Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Dr. İzzet Gökhan Özbilgin[1], Mustafa Özlü[1,2]

[1] Sermaye Piyasası Kurulu, Ankara

[2] Türk Patent Enstitüsü, Ankara

gokhan@spk.gov.tr, mustafa.ozlu@tpe.gov.tr

Özet: Yazılım geliştirme süreçleri analiz, tasarım, kodlama, test ve bakım olmak üzere beş ana sürece ayrılabilir. Tüm bu süreçler gerçekleştirilirken ele alınması gereken hususlardan biri güvenliktir. Güvenlik hususu daha çok yazılım tamamlandıktan sonra ele alınmakta ve ihmal edilebilmektedir. Aslında güvenlik sadece yazılım geliştirme sürecinde değil, ağ kurulumu, veritabanı yönetimi gibi bilgi sistemleri ile ilgili tüm süreçlerde daha en baştan düşünülmesi ve yaşatılması gereken bir husustur. Uluslararası kabul görmüş olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı, ister kamu ister özel olsun, her ölçekteki kuruluşa uygun, etkili bir güvenlik yönetim sisteminin gerekliliklerini ortaya koymaktadır. Bu kapsamda, kuruluşların geliştirecekleri yazılımlarda güvenlik unsurlarının yönetilmesi için rehber olabilecek bir standarttır. Bu çalışmada yazılım geliştirme süreçlerinde oluşabilecek risklerin bu standart ile ilişkisi incelenecek, bu standartta yer alan ve yazılım geliştirme süreçlerinde ele alınması gereken kontroller değerlendirilecektir.

* Çalışmada geçen görüşler yazarlara aittir.

Anahtar Sözcükler: Yazılım Geliştirme, ISO 27001, Bilgi Güvenliği

Software Development Processes and ISO 27001 Information Security Management System

Abstract: The software development processes can be divided into five main process; analysis; design, coding, testing and maintenance. One of the important issues which need to be held during these processes is security. Mostly, the security issues could be neglected while developing software and addressed after the completion of it. In fact, the security needs to be considered at the beginning and held continuously not only in the software development processes, but also in all processes related to information technology such as network implementation and database management. The internationally ISO/IEC 27001 Information Security Management System standard covers all the requirements needed for an effective information security and is designed for use in organizations of all sizes, either public or private. Therefore, this standard may be a guide for the companies while developing their own software. In this study, the relation between the risks occurring during software development processes and this standard will be examined. Also the controls which must be discussed during software development processes will be investigated.

Keywords: Software Development, ISO 27001, Information Security

1. Giriş

Yazılımların hayatımızdaki yeri ve öneminin gün geçtikçe artması yazılımlara ilişkin çalışmaları hızlandırmakta, bu durum yeni yazılım geliştirme yöntemleri, programlama kuralları veya programlama dilleri ve araçları ortaya çıkarmaktadır. Tüm bu gelişmelere rağmen yazı-

lım projelerinde tasarlanan zamanın gerisinde kalma, bütçeyi aşma, düşük kalite, sürekliliği ve güvenilirliği sağlayamama, kullanıcı taleplerinin karşılanmasında yetersizlik gibi problemlerle sıkça karşılaşılmaktadır. Gartner araştırmasına göre bilişim güvenliği ihlallerinin yazılım güvenliği problemlerinden kaynaklananlarının oranı %80'dir [1]. Genel olarak problemlerin çoğu, yazılım geliştirme sürecinin en başında gereksinim ve sistem analizlerinin doğru ve yeterli yapılmamasından kaynaklanmaktadır.

Bilgi güvenliği; karşılaşılabilecek tehditlerin farkında olunması, işlerin devamlılığını sağlama, yaşanabilecek her türlü problemlerde kayıpları en aza indirme, firmaların varlıklarının her koşulda gizliliği, erişebilirliği ve bütünlüğünü korunma amaçları taşımaktadır. Bu kapsamda ortaya çıkartılan ve sürekli geliştirilmekte olan bir süreç de "Bilgi Güvenliği Yönetim Sistemi (BGYS)" dir.

Yazılımlarda bilgilerin korunması yazılımın geliştirme sürecinin başından itibaren tüm aşamaların bilgi güvenliği kontrollerine uygun olarak gerçekleşmesine bağlıdır. Yazılımın geliştirme sürecinde bilgi güvenliği yönetim sisteminin sağlanmış olması, yazılımlardaki bilgilerin kullanıma hazır olduğunu, sadece yetkisi olanların erişebildiğini ve kullanılan bilginin doğru ve güncel olduğu anlamına gelmektedir.

Bu çalışmanın ikinci ve üçüncü bölümünde yazılım, yazılım geliştirme süreçleri ve güvenli yazılım geliştirmeye ilişkin bilgilere yer verilecektir. Dördüncü bölümde uluslararası bir standart olan "ISO/IEC 27001 Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi- Gereksinimler Standardı (ISO 27001)" ele alınacak, sonrasında ISO 27001'in yazılım geliştirme süreçleriyle ilişkili kontrol maddelerine ve sonuç bölümüne yer verilecektir.

2. Yazılım Geliştirme Süreçleri

Yazılım, mevcut bir problemi çözmek amacıyla değişik cihazların birbirleriyle haberleşebilmesini sağlayan ve görevlerini ya da kullanılabilirliklerini geliştirmeye yarayan bilgisayar dili kullanılarak oluşturulmuş anlamlı ifadeler bütünü olarak da nitelendirilebilir [2]. Yazılım geliştirme ise yazılımın hem üretim hem de kullanım süreci boyunca geçirdiği tüm aşamalar olarak tanımlanabilir.

Geçmişte yazılım geliştirmede başvurulan iş akış şemaları gibi yöntemler günümüzde gereksinimleri karşılayamadıklarından ve güvenlik odaklı olmadıklarından yetersiz kalmışlar, etkinliklerini yitirmişlerdir. Yazılımın her aşamasında güvenliğe ilişkin ortaya çıkabilecek problemleri gözeten etkin bir geliştirme süreci sonuç ürünün daha güvenilir olmasına önemli katkı sağlayacaktır. Yazılım geliştirmede çok sayıda farklı model ve süreç değerlendirmelerinden söz etmek mümkündür. Bununla birlikte; yazılım mühendisliğindeki diğer modellere temel teşkil eden "Çağlayan Modeli (Waterfall Model)" yazılım yaşam döngüsünü beş aşamada ele almaktadır [3]:

2.1. Analiz: Bir problemin çözümü olarak nitelediğimiz yazılımların ne yapacağını ve nasıl yapacağını belirlediğimiz yani problemi tanımladığımız aşama analiz aşamasıdır.
2.2. Tasarım: Analiz aşaması sonucunda belirlenen gereksinimlere yanıt verecek yazılımın temel yapısının oluşturulduğu aşamadır.
2.3. Kodlama: Kodlama aşaması, tasarım sürecinde ortaya konan veriler doğrultusunda yazılımın gerçekleştirilmesi aşamasıdır.
2.4. Test: Test aşaması, yazılım kodlanması sürecinin ardından gerçekleştirilen sınama ve doğrulama aşamasıdır.
2.5. Bakım: Yazılımın tesliminden sonra hata giderme ve yeni eklentiler yapma aşamasıdır.

3. Güvenli Yazılım Geliştirme

Yazılımların yaygın olarak kullanılmaya başlandığı ilk yıllarda kaliteli ve olgun yazılım üretmek, son yıllarda ise özellikle güvenli yazılım geliştirmek için çok sayıda model ve çerçeve üzerinde çalışılmıştır. Bu durumun en

büyük tetikleyicisi son yıllarda güvenlik açıklıklarının artmasıdır [4]. Artan bu güvenlik tehditleri Şekil 1'de görüldüğü üzere hiç hesaba katılmayan sürpriz maliyetleri de beraberinde getirmektedir. Yazılım geliştirmede erken bir süreçte farkına varılan yazılım açıklıklarının düzeltilmesinin daha ileri süreçlerde farkına varılan açıklıklara göre daha az maliyetli olacağı yazılım endüstrisince yaygın olarak kabul edilen bir ilkedir [5].

Şekil 1 - Yazılım Geliştirme Süreçlerinde Yazılım Açıkları Giderme Maliyeti [5]

Güvenli yazılım geliştirme süreçlerinde değişiklik ve konfigürasyon yönetimi, geliştirme, test ve üretim ortamı ayrışımı, geliştirme ortamında gerçek verilerin kullanılmaması, üretim ortamına almadan önce kod incelemesi, güvenli programlama teknikleri kullanımı, uygulama güvenlik duvarı kullanımı ya da kaynak kod inceleme hizmeti alınması gibi çalışmaların yapılması da güvenliğe ayrıca katkı sağlayacaktır[1]. Güvenli yazılım geliştirme sürecinde ele alınması gereken temel olarak dokuz ana güvenlik konusu vardır [6]:

1. Girdi Geçerleme (Input Validation): Günümüzde bilinen ve gelecekte de muhtemel tehditlerin çoğu kötü niyetli girdi ile başlamaktadır.
2. Kimlik Doğrulama (Authentication): Kimlik doğrulama, varlıkların (kullanıcı, cihaz veya bir uygulama) kimlik kontrolünden geçmesi işlemidir ve farklı kimlik doğrulama yöntemleri bulunmaktadır.
3. Yetkilendirme (Authorization): Kullanıcıların tanımlanması aşaması olan kimlik doğrulamadan sonra kullanıcının kimliği doğrultusunda erişim haklarının belirlendiği ve kontrolünün gerçekleştiği aşama yetkilendirmedir.
4. Konfigürasyon Yönetimi (Configuration Management): Konfigürasyon, uygulama ile ilgili hassas bilgileri içermektedir. Örnek vermek gerekirse veri tabanına erişim için gerekli bağlantı bilgilerini içeren dosyalar bu kapsamdadır.
5. Hassas Bilgi (Sensitive Information): Hassas bilginin ne olduğunun belirlenebilmesi için uygulamanın ve işin bir arada ele alınması gerekir.
6. Kriptografi (Cryptograhy): Veriyi korumanın yollarından biri de şifrelemedir. Bugün şifreleme çalışmaları oldukça ilerlemiş, bilgisayarlar oldukça gelişmiştir.
7. Parametre Manipülasyonu (Parameter Manipulations): Dağıtık algoritmalar modüller arasında parametre gönderirler. Eğer bu parametreler arada değiştirilirse, saldırı gerçekleştirilmiş olur.
8. Hata Yönetimi (Exception Management): Bazı teknolojiler hataları kullanarak hata yönetimi gerçekleştirmektedirler. Hatalar geliştiriciler ve sistem yöneticileri için uygulama ile ilgili birçok önemli bilgi ihtiva ettiği için çok önemlidirler.
9. Kayıt Tutma ve Denetim (Logging and Auditing): Uygulama veya uygulamanın yöneticileri saldırı altında olduklarını anlamalıdır. Bu durum aslında neyin normal neyin anormal olduğunun belirlenmesi ile sağlanır.

Yukarıdaki ve bunlara benzer onlarca tehdit güvenilir uygulamalar geliştirmek için yazılım geliştirme sürecinin güvenliğinin yönetilmesinin büyük önem arz etmekte olduğunu gözler önüne sermektedir.

4. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliği, yazılı, sözlü, elektronik ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişebilirlik bakımından güvence altına alınması ve bu güvence durumunun sürekliliğinin sağlanmasıdır. Bilgi sistemlerinin hayata geçmesiyle ortaya çıkan depolama ve işleme imkânlarının artması, izinsiz erişimler, bilginin yetkisiz imhası, yetkisiz değiştirilmesi veya

yetkisiz görülmesi ihtimallerinin artması gibi hususlar nedeniyle bilgi güvenliği kavramı gündeme gelmektedir. Bilgi sistemlerinin çoğu, bilgi saklanırken, paylaşılırken, gönderilirken güvenlik kaygıları düşünülerek tasarlanmamıştır. Bilgi güvenliği ihlali ve buradan doğacak kayıpların riskini minimize etmek kurulan sistemlerin en başında BGYS gelmektedir. BGYS, bilgi güvenliğini kurmak, işletmek, izlemek ve geliştirmek için iş riski yaklaşımına dayalı, dokümante edilmiş, işlerliği ve sürekliliği garanti altına alınmış bir yönetim sistemidir. BGYS, bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. BGYS'nin ihtiyaç duyduğu gereksinimlere cevap vermek için çok sayıda standart vardır. Bunların en önde geleni ISO 27001 standardıdır.

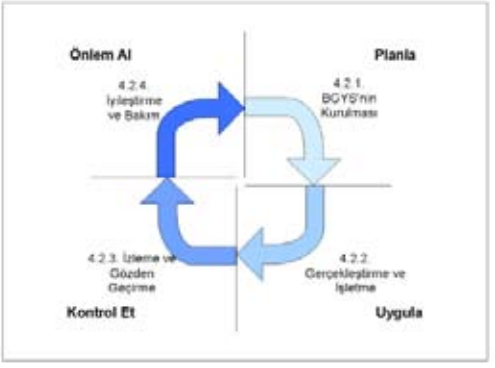
ISO 27001 kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlayan tek denetlenebilir BGYS standardıdır. ISO 27001 ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu uluslararası standardıdır. ISO 27001 standardı; kuruluşların kendi bilgi güvenlik sistemlerini sağlamasını mümkün kılan teknoloji tarafsız, satıcı tarafsız yönetim sistemleri için bir çerçeve sağlar. ISO 27001, kuruma uygun politikalar, prosedürler ve kılavuzlar oluşturmaya yol gösteren uluslararası kabul görmüş yapısal bir metodoloji sunar. ISO 27001 sertifikası, kurumların güvenlik seviyesine ve kurumun konuya ciddi yaklaşımına ilişkin bir göstergedir.

Bilgi güvenliği ile ilgili olarak ISO/IEC 27000 serisi güvenlik standartları, kullanıcıların bilinçlenmesi, güvenlik risklerinin azaltılması ve de güvenlik açıklarıyla karşılaşıldığında alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır[7]. ISO/IEC 27000 standart serisi altında yer alan ve ISO 27001 için gereken güvenlik kontrollerini içeren standart; ISO/IEC 27002:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzu'dur. [8].

Güvenlik kontrol alanları, ISO 27001'de BGYS oluşturmada güvenlik için gereken 11 kontrol alanı, 39 kontrol hedefi ve 133 kontrolü tanımlayan bir uygulama kılavuzudur. BGYS'de kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır. Risk işleme için standartta öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. ISO 27001 yaşayan, dolayısı ile tehdit ve saldırılara reaksiyon gösteren ve kendini yenileyen bir bilgi güvenliği sisteminde yer alması gereken öğeleri tanımlamaktadır [9].

ISO 27001, BGYS'yi kurmak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için standart proses yaklaşımını benimsemiştir. Bu proses yaklaşımı güvenlik önlemlerinin belirlenip kurulması, uygulanması, etkinliğinin gözden geçirilmesi ve iyileştirilmesi süreçlerini ve bu süreçlerin sürekli olarak tekrarlanmasını içerir. Bu süreçler Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünden oluşan bir model olarak da ortaya konmuştur.

Şekil 2'de gösterilen PUKÖ Modeli uyarınca risk yönetimi faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye geriletilene kadar çalışmayı sürdürmelidir [10].



Şekil 2- BGYS'nin PUKÖ Modeli [9]

5. Yazılım Geliştirme Süreçleri ve ISO 27001

ISO 27001, gerek yazılım geliştirme süreçleriyle doğrudan ya da dolaylı ilişki içerisinde

olan birçok kontrol içermektedir. Bu kontroller ve kontrol kapsamında yazılım geliştirme süreci aşamalarında gerçekleştirilmesi gereken hususlar aşağıdaki gibidir.

5.1 Analiz Aşamasına İlişkin Kontroller

Yazılım geliştirme sürecinin en önemli aşamasıdır. Bu aşamada yapılacak yanlışlıklar yazılım projesinin başarısını en yüksek düzeyde etkilemektedir. Bu aşamada kurumun mevcut bilgi teknolojileri, varsa sistem veri tabanı yapısı, sistem veri yapıları tanımlanmalıdır. Yapılacak analiz, uygulama servislerinin performans ya da kısıtlamalar yönünden zorlanması ve doğru hizmet vermelerini engelleme girişimlerini de hesaba katmalıdır. Sunucu tarafındaki konfigürasyonların güvenli şekilde yapılması gerekir. Yazılım için devreye alınacak yeni bilgi sistemleri için iş gereksinimleri bildirgeleri ya da mevcut bilgi sistemlerine yapılan iyileştirmeler güvenlik kontrolleri için gereksinimleri belirlemelidir. (A.12.1.1 - Güvenlik gereksinimleri analizi ve belirtimi) Yeni bilgi işleme tesisleri için, bir yönetim yetki prosesi tanımlanmalı ve gerçekleştirilmelidir. (A.6.1.4 - Bilgi işleme tesisleri için yetki prosesi)

Yetkilendirilmiş kullanıcıların sistemde neler yapabileceği uygun şekilde belirtilmelidir, aksi durumlarda başka kullanıcı haklarını kullanma, yetkisiz olduğu halde verilere erişebilme gibi sakıncalar doğabilir. Kuruluş içinden ya da dışından sağlanmış olsun tüm ağ hizmetlerinin güvenlik özellikleri, hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalıdır. (A.10.6.2 - Ağ hizmetleri güvenliği)

İletişimin bütün türlerinin kullanımıyla ve bilgi değişimini korumak için resmi değişim politikaları, prosedürleri ve kontrolleri oluşturulmalıdır. (A.10.8.1 - Bilgi değişim politikaları ve prosedürleri) Yazılımda kullanılacak harici materyaller için fikri mülkiyet haklarına göre materyallerin kullanımı ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla doğan gereksinimlere uyum sağlanmalıdır. (A.15.1.2 - Fikri mülkiyet hakları (IPR) Kuruluşun dış taraflarla yapacağı bilgi ve yazılım değişimi için anlaşmalar yapılması gerekir, bu gereksinim analiz aşamasında karşılanmalıdır. (A.10.8.2 - Değişim anlaşmaları)

5.2 Tasarım Aşamasına İlişkin Kontroller

Tasarım aşamasında, uygulanacak geliştirme safhaları, her safha için girdiler, çıktılar ve kontrol metotları, iş zaman planları, uygulama planlarının yanı sıra yapılacak işlerin neler olduğu, bu işler için gerekli zaman ve kaynak ihtiyaçlarının tespiti, ilerlemenin izlenmesi için kullanılacak metotlar belirlenmelidir. Bilgi sistemlerinin birbirine bağlantısı ile ilişkili bilgiyi korumak için politikalar ve prosedürler geliştirilmeli ve gerçekleştirilmeli, bilgi sızması fırsatları önlenmelidir. (A.10.8.5 - İş bilgi sistemleri, A.12.5.4 - Bilgi sızması) Bu kapsamda tasarım aşamasında yüksek riskli uygulamalara ek güvenlik sağlamak için bağlantı sürelerinde sınırlandırmalar kullanılması gerektiği hesaba katılmalıdır. (A.11.5.6 - Bağlantı süresinin sınırlandırılması)

Tehditlerden korunmak için ve iletilmekte olan bilgi dâhil ağı kullanan sistemler ve uygulamalar için güvenliği sağlamak amacıyla ağlar uygun şekilde yönetilmeli ve kontrol edilmelidir. (A.10.6.1 - Ağ kontrolleri) Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, oluşturulması önerilen tanımlanmış erişim kontrol politikasına uygun olarak kısıtlanmalıdır. (A.11.6.1 - Bilgi erişim kısıtlaması)

5.3 Kodlama Aşamasına İlişkin Kontroller

Yazılımların karşılaştığı en önemli tehditlerden biri uygulamalarda gerçekleşen veri girişçıkışında kontrollerin tam ve sağlıklı olarak yapılmadan işleme alınması ya da çıktı olarak verilmesidir. Uygulamalara gerçekleşen veri girişinin, bu verinin doğruluğunun ve uygunluğunun geçerlenmesi gerekmektedir. Yazılımda girdi parametreleri yazılım dışından verilebilir olmamalıdır. Kayıt olanakları ve kayıt bilgisi kurcalanma ve yetkisiz erişime karşı korunmalıdır. (A.10.10.3 - Kayıt bilgisinin korunması)

Böyle bir koruma olmaması durumunda SQL (Structed Query Language) enjekte etme ve komut enjekte etme gibi yöntemlerle sistemlere girebilecek kodlar büyük zararlar verebilir. (A.12.2.1 - Giriş verisi geçerleme) Giriş verisi kadar çıkış verisi de önemlidir. Yazılımda çıkış verisi sistemimiz hakkında bilgi vermemeli veri sızıntısına açıklık bırakmamalıdır. Bir uygulamadan gerçekleşecek veri çıktısı, depolanan bilginin işlenmesinin koşullara göre doğruluğunun ve uygunluğunun sağlanması için geçerlenmelidir. (A.12.2.4 - Çıkış verisi geçerleme) Veri işleme hataları veya kasıtlı eylemler nedeniyle herhangi bir bilgi bozulmasını saptamak için geçerleme kontrolleri uygulamalar içine dâhil edilmelidir. (A.12.2.2 - İç işleme kontrolü) Uygulamalarda verinin kimliğinin doğruluğunu sağlama ve mesaj bütünlüğünü koruma gereksinimleri tanımlanmalı bunlarla ilgili uygun kontroller tanımlanmalı ve gerçekleştirilmelidir. (A.12.2.3 - Mesaj bütünlüğü)

Kötü niyetli koda karşı korunmak için saptama, önleme ve kurtarma kontrolleri ve uygun kullanıcı farkındalığı prosedürleri gerçekleştirilmeli, elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır. Benzer bir biçimde mobil kod kullanımı yetkilendirildiğinde, konfigürasyon yetkilendirilmiş mobil kodun açıkça tanımlanmış bir güvenlik politikasına göre işletilmesini sağlamalı ve yetkilendirilmemiş mobil kodun yürütülmesi önlenmelidir. (A.10.4.1 - Kötü niyetli koda karşı kontroller, A.10.8.4 - Elektronik mesajlaşma, A.10.4.2 - Mobil koda karşı kontroller)

Kriptografi teknikleri yazılımlarda güvenliği sağlamada faydalanılan önemli tekniklerdir. Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmeli ve gerçekleştirilmelidir. (A.12.3.1 - Kriptografik kontrollerin kullanımına ilişkin politika) Kriptografi için yeterli rastgeleliği sağlayan kriptografik tekniklerin kullanım desteklenmeli ve anahtar yönetimi bulunmalıdır. (A.12.3.2 - Anahtar yönetimi)

Yazılım geliştirme hizmetinin kuruluş dışından sağlanması durumunda, hizmeti sunan şirketin hareketleri ve yaptığı işler denetlenmeli ve izlenmelidir. (A.12.5.5 - Dışarıdan sağlanan yazılım geliştirme) Yazılım geliştiricilerce gerçekleştirilen ve revizyon kontrolü yapılmayan yazılım değişiklikleri karmaşaya ve çeşitli sorunlara neden olabilmektedir. Yazılım değişikliklerin gerçekleştirilmesinde resmi değişim kontrol prosedürlerinin kullanılması bu karmaşayı ortadan kaldıracaktır.(A.12.5.1 - Değişim kontrol prosedürleri)

5.4 Test Aşamasına İlişkin Kontroller

Kodlama aşamasından sonra gerçekleştirilecek test aşamasında yazılım uygulaması modüllerinin nitelik ve nicelik testleri yapılır. Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmalıdır. (A.10.1.4 - Geliştirme, test ve işletim olanaklarının ayrımı)

Bu aşamada bir test planı oluşturulmalı bu planda; test senaryoları, veri çeşitleri ve veri örnekleri ve test tasarım tanımlamaları ayrıntılı olarak belirtilmelidir. Veri tabanının büyüklüğü ve listelenen, sorgulanan kayıt sayısı ile sistemin performans ilişkisi kontrol edilmelidir. (A.12.2.1 - Giriş verisi geçerleme, A.12.2.4 - Çıkış verisi geçerleme, A.12.2.2 - İç işleme kontrolü) Test verisi dikkatlice seçilmeli, korunmalı ve kontrol edilmelidir. (A.12.4.2 - Sistem test verisinin korunması) Yazılım ürünlerinin, sistemin ve alt sistemlerin modül, fonksiyon, entegrasyon ve performans testlerinden sonra testlerde ortaya çıkan değerlere uygun olarak gerçek bilgi ve verilerle, gerçek kullanıcı donanım ve işletim ortamında tüm ihtiyaçların karşılandığı kontrol edilmelidir.

Test aşaması bitip uygulama devreye alınırken tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi ve bilgi işleme olanaklarına olan erişim hakları, istihdam, sözleşme veya anlaşmalarının sonlandırılmasıyla birlikte kaldırılmalı ya da değiştirilmesiyle birlikte ayarlanmalıdır. (A.8.3.3 - Erişim haklarının kaldırılması)

5.5 Bakım Aşamasına İlişkin Kontroller

Yazılım geliştirme sürencin son aşaması, bakım aşamasında da alınması gereken bir takım güvenlik önlemlerinden söz etmek mümkündür. Yazılım paketlerine yapılacak değişiklikler, belirli bir incelemeden geçirilmeli, gerek duyulanlar gerçekleştirilmeli, bunun dışındakiler önlenmelidir. Tüm değişiklikler sıkı bir biçimde kontrol edilmelidir. (A.12.5.3 - Yazılım paketlerindeki değişikliklerdeki kısıtlamalar) Benzer bir biçimde kullanıcıların erişim hakları da resmi bir proses kullanarak düzenli aralıklarda gözden geçirmelidir. (A.11.2.4 - Kullanıcı erişim haklarının gözden geçirilmesi)

Yazılım Kaynak kodlarının bozulma riskini azaltmak ve bilgi kaybından korumak amacı ile kaynak kodları yazılım uzmanlarının işletim sistemleri içinde değil sunucu terminal üzerinde bulunmalıdır. Program kaynak koduna erişim kısıtlı olmalıdır. (A.12.4.3 - Program kaynak koduna erişim kontrolü) Söz konusu ortama erişim yalnızca ilgili yazılım uzmanı tarafından sağlanmalıdır.

Donanım arızaları, yazılım hataları, insandan kaynaklanan nedenler ve doğal afetler yazılımlarda bilgi kayıplarının ana sebepleridir. Sebep her ne olursa yedekleme yazılımlarda hatalardan ve problemlerden geri dönüş için son derece önemlidir. Yedekleme için kurtarılabilir veri saklama yöntemleri uygulanmalı, bilgi ve yazılımlara ait yedekleme kopyaları düzenli olarak alınmalı ve alınan yedekler belirlenecek bir politikaya göre uygun şekilde düzenli olarak test edilmelidir. (A.10.5.1 - Bilgi yedekleme)

Belirlenmiş bir ön yetkilendirme olmaksızın teçhizat, bilgi veya yazılım bulunduğu yerden çıkarılmamalıdır. (A.9.2.7 - Mülkiyet çıkarımı) Eğer yetkilendirme varsa ve bilgi içeren ortamın, kuruluşun fiziksel sınırları ötesinde taşınması söz konusu ise taşıma esnasında, bilgiler yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalıdır. (A.10.8.3 - Aktarılan fiziksel ortam)

Bilgisayar donanımlarının depolama ortamı içeren tüm parçaları, elden çıkarılmadan önce, herhangi bir hassas veri ve lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlanmalıdır. (A.9.2.6 - Teçhizatın güvenli olarak elden çıkarılması ya da tekrar kullanımı) Kurumların ve şirketlerin operasyonel sistemlerindeki yazılımların kurulmasını kontrol etmek için prosedürler bulunmalıdır. (A.12.4.1 - Operasyonel yazılımın kontrolü)

Zayıf parolalar ve şifreler bilişim sistemleri açısından önemli açıklıklar ortaya çıkarmaktadır. Kullanıcılardan, parolaların seçiminde ve kullanımında iyi güvenlik uygulamalarını izlemeleri istenmelidir. Bu ve bunun gibi hususlar için bilinçlendirme çalışmaları yapılmalı eğitimler verilmelidir.(A.11.3.1 - Parola kullanımı)

İşletim sistemleri değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir. (A.12.5.2 - İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme)

6. Sonuç

Kurumların güvenli bir ortamda faaliyet gösterebilmeleri için dokümante edilmiş bir BGYS'yi hayata geçirmeleri gerekmektedir. Bu kapsamda ISO 27001 standardı tüm dünyada kabul görmüş ve en iyi uygulamaları bir araya getiren bir modeldir. Standart bu yönetim sistemini oluştururken ele aldığı önemli alanlardan biri de yazılım geliştirme süreçlerinde güvenliğinin sağlanması ve buna ilişkin olarak yazılım geliştirme politikasının oluşturulmasıdır. Yazılım geliştirme süreçlerinde standardın belirttiği gizlilik, bütünlük ve erişebilirlik kavramları mutlaka dikkate alınmalıdır. Bu kapsamda, yazılım geliştirmenin her aşamasında belirli bir güvenlik politikasının uygulanması kritik önem taşımaktadır. Kurumsal güvenlik için öncelikle yazılı olarak kurallar belirlenmelidir. Etkin bir BGYS kurmaya çalışan ve bunu ISO 27001 standardına uyumlu yapmak

isteyen tüm kurumların oluşturacağı bu politikada belli kontrol maddeleri asgari olarak yer almalıdır.

7. Kaynaklar

[1] Dayıoğlu, Burak, "Yazılım Geliştirme Yaşam Döngüsü ve Güvenlik", http://www.pro-g.com.tr/pciveriguvenligi 2008/pdf/pro-g-presentation-v1.1.pdf (Erişim tarihi: 10.12.2009)

[2] "Yazılım", http://tr.wikipedia.org/wiki/Yaz %C4%B1 l%C4%B1m (Erişim tarihi: 22.12.2009)

[3] "Waterfall model", http://en.wikipedia.org/wiki/Waterfall_model (Erişim tarihi: 24.12.2009)

[4] Alparslan, Erdem, "Güvenli Yazılım Geliştirme Modelleri", TÜBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/guvenli-yazilim-gelistirme-modelleri.html (Erişim tarihi: 10.12.2009)

[5] Michael, C.C., Radosevich, Will, "Risk-Based and Functional Security Testing", https://buildsecurityin.us-cert.gov/daisy/ bsi/articles/best-practices/testing/255-BSI .html (Erişim tarihi: 16.12.2009)

[6] Cohen, Manu, "Practical Application Security", Security Acts The Magazine for IT Security, Ekim 2009.

[7] International Standard, "ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements", First Edition, 15.10.2009.

[8] Calder, Alan, Bon, Jan Van, "Implementing Information Security based on ISO 27001/ISO 17799 - A Management Guide", Van Haren Publishing, 2006 ISBN: 9789077212783.

[9] Ottekin, Fikret, "Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgiguven liginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-ontrolleri.html?Itemid=6. (Erişim tarihi: 03.12.2009)

[10] Çetinkaya, Mehtap, "Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması", Akademik Bilişim 2008, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak - 01 Şubat 2008.