve çalışanlar, yapması ve yapmaması gereken işlemleri bütün gerekçeleri ile bilmelidirler.[2, 3] Ancak bu şekilde BGYS sahibi kurumların çalışanları daha bilinçli olabilirler.

Bilişim hukukuna konu olan çalışmaların iki temel bakış açısı ile yapılması gerekecektir. Birincisi kurum yönetiminin gözüyle, diğeri de çalışanların hakları ve ödevleri başlıklarıyla. Kurum, sahip olduğu varlıkları korumak, bundan en yüksek faydayı sağlamak ve bunu da uzun süre devam ettirmek ister. Bu yüzden de gerek bilgi güvenliği gerekse firmanın temsil ettiği kurumsal kimliğin zarar görmemesi için önlemler alır. Devletin çıkardığı her kanun ya da yönetmelik ilgi alanına göre kurumlara yeni görev ve sorumluluklar getirebilir. Kurum tarafından tahsis edilen ve kullandırılan her teknoloji beraberinde özel yükümlülükler yaratıyor olabilir. Bu nedenle de kurum tarafından sağlanan her bilişim sisteminin ve hizmetinin kurallarının BGYS kapsamında tanımlı olması gerekmektedir. Neyin, hangi amaçla, nasıl ve ne zaman kullanılacağı bilinmelidir. Böylece, çalışanlar BGYS'nin kendilerine sunduğu olanakları ve çizdiği sınırları da bilerek çalışacaklardır. Ayrıca, denetleme yöntemlerinin ve şekillerinin de açıkça ortaya konması gerekmektedir. Bu bilgiler ve süreçler eski yeni fark etmez tüm çalışanların bilgisi dahilinde olmalı ve iş sözleşmelerinde özel maddeler ile imza altına alınmalıdır. Aynı şekilde, BGYS kapsamı içinde yapılan tüm faaliyetler, çalışanların anayasa ve kanunlardan gelen temel haklarını ve kişisel mahremiyetlerini de korumalıdır. Keyfi uygulamaların, önceden tasarlanmamış ya da duyurulmamış önlem veya denetimlerin mümkün olmaması gerekmektedir. BGYS, kurumun değerlerini, bilgisini, kurumsal kimliğini ve varlıklarını korurken aynı şekilde çalışanların da kişisel haklarını ve özel hayatlarını korumalıdır. Zira, çalışanlar da kurumun en değerli varlıkları arasındadır.

Gelişen ve ilerleyen düzenlemeler içinde Devlet eli ile yeni kanunlar ve yönetmelikler çıkarıldıkça BGYS'nin de buna uyum sağlaması gereken noktaları olacaktır. Bu çalışmalar da yine kurumsal çatı altında yapılmalı ve çalışanlar da yeterli şekilde bilgilendirilmelidir. Ayrıca BT konularında yeni çıkan teknolojiler, tehditler, kurum için zararlı olabilecek konular ve tehlikeler ortaya çıktıkça, aynı şekilde BGYS altyapıları yeniden gözden geçirilmeli ve çalışanlara gerekli teknik bilgiler düzenli olarak aktarılmalıdır. Bu da hem hukuki düzenlemeler açısından hem de teknolojik gelişmeler açısında kurum çalışanlarının, güncellenen BGYS süreçleri konusunda periyodik olarak bilgilendirilmelerini ve farkındalık düzeylerinin hep yukarıda tutulmasını sağlar.

[1] *Önel, D., (2008). Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu.* (s. 14-21)

[2] Eralp, Ö., (2010). *Bilgi İşlem Merkezi Yöneticilerinin Hukuki ve Cezai Sorumluluğu.*

[3] Tanrıkulu, C., (2011). *Bilgi Sistem Yöneticilerinin Hukuki Yükümlülükleri.*

3.6. Belgelendirme Çalışmaları

Bir kurum BGYS çalışmalarını genelde sertifikasyon hedefi ile yapar. Bu yüzden de önceden yaptığı tüm çalışmaları akredite edilmiş bir kuruma denetlettirerek onaylatmak zorundadır. Belgelendirme çalışmaları, Türkiye'de TÜRKAK tarafından akredite edilmiş bir kuruluşa yapılacak başvurunun alınması ile başlar.[4]

Dünya çapında organizasyon hiyerarşisi şu şekilde alt başlıklara ayrılabilir:

IAF - Uluslararası Akreditasyon Forumu gibi en üst çatı organizasyonu

EA gibi Bölgesel/Kıtasal Akreditasyon Forumları

TÜRKAK gibi Ulusal Akreditasyon Kurumları

TSE, KALİTEST gibi Belgelendirme Kuruluşları[5]

TÜRKAK, Türkiye'de tek yetkili akreditasyon kurumudur. IAF *(International Accreditation Forum)* ile MLA (*Multi Lateral Agreement*) anlaşması vardır. Bu, TÜRKAK akrediteli belgelerin dünyada tanınması anlamındadır. Türkiye'de üretim / hizmet sunan bir firmanın TÜRKAK akrediteli belgelendirme kuruluşundan belge alması, uluslararası akreditasyon kurallarının istediği bir durumdur. Çünkü belgeli firmadan hizmet alan tüketici, belgeyi veren kurum, akreditasyon kurumu vb. ilgili kuruluşlar zincirinin güven ve izlenebilirliği sağlanmalıdır.

Seçilen Belgelendirme Kuruluşunun seçimi ve değerlendirmesinde başlıca dikkat edilmesi gereken noktalar:[6]

•TÜRKAK tarafından verilmiş bir akreditasyona sahip olup olmaması,

•Dış akreditasyona sahip ise bu akreditasyonun Türkiye'yi kapsayıp kapsamadığı,

•Sertifikanın üçüncü taraflar tarafından kabul görüp görmediği,

•Belgelendirme kuruluşunun görevlendirdiği denetçilerin yetkinliği,

•Tarafsızlık ve bağımsızlığın sağlanması

•Danışmanlık ve belgelendirme ilişkisi (ISO 17021 şartları)

•Denetim ekibinin (baş denetçi ve denetçilerin) denetlenen kuruluştan bağımsız olmaları

•Belgelendirme kuruluşunun danışmanlık şirketi ile çıkar ilişkisinin olmaması (komisyon alma verme gibi)

Kurumun ISO/IEC 27001 sertifikası almak için yaptığı başvuru Belgelendirme Kuruluşu tarafından incelenir. Yeterli görülürse kurum ile belgelendirme kuruluşu arasında bir sözleşme imzalanır. Bu aşamadan sonra çalışmalar resmen başlamış olur. Bu adımı sırası ile 1. Aşama denetimleri; 2.

[4] Köse, O., (2010). *ISO/IEC 27001 Denetim ve Belgelendirmesi.* (s. 7)

[5] *Aynı makale,* (s. 39)

[6] *Aynı makale, (s. 35-38)*

Aşama denetimleri; Belgelendirme; Gözetim Denetimleri ve Belge Yenileme süreçleri geniş zaman içinde izleyecektir.[1]

4. Tartışma

İster kamu veya özel sektör olsun, isterse devlet ya da birey, Bilgi Çağı'nı yaşarken onun sunduğu yenilikleri, verimlilikleri, avantajları, özgürlükleri ve fırsatları kullanırken, kişisel, kurumsal, toplumsal ve ülkesel olarak bilgi güvenliği kavramlarını ve gereklerini de öğrenmeli ve onu da yaşam kültürü içinde tutmaya çalışmalıdır.

Kurumlar artık her türlü faaliyet alanlarında Bilgi Güvenliği süreçlerini kullanmak zorundadır. Bunu ister sertifika amacı ile yapsınlar ister kurumsal kültür olarak kullansınlar sonuç değişmeyecektir. Ticari başarı doğru zamanda doğru teknolojiyi kullanmak ya da üretmek olduğu kadar, yakın zamanda onu güvenli olarak kullanabilmeye devam edebilmek olacaktır. Çünkü bilgiye sahip olan ve bilgiyi doğru ve güvenli olarak kullanabilenlerin çağını yaşıyoruz. Bu yarışın içinde olmak isteyen her kurum, BGYS tarzı süreç yönetimleri bünyesinde kullanmak zorundadır.

Dikkat edilmesi gereken bir diğer öge de bu süreçlerin robotlaşmış yapılar ve kişiler tarafından kullanılmadığının bilincinde olmaktır. Kurumlar, çalışan süreçlerini tasarlarken ve uygularken, bunlarla beraber yaşayan çalışanlarının da haklarını ve mahremiyetlerini öncelikler listesinin üstlerinde tutmalıdır. Çalışanların sahiplenmediği hiç bir süreç bir kurum içinde uzun süre yaşayamaz. Yaşasa bile verimli olamaz. Çalışanlar da kendilerine sürekli zorluklar çıkartan, ama hiç bir katma değer sunmayan süreçleri kabullenmezler. Burada kurum çıkarları ile çalışan memnuniyetinin dengesini yakalamak zordur, ama çok önemlidir.

5. Sonuçlar

Bilgi Güvenliği'ni artık hayatımızın her aşamasında teknolojiyi ve iletişim sistemlerini kullanırken hissedeceğiz. Bu da çevremizdeki Bilgi Çağı aktörlerinin iyi tanınmasını ve amacına uygun kullanılması gerekliliğini tartışmasız olarak bize öğretecektir.

BGYS'nin sadece bir belge olmaması ve firma içinde yaşayan bir kültür olması da gerekmektedir. Gerek kurum yöneticileri gerekse çalışanlar bu bilinçle ve yaklaşım ile iş hayatlarını devam ettirmeliler. Sadece belge ya da sertifika odaklı çalışıldığında resmi süreçler belki sorunsuz halledilebilir, fakat süreçlerin katma değer olarak sunduğu bilgi ve varlık güvenliği ile kurumsal bilgi bütünlüğü bir yerde kesinlikle yara alır. Riskleri tanımlarken gösterilen hassasiyetlerin onu yaşarken de aynı olgunlukta devam ettirilmesi beklenmelidir. BGYS sertifika süreçleri yüz metre koşuları ile başarıya ulaşmak gibi görünse de PUKÖ döngüsü ile kendisini sürekli tekrar etmesi gereken bir maratondur aslında. Bu maratonda kurumların karşısına sürekli değişen ve gelişen teknolojiler, araçlar, hizmetler ve kavramlar çıkacaktır. Düzenli yapısını korurken, yeni teknolojileri de bünyesine katabilen kurumlar, günümüzde hep bir adım önde gitme şansını yakalayabilecektir.

[1] *Köse, O., (2010). ISO/IEC 27001 Denetim ve Belgelendirmesi. (s. 15-18)*

Bilgi Güvenliği felsefesinin, süreçlerinin ve kullanımının kurumların geleceği için vazgeçilmezliği kabul edilmelidir. Ancak bu şekilde, BGYS süreçleri kurum içinde bir kültür olarak yerleşebilir.

6. Kaynakça

[1] BDDK (2010). Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik. Resmi Gazete: 13 Ocak 2010. Erişim: 11.09.2011. http://www.bddk.org.tr/websitesi/turkce/Mevzuat/Mevzuat.aspx

[2] Çetinkaya Kılıç, M., Gökçöl, O., (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. 3. Ağ ve Bilgi Güvenliği Sempozyumu 2010, Ankara.

[3] Devlet Planlama Teşkilatı Müsteşarlığı (DPT), (2010). Bilgi Toplumu İstatistikleri, Erişim: 11.09.2011, http://www.dpt.gov.tr/DocObjects/View/9776/BilgiToplumuIstatistikleri_2010.pdf

[4] Elektronik Haberleşme Kanunu (2008). Resmi Gazete, Sayı: 27050 (Mükerrer), 10 Kasım 2008. Ankara.

[5] Eralp, Ö., (2010) Bilgi İşlem Merkezi Yöneticilerinin Hukuki ve Cezai Sorumluluğu, 5. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2010, Ankara.

[6] Ergin, H., (2010). TSE Bilgi Güvenliği Belgelendirme, Türk Standartları Enstitüsü, Ankara.

[7] Evrin, V., (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği, Hacettepe Üniversitesi Bilişim Hukuku Tezsiz Yüksek Lisans Programı Proje Raporu, Ankara.

[8] ISACA, (2010). COBIT, Val IT and Risk IT — Synergistic Relationship.

[9] ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. First edition, 2009-05-01.

[10] ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements. First edition 2005-10-15.

[11] ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management. Second edition 2005-06-15.

[12] İbrişim, Ayşegül., (2008). TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları. Türk Standartları Enstitüsü, Ankara.

[13] Koç, F., (2008). BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[14] Köse, O., (2010). ISO/IEC 27001 Denetim ve Belgelendirmesi. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[15] Ottekin, F., (2008). ISO/IEC 27001 Denetim Listesi. Sürüm 1.00, UEKAE, TÜBİTAK.

[16] Ottekin, F., (2011). BGYS ve BGYS Kurma Deneyimleri. 6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2011, Ankara.

[17] Önel, D., (2008). Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[18] Önel, D., Dinçkan, A., (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. Sürüm 1.00, UEKAE, TÜBİTAK.

[19] Öztürk, G., (2008). Bilgi Güvenliği Politikası Oluşturma Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[20] Pattinson, F., (2007). Certifying Information Security Management Systems. ATSEC Information Security Corporation .

[21] Pekel, A., (2010). Bilişim Teknolojilerinde Yönetişim. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[22] Perendi, Ü., (2008). BGYS Kapsamı Belirleme Kılavuzu. Sürüm 1.00, UEKAE, TÜBİTAK.

[23] Tanrıkulu, C., (2011). Bilgi Sistem Yöneticilerinin Hukuki Yükümlülükleri. 6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı, 2011, Ankara.

[24] Taşkın, E., (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[25] The IT Service Management Forum (2007). An Introductory Overview of ITIL® V3.

[26] TS ISO/IEC 27001 (Mart 2006). Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler. Türk Standartları Enstitüsü, Ankara

[27] TÜBİTAK Bilim, Teknoloji ve Yenilik Politikaları Daire Başkanlığı (2010). Ulusal Bilim, Teknoloji ve Yenilik Stratejisi 2011-2016. Ankara

[28] Türkyılmaz, M., (2010). COBIT® ve Diğer Standartlar ile Karşılaştırılması. Bilgi Teknolojileri Yönetişim ve Denetim Konferansı (BTYD 2010), Ankara.

[29] Ünver, M., Canbay, C., Mirzaoğlu, A.G., (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

[30] Ünver, M., Ketevanlıoğlu, M.S., (2010). Bilgi Teknolojisi Hizmetleri Düzenleyici Çerçeve Yaklaşımı. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

[31] Wikipedia. Information Age (t.y.). Erişim : 11.09.2011, http://en.wikipedia.org/wiki/Information_Age