Makale Türü: Araştırma Makalesi
Paper Type: Research Paper

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YAZILIMLARI: ÖRNEK BİR YAZILIM GELİŞTİRİLMESİ

***

CORPORATE INFORMATION SECURITY MANAGEMENT SYSTEM SOFTWARES: DEVELOPING AN EXAMPLE SOFTWARE

Sinan UĞUZ*

Öz

Kişisel ve kurumsal bilgi güvenliği artık günümüzde birbiri ile doğrudan ilişkili kavramlar haline gelmiştir. Birçok organizasyon müşterileri veya çalışanlarının kişisel bilgilerini korumanın yanı sıra kurumsal açıdan önemli olan bilgi varlıklarını da korumak zorundadır. Bu yüzden dünyaca kabul görmüş standartları uygulamak ve kurumsal bilgi güvenliğini sağlamak bir gereklilik halini almıştır. Günümüzde ISO/IEC 27001 bilgi güvenliği standardı gibi standartlara uygun bilgi güvenliği yönetim sistemleri (BGYS) uygulamalarının kurumlar ya da firmalar tarafından gerçekleştirilmeye çalışıldığı görülmektedir. Bu noktada bir BGYS sistemini dinamik bir yazılım sistemi ile oluşturmak daha hızlı ve etkili bir sonuç verecektir. Bu çalışmada bir BGYS sisteminin temel unsurları açıklanmış ve geliştirilen açık kaynak kodlu BGYS yazılımı incelenmiştir.

***Anahtar Kelimeler**: bilgi güvenliği, ISO/IEC 27001, bilgi güvenliği yönetim sistemi.*

Abstract

Nowadays, personal and corporate information security has become directly concepts related to each other. Many organizations must protect institutionally important information assets as well as personal information of its employees or customers. Therefore, to implement the standards accepted worlwide and to ensure corporate information security has become a necessity. It is observed that pursued by institutions or companies of the information security management systems (ISMS) applications that related to standarts such as ISO / IEC 27001 information security standards. At this point, to develop the ISMS system with a dynamic software system, it will give a faster and more effective results. In this study, has been described the main factors of a ISMS and has been investigated developed open source the software of ISMS.

***Keywords:** information security, ISO/IEC 27001, information security management system.*

* Yrd. Doç. Dr., Süleyman Demirel Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, sinanuguz@sdu.edu.tr

Geliş Tarihi / Received: 22.01.2018
Kabul Tarihi / Accepted: 13.02.2018

1. GİRİŞ

İnternet ortamında son yıllarda artan saldırılarla açık hedef hale gelen kişi ve organizasyonlar için bilgi güvenliği önemli bir konu haline gelmiştir. Bilgi güvenliğinin amacı, bilginin güvenilirliğini, bütünlüğünü ve erişilebilirliğini korumaktır. Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanmıştır (Canbek ve Sağıroğlu, 2016). Ülkemizde ve dünyada GSM şebekelerinin, internete daha hızlı bağlanabilmesi için 4.5G ya da 5G gibi üst düzey veri iletim teknolojisi hizmetlerini abonelerine sunmaya başlaması ile birlikte daha çok veri üretilmeye ve paylaşılmaya başlanmıştır. Bu durum bilgi güvenliği kavramını hem kişisel hem de kurumsal anlamda daha önemli hale getirmiştir. Kişilerin günlük hayatta e-devlet uygulamaları, internet bankacılığı veya e-ticaret uygulamalarını daha fazla kullanması hem kişisel hem de kurumsal bilgi güvenliğini ön plana çıkarmaktadır. Kurum içerisinde BGYS'ler aracılığı ile önem arz eden varlıkların tespit edilip bir risk analizi ile sınıflandırılması, kurumsal bilgi güvenliği için artık kaçınılmaz hale gelmiştir. Bu noktada kurumlara yol göstermek amacıyla çeşitli standartlar oluşturulmuştur. ISO/IEC 27001 standardı (ISO, 2005a), günümüzde bilgi güvenliği standartları arasında en yaygın olarak kabul gören standartlardan biridir. ISO/IEC 27000 standart serisi ISO (International Standard Organization) ve IEC (International Electrotechnical Commission) tarafından bilgi güvenliği için oluşturulmuş standartlardır. Özellikle ISO/IEC 27001 standardı bilgi güvenliği yönetim sistemleri için önemli tanımlamaları ve gereksinimleri ifade eder (Li vd., 2015). Aslında bir İngiliz standardı olan BS 7799-2, 2005 yılında ISO/IEC 27001:2005 adını almış ve 2013 yılında tekrar güncellenmiştir (Dünya ISO/IEC 27001 İstatistikleri ve Türkiye'nin Konumu , 2016). Ülkemizde de TS ISO/IEC 27001 (Bilgi teknolojisi- güvenlik teknikleri- bilgi güvenliği yönetim sistemleri- gereksinimler) bilgi güvenliği yönetim sistemi adı altında Türk Standartları Enstitüsü (TSE) tarafından yayınlanmıştır (TS ISO/IEC 27001 Bilgi Güvenliği. Yönetim Sistemi, 2016). Bu standart, kuruluşlarda BGYS oluşturmak, gerçekleştirmek ve sürdürmek için değerlendirme ve denetim mekanizması sağlar. Dünya genelindeki birçok kurum ISO/IEC 27001 uygunluk denetim birimleri tarafından akredite edilmektedir. Örneğin 2012 yılında akredite edilen firma sayısı Japonya'da 7199, Hindistan'da 1600, Macaristan'da 199 iken Türkiye'de 133 olarak kalmıştır (Dünya ISO/IEC 27001 İstatistikleri ve Türkiye'nin Konumu, 2016). Bu istatistik ülkemizdeki kurumların ve firmaların BGYS'yi uygulama anlamında yetersiz kaldığını göstermektedir.

BGYS'nin farklı konuları ile ilgili literatürde çeşitli çalışmalar mevcuttur. Haufe vd. (2016), çalışmalarında BGYS sistemi tasarlayan ve uygulayan kurumlar için başarılı bir BGYS sisteminin temel süreçlerini tanımlayarak kilit unsurlarını açıklamışlardır. Bunun için 90 katılımcıdan oluşan bir gruba BGYS temel süreçlerini belirlemek için kriterlerin adını vermelerini istedikleri bir anket formu sunmuşlardır. Daha sonra kendi tanımladıkları kriterler ile katılımcıların önerdikleri arasındaki uygunluğu ortaya koymuşlardır. Chang (2013), bilgi, bütçe, insan kaynakları ve maliyet karşılığı etkisi gibi çeşitli nedenlerden dolayı kurumların BGYS'ye geçmeyi ertelediğini belirtmiştir. Bu problemi çözmek için çalışmasında BGYS'nin kurumlara olan ekonomik etkisi üzerine bir analiz gerçekleştirmiştir. Sonuç olarak bir BGYS'nin bir kuruma olan yıllık ekonomik etkisinin 220 milyon won (Güney kore para birimi) olduğu belirtilmiştir. Ayrıca BGYS ile yıllık 2.47 kişilik iş gücü yaratma etkisinin oluşturulduğu belirtilmiştir. Tupa vd. (2017) ise Endüstri 4.0 gerçekleştirilmesinde risk yönetimi alanında uygulanabilecek yaklaşımlar üzerinde durmuşlardır. Endüstri 4.0 ile değişen koşullarda siber saldırılar, veri entegrasyonunda kayıplar gibi yeni riskler ortaya çıkmıştır. Özellikle gerçek zamanlı erişimden dolayı oluşacak çoğu riskin tanımlanmasının ve önlem alınmasının öneminden bahsetmişlerdir.

BGYS uygulamaları, kurumların iş ihtiyaçlarına, çevre özelliklerine ve kurum içinde iş hedeflerine ulaşılmasını engelleyen faktörlere bağlı olduğu için her kurum için benzersiz özelliklere sahip olacaktır. BGYS ile ilgili standartlar sağladıkları genel talimatlar ile kurum içinde bir BGYS

sisteminin nasıl kurulması ve yürütülmesi gerektiği ile ilgili bilgiler verir (Bialas, 2005). Kurumlar bir nevi bu yol haritasını kullanarak kendi içinde ihtiyaç duyacağı BGYS sistemlerini oluşturmaktadır. Özellikle bu konuda kurum içi yazılım araçları geliştirilmesi sistemin sağlıklı ve hızlı gerçekleşmesi için önem taşımaktadır. Bu çalışmada uluslararası BGYS standartları dikkate alınarak örnek bir BGYS yazılımı gerçekleştirilmiştir. Çalışmanın temel amacı kendi bünyesinde BGYS sistemi oluşturmak için kendi yazılımlarını geliştirmek isteyen kurumlara bir yol haritası sunmak ve bu konuda yapılacak akademik çalışmalara katkı sağlamaktır.

Bu çalışmanın bundan sonraki kısmında Bölüm II'de BGYS hakkında teorik bilgiler Bölüm III'de ise geliştirilen BGYS yazılımı detaylı olarak incelenmektedir.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

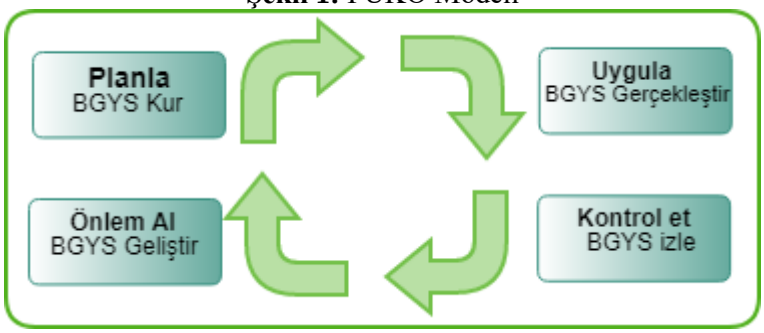
Broderick (2006), BGYS hakkında yanlış bilinenler ve bunların doğruları ile ilgili bir çalışmasında aşağıdaki yargılara ulaşmıştır.

- BGYS, teknik bir bilgi güvenlik standardı değil bir yönetim sitemidir,
- Bir BGYS'nin merkezi, BGYS tarafından ele alınması gereken genel alanların bir çerçevesidir,
- BGYS bir kalite yönetim sitemi kullanan çoğu organizasyon tarafından kullanılır. Bir BGYS, ISO 27001 gibi resmi bir standardı tamamen uygulamak yerine onu rehber edinerek organizasyona yapısına göre şekillendirilebilir,
- Organizasyon içinde idari yönetimin BGYS'ye inanması çok önemlidir.

BGYS ile kurum içerisindeki hassas bilgilerin yönetilmesi ve korunması amacıyla sistematik bir iş süreci oluşturulur. BGYS için politikalar oluşturulması bir risk yönetim yaklaşımını temel alır. Politikaların tanımı var olabilecek bilgi güvenliği risklerini belirlemek amacıyla iş ortamının anlaşılması, kaynakların ve süreçlerin değerlendirilmesi ile başlar. Kuruluşlar risklerin belirlenmesinden sonra riskleri yönetme stratejileri için çözüm bulma arayışlarına girer ve risklerin her birinin potansiyel etkilerini değerlendirir. Bu adımlar, işlemleri yürüten çalışanların yanı sıra yönetiminde kapsamlı katılımını gerektirir. Çevre ve iş süreçleri kuruluştan kuruluşa farklılık göstereceği için, geliştirilen strateji ve risk tanımları da farklı olacaktır. Bu noktada ISO 27001 standardı BGYS gerçekleştirmek için gereksinimleri ve özellikleri kuruluşlara sağlamaktadır (Hsu vd., 2016). ISO/IEC 27001 standardı güvenlik politikası, bilgi güvenliğinin organizasyonu, varlık yönetimi, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, haberleşme ve operasyon yönetimi, erişim kontrol, bilgi sistemleri edinimi, geliştirme ve bakım, bilgi güvenliği olay yönetimi, iş sürekliliği yönetimi ve uygunluk olmak üzere onbir kontrol alanına sahiptir (Li vd., 2015). Bu alanlar "Planla- Uygula- Kontrol et- Önlem al" (PUKÖ) çevrimini takip eden bir yapıya sahiptir ve BGYS konusunda temel bir başvuru kaynağıdır (Şekil 1).

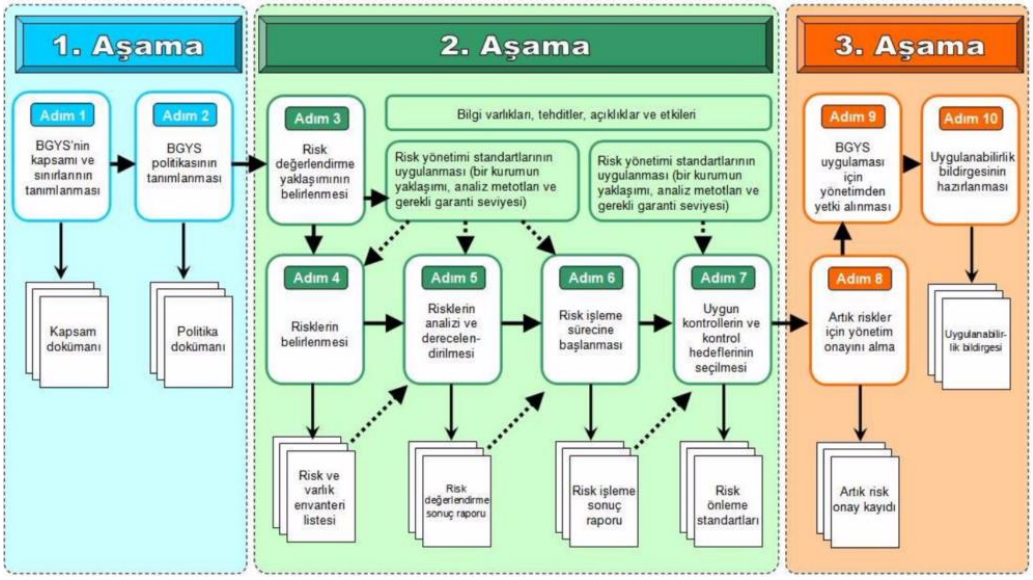
PUKÖ modelindeki aşamalar kısaca şu şekilde özetlenebilir. Planla aşamasında BGYS politikası, amaçları, hedefleri ve prosedürlerinin geliştirilmesi yani BGYS'nin kurulması gerçekleştirilir. Uygula aşamasında, planla aşamasında ortaya konan hedeflerin gerçekleştirilmesi ve işletilmesi sağlanır. Kontrol et aşamasında, planla aşamasında ortaya konan hedeflerin değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi gerçekleştirilir. Önlem al ise yönetimin gözden geçirme sonuçlarına göre düzeltici ve önleyici faaliyetleri gerçekleştirdiği PUKÖ modeli aşamasıdır (Marttin ve Pehlivan, 2010).

Şekil 1: PUKÖ Modeli



BGYS'nin kurum içinde oluşturulması ciddi bir süreç olup sadece teknik, teknolojik bir konu olmadığı için kurum içindeki tüm çalışanları ilgilendirir ve kurum içerisindeki tüm birimlerin temsilcilerinin oluşturacağı bir komisyonca işleyişin gerçekleştirilmesi gerekir. Bir BGYS'nin kurulum aşamaları, TS ISO/IEC 27001:2005'teki "BGYS'nin kurulması" başlığı altında açıklanmaktadır. Bu adımlar Şekil 2'deki gibi özetlenmiştir.

Şekil 2: BGYS kurulum aşamaları (Öner ve Dinçkan, 2007)



Şekil 2 incelendiğinde ilk aşamada kapsam ve politikalar belirlenir. Kapsam dâhilinde kurumun tamamının mı yoksa belli bir bölümünün mü BGYS'ye dâhil edileceği belirlenir. Politikanın tanımlanmasında hedefler yönetim tarafından iyi belirlenmelidir. İkinci aşamada ise risk yönetimi gerçekleştirilir. Kurum içinde korunması gereken varlıklar önem derecesine göre tespit edilir ve bu varlıkları tehdit eden riskler belirlenir. Tespit edilen riskler hakkında nicel (0, 1, 2 vb.) ya da nitel (çok yüksek, yüksek vb.) dilsel ifadelerle derecelendirilerek belli bir etki değeri kazandırılır ve risk değerlendirme sonuç raporuna işlenir. Risk işleme adımında, risk değerlendirme sonuç raporuna göre riskin ortadan kaldırılması ya da kabul edilebilir bir seviyeye düşürülmesi yolu izlenebileceği gibi riski oluşturan faktörler ortadan kaldırılabilir ya da risk sigorta şirketleri veya kurum dışı diğer taraflara aktarılabilir. Son aşamada ise geri kalan artık riskler için uygulanıp uygulanmaması gerekliliği ortaya koyulur. Yönetim onayından geçtikten sonra ise uygulanabilirlik bildirgesi hazırlanarak BGYS kurulum işlemi tamamlanır (Öner ve Dinçkan, 2007).

2.1. Varlıkların Belirlenmesi ve Sınıflandırılması

Kurum içindeki bilgi varlıklarının envanteri oluşturulurken bilgi varlıkları önce kategorilere ayrılmalıdır. Örneğin bilişim sistemi ile ilgili varlıklar yazılım ve fiziksel varlıklar olarak ikiye

ayrılabilir. Her bir kategori ise alt kategorilere ayrılabilir. Yazılım kategorisinin alt kategorileri sistem yazılımları, uygulama yazılımları ve diğerleri olabilir. Daha sonra bilgi varlıkları çok gizli, gizli, kişiye özel, hizmete özel gibi dereceler ile sınıflandırılabilir. Bilgi varlığının kurum açısından değeri ise alçak (0), düşük (1), orta (2), yüksek (3) gibi derece isimleri ve değerleri ile ifade edilebilir. Bu işlemlerden sonra her varlık için, sorumlu kişiler, varlığın bulunduğu yer ve varlık için tanımlama kodu oluşturulur. Kod oluşturulurken kategori, alt kategori ve diğer özellikler için uygun bir kodlama yapısı tercih edilebilir. Tablo 1'de iki farklı varlığın tanımlandığı özellikler görülmektedir.

Tablo 1: Varlık Tanımlanması

Bilgi varlığı	Varlık Kategorisi	Alt kategori	Sınıflandırma	Değeri	Sorumlular	Bulunduğu yer	Kodu
Windows Server 2016	Yazılım	Sistem Yazılımları	Hizmete Özel	Orta	İsim	İnsan Kaynakları	İKY_01_02_2
Router	Fiziksel Varlık	İletişim Ekipmanı	Kuruma Özel	Yüksek	İsim	Bina	B_02_02_3

2.2. Risk Yönetimi

BGYS kurulum aşamaları içinde risk yönetimi önemli bir yer tutmaktadır. Her kurum kendi yapılarını ve kurumsal, yasal bağlılıklarını dikkate alarak ISO 27001, ISO 27005, COBIT ve BASEL II gibi uluslararası kabul görmüş standartlarca desteklenen bir BGYS sistemini yönetimin onayladığı bir yöntem ile benimsemeli ve uygulamalıdır (Şahinaslan vd., 2010). Susanto vd. (2011) çalışmalarında, ISO27001, BS 7799, PCIDSS, ITIL ve COBIT standartlarını, bilgi güvenlik politikaları, erişim kontrolü, bilgi güvenlik organizasyonu, varlık yönetimi gibi on bir konu bakımından karşılaştırmalı olarak incelemiştir. Günümüzde NIST, COBRA, OCTAVE, FRAP, Risk Watch gibi risk yönetim yöntemleri tespit edilen riskleri nicel ya da nitel olarak ifade edip bir risk değerlendirmesi sunmaktadır (Elky, 2006). Tablo 2'de basit bir risk yönetim örneği görülmektedir. Örnekte başlangıçtaki risk düzeyi "orta" iken risk yönetim stratejisinin gerçekleştirilmesi durumunda "düşük" seviyesine gerilediği görülmektedir.

Tablo 2: Risk yönetim tablosu örneği

Risk	Risk Tanımı	Etki	Olasılık	Strateji	Maliyet	Kalan risk
Orta	Çevresel birimlerin başarısızlığı (klima arızası)	Sistemin 48 saatten fazla devre dışı olmasına neden olabilir.	Geçmiş verilere göre yılda 1- 2 kez olabilir.	Alternatif bir yerde yedek oluşturma	$250,000	Düşük

Günümüzde Art of Risk, Real ISMS, ISMart, Callio gibi çeşitli risk yönetim yazılımları mevcuttur. Bunlar farklı programlama dilleri ve veri tabanı yönetim sistemleri kullanılarak uluslararası standartlara bağlı kalınarak geliştirilmiş açık kaynak kodlu olmayan yazılımlardır. Bu çalışmada bu programlara alternatif olabilecek yerli ve açık kaynak kodlu bir BGYS yazılımı geliştirilmiştir.

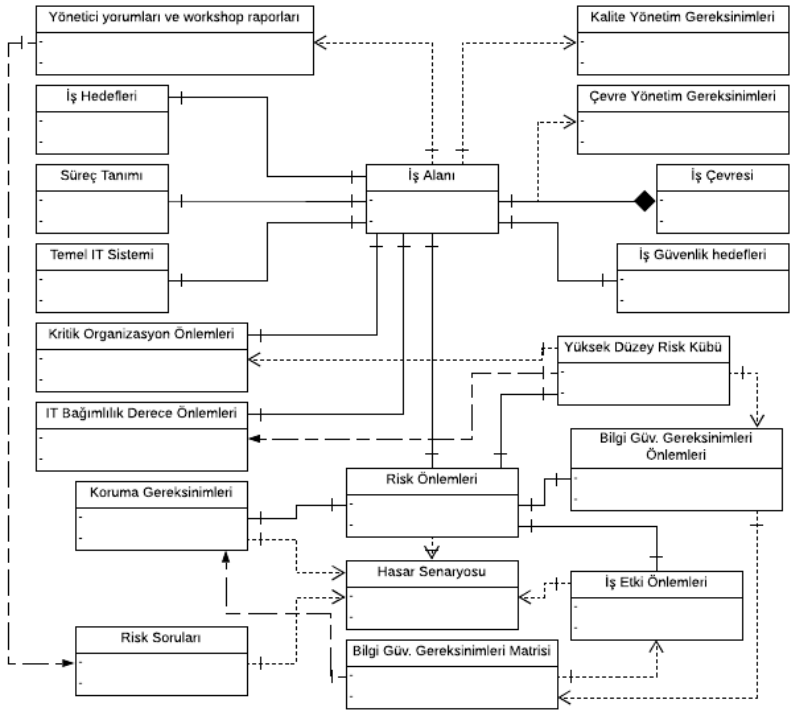
3. GELİŞTİRİLEN BGYS YAZILIMI

BGYS organizasyonun genel yönetim sisteminin bir parçasıdır ve işletme ihtiyaçları ile mevcut riskleri yansıtmalıdır. Bilgi güvenliği ile iş süreçleri arasındaki tüm ilişkiler eksiksiz şekilde tanımlanmalıdır. Bu ilişkileri doğru şekilde ifade etmek için Bialas (2005) gerçekleştirdiği çalışmasında, PUKÖ modeline dayanan bir BGYS yazılımı geliştirmek için UML (Unified Modelling Language) yaklaşımı ortaya koyarak iş alanlarını kapsayan bir iş ortamı sınıfı

tanımlamıştır (Şekil 3). Buna göre "İş çevresi", güvenlik gereksinimlerini ifade eden "İş güvenlik hedefleri" grubuyla incelenmiştir. İş çevresinin belirlenmesi "Yüksek düzey risk analizi" ile ilgilidir ve risk konuları ile ilgili bilgiler organizasyon içinde yapılan görüşmeler ve iş atölyeleri ile elde edilir. Bu bilgiler "İş alanı" nitelik kümesi ile temsil edilir. Elde edilen küresel risk değeri, "yüksek düzey risk kübü" ile ifade edilir.

İş hedeflerini sağlayan tüm iş süreçleri analiz edilmeli ve organizasyon için önemleri değerlendirilmelidir. Bir diğer nokta ise bu sürecin gelişiminde IT sistemlerinin katılım düzeylerinin belirlenmesidir. Güvenlik özellikleri ile ilgili koruma ihtiyaçları, yani bilgi bütünlüğü, kullanılabilirliği ve gizliliği, iş süreçlerinin her biri için tanımlanmalıdır. Bu niteliklerin kaybından kaynaklanan ticari etki, önceden tanımlanmış zarar senaryoları kullanılarak analiz edilir. "Koruma gereksinimleri", güvenlik özeliklerine ilişkin koruma gereksinimleri ve bu niteliklerin değer kaybından kaynaklanan ticari etkilerden türetilir. Bu gereklilikler, önceden tanımlanmış risk değerlerinin varsayılan matrisine dayanır. Bilgi güvenliği koruma gereksinimleri, kritiklik düzeyi ve BT bağımlılığı derecesi ile iş alanındaki yüksek düzeyli riskin üç boyutlu bir ölçüsüdür. Bu ölçü risk küpü olarak ifade edilmiştir. Buna ek olarak, bilgi güvenliği gereksinimleri, her nitelik için ayrı olarak düşünülür ve bütünlük, gizlilik ve erişilebilirlik kesitleri içindeki riski izlemeye imkan tanır.

Şekil 3: BGYS iş çevresinin genel yapısı



Bialas (2005)'in çalışmasındaki UML yapısı ve diğer BGYS standartları dikkate alınarak geliştirilen BGYS yazılımda C# programlama dili ve SQL Server veri tabanı yönetim sistemi temel programlama yapısını oluşturmaktadır. BGYS sistemi bir biri ile ilişkili verileri içerdiği için ilişkisel veri tabanı sistemi kullanılmıştır. Yazılımın ilişkisel veri tabanında oluşturulan tablolar aşağıda verilmiştir.

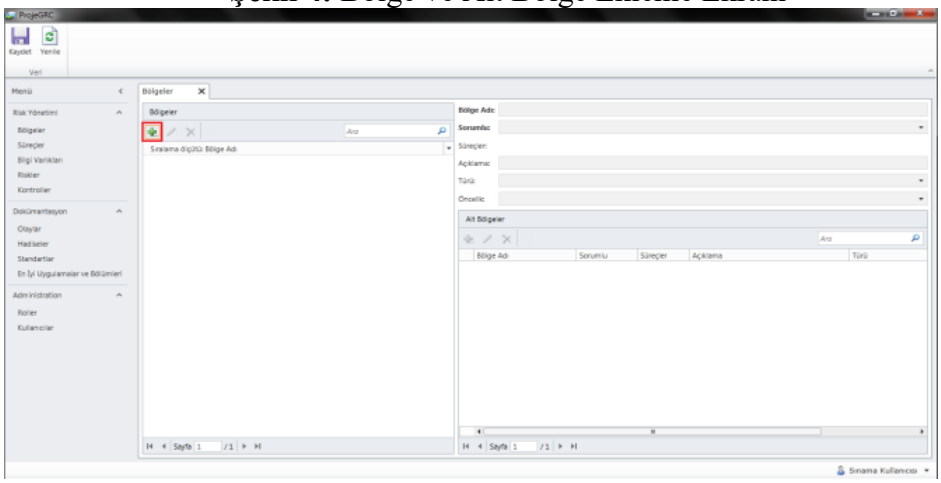
- Bölgeler tablosu, Bölge türleri tablosu, Bölge öncelikleri tablosu,
- Süreçler tablosu, Süreçlere atanan bilgi varlıkları tablosu, Süreç türleri tablosu,
- Bilgi varlıkları tablosu, Bilgi varlıkları kategorisi tablosu,
- Riskler tablosu, Risk türü tablosu,
- Kontroller tablosu, Kontrol türleri tablosu, Kontrollere atanan riskler tablosu

Geliştirilen yazılımda kullanıcılara çeşitli yetkiler atanmıştır. Yazılım sürecinde kurum içindeki varlıklar ve riskler zamanla değişim gösterebileceğinden dolayı dinamik bir yapıya sahip olacağı için kategori, alt kategori, varlık, risk gibi öğeleri oluşturmaya yetkili kişiler bu öğelere ekle, sil, güncelle gibi işlemlerle müdahale edebileceklerdir. Yazılımın en önemli kısmı risk yönetimi aşamasıdır ve kategori (bölge), alt kategori (alt bölge), süreçler, bilgi varlıkları, riskler ve kontroller olmak üzere 6 temel öğeden oluşmaktadır.

3.1. Kategoriler (Bölgeler) ve Alt Kategoriler (Alt Bölgeler)

Bu kısmı kullanmaya yetkili kişi kurum içindeki bölgeleri ve alt bölgeleri oluşturma, silme ve değiştirme hakkına sahiptir. Bölge adı, sorumlu kişi, türü (fabrika, merkez, ofis vb.), öncelik (öncelik derecelendirmesi orta, düşük, yüksek vb.) gibi alanlardan oluşmaktadır. Yazılımda yer alan öğeler içerisinde en öncelikli oluşturulması gereken kısımlar bölgeler ve alt bölgelerdir. Şekil 4'te programın bölge ve alt bölge ekleme sayfası yer almaktadır.

Şekil 4: Bölge ve Alt Bölge Ekleme Ekranı

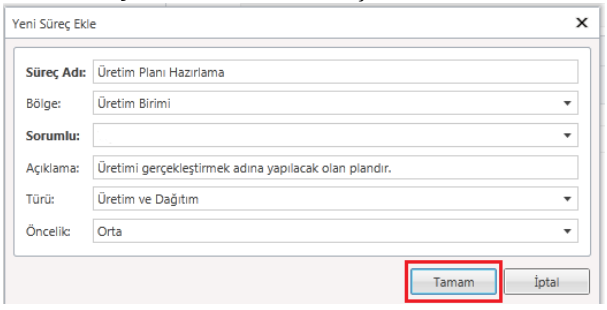


Örneğin bölge adı "İstanbul ana merkez", alt bölge adı "üretim birimi" olarak tanımlanabilir. İlişkisel veri tabanı yapısı sayesinde üretim birimi İstanbul ana merkeze bağlanacaktır.

3.2. Süreçler

İlgili alt bölgeye çeşitli süreçler atanabilir. Bunun için önce süreç oluşturulması gerekmektedir. Süreçler formunda süreç adı, öncelik, tür (çevre, sağlık ve güvenlik, muhasebe ve finans, insan kaynakları vb.) gibi alanlar yer almaktadır. Şekil 5'te süreç ekleme sayfası görülmektedir.

Şekil 5: Yeni Süreç Ekleme Ekranı



Örneğin "üretim birimi" alt bölgesine "üretim planı hazırlama" adlı süreç atanmıştır.

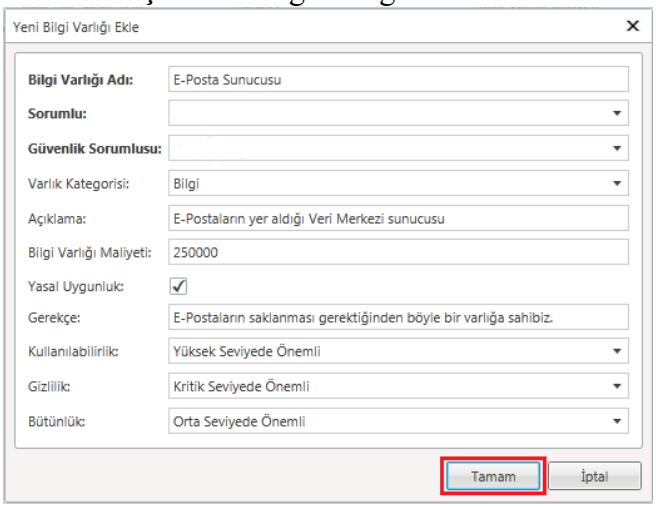
3.3. Bilgi Varlıkları

Bilgi varlığı ekleme ekranında;

- Bilgi varlığının adı, sorumlu kişi, maliyet, gerekçe,
- Güvenlik sorumlusu (varlıkla ilgili güvenlik kısmından sorumlu olan kişi),
- Varlık kategorisi (bilgi, hizmetler, insanlar, maddi varlıklar, maddi olmayan varlıklar, yazılım varlıklar),
- Yasal uygunluk (varlığın bir yasal zorunluluktan mı yoksa şirket politikasınca mı eklendiği),
- Kullanılabilirlik (önemsiz, düşük seviyede önemli, orta seviyede önemli vb. seçeneklerle bilgi varlığı talep gördüğünde kullanılabilir olma durumu),
- Gizlilik (önemsiz, düşük seviyede önemli, orta seviyede önemli vb. seçeneklerle bilgi varlığının gizlilik seviyesi),

gibi alanlar yer almaktadır. Oluşturulan bilgi varlığı bir sürece eklenmelidir. O yüzden süreçler ekranına geçip bilgi varlığı bir sürece atanmalıdır. Şekil 6'da bilgi varlığı ekleme sayfası görülmektedir.

Şekil 6: Bilgi varlığı ekleme ekranı

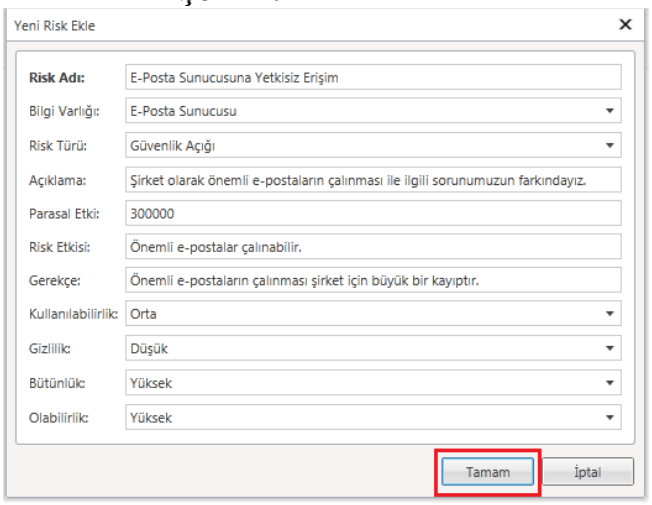


Örneğin "E-Posta Sunucusu" bilgi varlığı oluşturulmuş ve "Üretim planı hazırlama" adlı sürece dâhil edilmiştir.

3.4. Riskler

Risk ekleme ekranında; risk adı, bilgi varlığı, risk türü (güvenlik açığı, olay, tehdit), parasal etki, risk etkisi (riskin gerçekleşmesi sonucunda ortaya çıkaracağı olumsuz etki), gerekçe, kullanılabilirlik, gizlilik, bütünlük, olabilirlik (riskin gerçekleşme olasılığı) gibi alanlar bulunmaktadır. Şekil 7'de risk ekleme sayfası görülmektedir.

Şekil 7: Risk Ekleme Ekranı

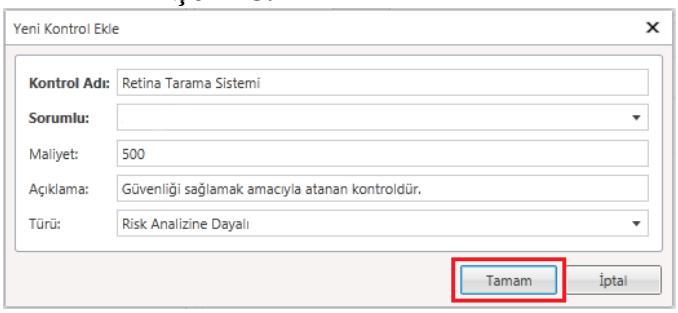


Örneğin "E-Posta sunucusuna yetkisiz erişim" adlı bir risk tanımlanmıştır ve önceden tanımlanan E-Posta sunucusu adlı bilgi varlığı ile ilişkilendirilmiştir.

3.5. Kontroller

Bilgi varlıklarını korumak amaçlı alınacak tedbirleri içeren kısımdır. Kontroller bilgi varlığının türüne ve oluşabilecek riske göre belirlenmektedir. Şekil 8'de yeni bir kontrol ekleme sayfası görülmektedir.

Şekil 8: Kontrol Ekleme Ekranı



Kontrole ait bir risk eklenmesi gerekmektedir. Bunun içinde "yeni risk kontrolü ekle" sayfasından kontrole bir risk atanması gerekir. Örneğin "retina tarama sistemi" adlı kontrol "E-Posta sunucusuna yetkisiz erişim" adlı risk ile ilişkilendirilmektedir.

4. SONUÇ

Bu çalışmada ISO/IEC 27001 standardı dikkate alınarak kurumlar ve firmalar için bir BGYS yazılımı geliştirilmiştir. Özellikle bir BGYS sisteminin omurgasını oluşturan risk yönetimi aşaması ilişkisel veri tabanı kullanılarak tasarlanmış ve yazılım geliştirme aşamasında C# dili ve yardımcı bazı yazılım araçları kullanılmıştır. Çalışma açık kaynak kodlu bir çalışma olup ticari olarak sunulan yazılımlara alternatif yerli bir yazılım olarak yerini almıştır. Özellikle BGYS sistemini kurumuna ya da firmasına kurmak isteyenlere BGYS siteminin aşamaları ve bir BGYS yazılımının içeriği hakkında fikir vereceği düşünülmektedir. Günümüzde özellikle KOBİ ölçeğindeki firmaların kurumsallaşması yönünde atacağı adımlarda BGYS uygulamalarının benimsenmesi firmaların geleceği açısından büyük önem taşımaktadır. Çalışmanın BGYS sistemi uygulamak isteyen tüm kurum ve firmalar için küçük bir rehber olacağı düşünülmektedir. BGYS sistemi geliştirecek araştırmacılara bulut sistemleri üzerinde geliştirilecek BGYS sitemlerine yönelmeleri

önerilmektedir. 11 Eylül saldırılarında Dünya ticaret merkezinde (World Trade Center) bulunan yüzlerce firma, verilerinin yedeklerini farklı bölgelerde bulundurmadıkları için büyük problemler yaşadılar. Gelecek süreçte firmaların benzer problemlerle karşılaşmayacaklarının garantisi verilemeyeceği için özellikle günümüzde hızla gelişen bulut teknolojileri ve güvenliği konularında çalışmalar yapılabilir.

KAYNAKÇA

Białas, A. (2005). A UML Approach in The ISMS Implementation. In Security Management, Integrity, and Internal Control in Information Systems (pp. 285-297). Springer, Boston, MA.

Broderick, J. S. (2006). ISMS, Security Standards and Security Regulations. Information Security Technical Report, 11(1), 26-31.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9(3).

Chang, H. (2013). Is ISMS For Financial Organizations Effective on Their Business?. Mathematical and Computer Modelling, 58(1-2), 79-84.

Dünya ISO/IEC 27001 İstatistikleri ve Türkiye'nin Konumu (2016). https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/dunya-iso-iec-27001-istatistikleri-ve-turkiyenin-konumu.html+&cd=1&hl=tr&ct=clnk&gl=tr Erişim Tarihi: 05.01.2016

Elky, S. (2006). An Introduction to Information System Risk Management. SANS Institute InfoSec Reading Room, pp.11.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). ISMS Core Processes: A Study. Procedia Computer Science, 100, 339-346.

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. In System Sciences (HICSS), 49th Hawaii International Conference on (pp. 4842-4848). IEEE.

ISO. (2005a). ISO/IEC 27001:2005. Information Technology- Security Techniques - Information Security Management Systems - Requirements. Geneva: International Organization for Standardization.

Li, S. H., Yen, D. C., Chen, S. C., Chen, P. S., Lu, W. H., & Cho, C. C. (2015). Effects of Virtualization on Information Security. Computer Standards and Interfaces, 42, 1-8.

Marttin, V., & Pehlivan, İ. (2010). ISO 270012005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. Mühendislik Bilimleri ve Tasarım Dergisi, 1(1).

Öner, D., & Dinçkan, A., (2007). TUBİTAK-UEKAE Bilgi Güvenliği Yönetim Sistemi Kurulumu Eğitim Dökümanı.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of The Big Five. International Journal of Electrical Computer Sciences , 11(5), 23-29.

Şahinaslan, E., Kandemir, R., & Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme. ABGS 2010–Ağ ve Bilgi Güvenliği Sempozyumu, Ankara.

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. https://www.tse.org.tr/tr/icerikdetay/2311/6890/ts-isoiec-27001-bilgi-guv--yonetim-sistemi-.aspx Erişim Tarihi. 05.07.2016

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of Risk Management Implementation for Industry 4.0. Procedia Manufacturing, 11, 1223-1230.