Journal of Humanities and Tourism Research

Araştırma Makalesi

Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme

Conceptual Review for Implementation of ISO/IEC 27001 and ISO 22301 for Information Security and Business Continuity in the Banking Sector

Oya GAZDAĞI[1], Tahsin ÇETİNYOKUŞ[2]

[1] Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, Türkiye

[2] Gazi Üniversitesi, Mühendislik Fakültesi Endüstri Mühendisliği Bölümü, Ankara, Türkiye

ORCID
O.G.: 0000-0001-6807-8734
T.Ç.: 0000-0002-9963-5174

Corresponding Author:
Tahsin ÇETİNYOKUŞ

Email: tahsinc@gazi.edu.tr

Citation: Gazdağı, O. ve Çetinyokuş, T. (2020). Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme. *Journal of Humanities and Tourism Research*, 10 (2), 475-491.

Submitted: 07.11.2019
Accepted: 22.06.2020

Özet

Gelişmekte olan bilgi ve iletişim teknolojileri günlük yaşamımızda vazgeçemediğimiz araçlar haline dönüşmektedir. Bilgi sistem arayüzleriyle son kullanıcı karşısına çıkan uygulamalar, mümkün olduğunca fazlaca veriyi yakalamak ve saklamaktadırlar. Müşteri beklentilerini karşılayarak muhtemel kayıpları önlemek iyi bir strateji iken bu teknolojileri kullananlar, kişi ve kurumlardan elde ettikleri bilgilerin güvenliği konusunda da sorumludurlar. Müşteri ilişkilerinin yoğun olduğu bankacılık sektöründe bahsedilen kullanıcılara dahildir. Bilgilerin etkin bir şekilde korunabilmesi için "Bilgi Güvenliği Yönetim Sistemi" kurulması ve kullanılması, akılcı bir yaklaşım olacaktır. Günümüzde bilgi güvenliği kadar önemli bir diğer konu da iş sürekliliği olduğu düşülmektedir. Bankalar gerçekleştirdikleri işlemlerin önemi sebebiyle, iş sürekliliğinin sağlanması gereken kurumlar arasında önde gelirler. Bankaların yaşayacağı iş kesintileri hem bankalara hem müşterilere hem de ülkemize büyük zararlara yol açmaktadır. Bilgi güvenliği yönetiminde de olduğu gibi etkin bir "İş Sürekliliği Yönetim Sistemine" sahip olmayan bankalar hem yasal (kanuni) hem de itibari olarak büyük zararlara uğramaktadır. COVID19 pandemi nedeniyle yaşadığımız zorunlu ve hızla dijital dönüşüm sürecinde, bahsedilen konu başlıklarının önemi göz ardı edilmemelidir. Bu çalışmada ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı ve ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Sistemi Standardının bankacılık sektöründe uygulanması ve sonuçları tartışılmıştır. Sonuçta bankaların "Bilgi Güvenliği Yönetim Sistemi" ve "İş Sürekliliği Yönetim Sistem"lerini kurarken dikkate alabilecekleri hususlar sunulmuştur.

***Anahtar Kelimeler**: İş Sürekliliği Yönetim Sistemi, Bilgi Güvenliği Yönetim Sistemi, Bilgi Güvenliği ve İş Sürekliliği, Süreç Yönetimi*

Abstract

The use of emerging information and communication technologies has become indispensable tools in our daily life. Applications, information systems interface with opened to end users, capture and store data as possible. It is good strategy to avoid loss of customers to meet customer expectations for using this technology, but they are responsible for the security of the information they receive from individuals and institutions. The banking sector, which has intense customer relations, is also included in mentioned user. Set up and use "Information Security Management System" for sufficient protection of

information located in banks will rational approach. Today, another important topic as information security is business continuity. Because of the importance of the performed, banks are one of the leading institutions among the others that need to ensure business continuity. The business interruption of the banks experiencing causes considerable damages to customers, banks and our country. As with the management of the information security, banks which do not have an effective 'Business Continuity Management System' results in exposure of banks to statutory and reputational damages. Therefore, what needs to be done to create a 'Business Continuity Management System' effectively and to bring into compliance with ISO 22301 Social Security and Business Continuity Management System Standard used in the banking sector and the key items of ISO 22301 Social Security and Business Continuity Management System Standard have been examined in detail. The importance of the mentioned topics should not be ignored during the mandatory and rapid digital transformation process we experience due to the COVID19 pandemic. In this study, the ISO / IEC 27001 Information Security Management Standard and ISO 22301 Social Security and Business Continuity Management System Standard implementation and results in the banking sector were discussed. As a result, the issues that banks can consider while establishing the "Information Security Management System" and "Business Continuity Management System" are presented.

***Keywords**: Business Continuity Management System, Information Security Management System, Information Security and Business Continuity, Process management*

1. GİRİŞ

Günümüzde tüm kamu kuruluşları ve özel şirketler çalışmalarını sürdürebilmek için bilgiye ihtiyaç duyarlar. İşlerinin gerekliliklerini yerine getirmek için kullanıldıkları bilgileri gereğince saklamayan kurumlar büyük maddi zararlarla karşılaşılabilirler. Çağımızın popüler konusu haline gelen bilgi güvenliği kavramı özellikle bankalar için hayati öneme sahip bir kavramdır ve teknolojinin gelişmesi ile de günden güne önemi daha fazla artmaktadır.

Bankalar bilgi ve iletişim teknolojilerinin gelişmesiyle günümüzde artık tüm bankacılık faaliyetlerini bilişim sistemleri aracığıyla gerçekleştirmektedir. Bankalara büyük kolaylık ve hız sağlayan bilişim teknolojisindeki gelişmeler aynı zamanda bilişim suçlarını da beraberinde getirmiştir. Günümüzde meydana gelen bilişim suçları diğer adıyla siber saldırıların en büyük hedeflerinden biri bankalardır. Bankalar gerçekleştirdikleri bankacılık işlemleri nedeniyle müşterilerine ait pek çok gizli bilgiye sahip olurlar. Sahip olunan bu gizli müşteri bilgilerinin etkin şekilde korunmaması bankaları hem yasal hem de itibari olarak büyük zararlara uğratmaktadır. Bu zararların telafisi oldukça güç hatta imkânsızdır. Bankalarda yer alan gizli bilgilerin gereğince korunması ancak etkin bir "Bilgi Güvenliği Yönetim Sistemi (BGYS)" ile yapılabilmektedir. Günümüzde bilgi güvenliği kadar önemli bir diğer konu da iş sürekliliğidir. Bankalar gerçekleştirdikleri işlemlerin önemi sebebiyle, iş sürekliliğinin sağlanması gereken kurumlar arasında önde gelmektedirler.

İlgili alanda literatür incelendiğinde; Ganbat (2013) ISO/IEC 27001 standardı ve BGYSnin temelini oluşturan Planla/Uygula/Kontrol Et/Önlem Al (PUKÖ) döngüsünün her bir safhasında elde edilen çıktılar sunmuş ve uygulama gerçekleştirecek kurumlara tavsiyelerde bulunmuştur. Susanto vd. (2011) bilgi güvenliği için geliştirilen IS0 27001, BS 7799, PCI DSS, ITIL ve COBIT standartlarını karşılaştırmıştır. Gencer (2015) kurumlarda ISO/IEC 27001 standardı kapsamında dinamik bir yaklaşım önermiştir. Bilgi Güvenliği Yönetmeliğinden bahsedilerek sistemin kurulması ve bakımının bir kültür haline getirilmesi gerektiğini vurgulamıştır. Aydemir (2013) İstanbul'daki Metro sisteminin güvenliği ve güvenirliği noktasında hizmet kesintisini sıfıra indirmek için önerilerde bulunmuştur. İş sürekliliği standartları ve sağlanması için başarı faktörlerini sıralamıştır. Disterer (2013) kurumlarda etkin bir BGYS yapısının kurulması için ISO/IEC 27000, ISO/IEC 27001 ve ISO/IEC 27002 standartlarının nasıl uygulanacağı konusunda bilgilendirme yapmıştır. Eren (2013) Türkiye Sigorta Sektöründe faaliyet gösteren bir sigorta şirketi tarafından 2012 yılında gerçek zamanlı olarak yürütülen iş süreklilik tatbikatı, örnek vaka olarak makale içerisinde ayrıntılı bir şekilde incelemiştir. Karaağaç (2013) iş Sürekliliği Yönetimi ve Kriz Yönetimi arasındaki ilişkiye yönelik "Kriz İletişimi"ne dair temel gereklilikleri ortaya

koymaya çalışmıştır. Komut, (2013) şirketlerin hangi tür risklere maruz kalabileceği ve bu tür risklere karşı önceden hazırlıklı olmadıkları sürece varlıklarını sürdürebilmelerinin imkânsız olduğu ve risklere karşın etkin bir İş Sürekliği Yönetim Sistemi yapısı kurmaları gerektiğinden bahsetmiştir. Özgen (2013) iş sürekliliği stratejilerinin belirlenmesine yönelik süreçleri açıklayarak İzlanda'nın yaşadığı büyük ekonomik sıkıntılar ve kriz ortamında alınan yanlış kararları örnek bir vaka olarak ele almış ve iş sürekliliği kavramının özellikle bankalar için önemini vurgulamıştır. Haklı (2012) kamu kuruluşlarında uygulanabilecek yeni bir bilgi güvenliği modeli önermiş ve bu modelin nasıl kullanılacağını detaylı bir şekilde açıklamıştır. Bingöl (2010) BGYSni yönetmek amacıyla kullanılan alt yazılım araçlarını tanıtarak, sanal bir firma ve hayali veriler oluşturarak, sanal bir yazılım firmasının içerisine BGYS yapısının kurulmasını aşama aşama anlatan örnek bir uygulamaya yer vermiştir. Özbilgin ve Özlü (2010) ISO/IEC 27001 BGYS standardını güvenlik unsurlarının yönetilmesi için rehber olarak sunmuş ve yazılım geliştirme süreçlerinde uygulanması gereken güvenlik gereksinimlerini ele almıştır. Akpınar(2009), enformasyon teknolojisinin tarihsel gelişimi ile doğru orantılı olarak İş Sürekliliği Yönetimi kavramı ve Felaket Planlaması kavramlarının ortaya çıkışı, devamında süreç içerisindeki farklı standart ve yapıları ele almıştır. Şahinaslan vd., (2009) bilginin korunması yolunda güvenlik unsurlarının en zayıf halkası olarak kabul edilen insanların, bilgi güvenliği farkındalık eğitimi programı hakkında bilgi vermiştir. Çetinkaya (2008) BGYS kurmanın tüm aşamaları ayrıntılı şekilde açıklandıktan sonra bu işlemin kurumlara sağlayacağı yararları sıralamıştır. Tekerek (2008) etkin bir bilgi güvenliği yapısının sağlanabilmesi için sadece teknik önlem almanın yetersiz olacağı ve bilgi güvenliği yapısının yaşayan bir süreç olarak düşünülmesi gerektiğini tartışmıştır. Vural ve Sağıroğlu (2008) kurumsal bilgi güvenliğini genel olarak incelemiş, bu kapsamda yapılan diğer çalışmaları özetleyerek mevcut bilgi güvenliği standartları ile yeni oluşturulmakta olan bilgi güvenliği standartlarını bu çerçevede ele alarak gözden geçirmiştir. Canbek ve Sağıroğlu (2006) bilişim teknolojilerinin bilgi üzerindeki etkilerini inceleyerek bilgi güvenliğini oluşturan ana unsurları açıklamış ve güvenliği oluşturabilmek için gerekli olan güvenlik süreçlerini özetlemiştir. Mittal ve Goel, (2005) Etkin bir İSYSnin nasıl olması gerektiğini anlatmış ve iş sürekliliği yönetiminin kurum ve devletler için önemini vurgulamıştır. Reynolds, (2004) İş sürekliliği yönetiminin kurum ve kuruluşlar için önemi, artık planın yalnızca bilgi teknolojileri ile ilgili bir sistem kurtarma planından ziyade tüm iş süreçlerini de kapsayan yeni bir yaklaşıma sahip olduğunu anlatmıştır. Ulusal ve uluslararası çalışmalar dikkate alınarak yorumlama yapıldığında her ikisi içinde anlamlı bir fark olmadığı ek olarak sektör, problem ve çözüm yöntemlerinin homojen olarak dağıldığı görülmektedir. Yapılan çalışma bu başlıklar altında özgünlük sağlamaktadır.

Bankaların yaşayacağı iş kesintileri hem bankalara hem müşterilere hem de ülkemizde büyük zararlara yol açmaktadır. Bilgi güvenliği yönetiminde de olduğu gibi etkin bir "İş Sürekliliği Yönetim Sistemi(İSYS)ne" sahip olmayan bankalar hem yasal (kanuni) hem de itibari olarak büyük zararlara uğramaktadır. Çalışmada ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı ve ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Sistemi Standardının bankacılık sektöründe uygulanabilirliği ele alınmıştır. Çalışma, literatür araştırması ve ondan elde edilen method, teknik ve alan bilgileri ile yöntem, bulgular ve sonuç kısımları ile tamamlanmıştır.

2. YÖNTEM

2.1. Bankacılık Sektörü, Bilgi Güvenliği ve Süreklilik

Çeşitli sembol, karakter, harf, rakam ve işaretlerden meydana gelen, farklı sensörlerden elde edilen, kendi başına bir anlam ifade etmeyen, ayrık ve nesnel edinim değerlerine veri tanımlaması yapılmaktadır. Nicel ve nitel olabilen veriler, bilgiye giden sürecin de temelini oluşturmaktadır. Günümüzde toplumlar, ülkeler hızla bilişim toplumu olma yolunda ilerlemektedir. Bu ilerlemenin sonucu olarak kişilerin, kurumların, ulusal kuruluşların ve ülkelerin varlıklarının temeli olan ve

stratejik öneme sahip olan bilgilerini sağlıklı bir şekilde korunması gerektiği yani bilgi güvenliği konusu gündeme gelmiştir. Bilgi güvenliği, bilişim dünyası içerisinde elektronik ortamlarda tutulan bilgilerin uygun şekilde saklanması, iletilmesi sırasında bütünlüğünün bozulmaması, üzerinde herhangi bir değişiklik yapılmaması ve buna benzer kavramları içeren çabaların tümü olarak tanımlanmaktadır. Bilgiye gelebilecek saldırılar, kişi ve kurumları büyük maddi ve manevi zarara uğratabilir ve hatta geri dönüşümü olmayan kayıplara yol açabilir. Tüm bu sebeplerden ötürü bilgi güvenliği üç temel amaç üzerine konumlandırılmıştır. Bunlar bilginin gizliliği, bütünlüğü ve kullanılabilirliğidir. Bilginin bu üç unsurunun korunmasının bilgi güvenliğinin amacına hizmet ettiği, bu üç unsurdan birinin ihlali durumunda ise bilginin korunamadığı anlamı çıkarabilir(Önaçan, 2015; Chouikha, 2016; Önel ve Dinçkan, 2007).

Özellikle bankacılık sisteminde bilginin korunması ve iş sürekliliğinin sağlanması azami önem taşımaktadır. Bankacılık sisteminde önemli bir yer tutan bilgi güvenliği ve iş sürekliliği kavramları kuruluşların yapılarına ve faaliyet alanlarına göre uygun yöntemler, politikalar, yazılım ve donanım desteği bir dizi denetimler ve iç güvenlik grupları gibi organizasyonların gerçekleştirilmesi ile sağlanabilir. Özellikle bankacılık sisteminde bilgi güvenliğinin sağlanması, iş kesintisi ve bilgi kayıplarının önlenmesi, iş sürekliliğinin sağlanması, maddi kayıplarının ve yasal yaptırımların önüne geçebilmek için büyük önem arz etmektedir.

Bankacılık sistemlerinde etkin bir bilgi güvenliği ve iş sürekliliği yapısının sağlanabilmesi için öncelikle BGYS ve İSYS yapısının kurulması gerekmektedir. BGYS tanım olarak bilginin gizliliği, bütünlüğü ve kesintisiz erişebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, üst yönetimce kabul edilmiş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünüdür. İSYS ise bankacılık operasyonlarının önceden tanımlanmış, kabul edilebilir bir düzeyde devamını sağlanmak amacıyla bankanın olaylara ve iş kesintilerine karşı planlama ve müdahale etme kapasitesidir. Bankacılık sisteminde sadece teknik önemler alarak bilgi güvenliği ve iş sürekliğinin sağlanmasının mümkün olmadığı, teknik önlemlerin yanı sıra BGYS ve İSYS kapsamında politika ve süreçlerin belirlenerek yaşayan bir süreç oluşturmanın gerektiği tüm dünyaca kabul edilmiş bir yaklaşımdır(Ersoy, 2012).

2.2. Bankacılık Sektöründe Bilgi ve İş Sürekliliği Yönetim Sistemlerinin Uygulanması

Veri bilgi dönüşümü ve saklanması hizmetlerini veren tüm sektörlerde BGYS sistematik bir şekilde tasarlanıp yürütülebilir. Bankacılık sektöründe etkin bir BGYS kurulması sürecinde, BGYS kurulacak bankanın tanınması, BGYS yönetecek kişilerin belirlenmesi ve rollerin atanması, varlık envanterinin oluşturulması, BGYS kurulumun değerlendirilmesi, dokümantasyonların tamamlanması ve son olarak gözden geçirme faaliyetleri ile sürekli iyileştirmenin sağlanması aşamaları kullanılabilir. (Dinçkan, 2008a; Dinçkan, 2008b; Dinçkan, 2010; Sağıroğlu ve Ersoy, 2007; Saymaz, 2012).

Birinci aşama bankacılık sektöründe yer alan ve BGYS kuracak olan bankanın ilk olarak gerçekleştirmesi gereken adım organizasyonun tanınmasıdır. Organizasyonun tanınması aşamasında bankanın güvenlik politikaları, iş süreçleri, banka içerisinde kullanılan yöntem ve prosedürlerin hepsi taranarak, BGYS kapsamına girdi olabilecek süreç ve politikalar belirlenmektedir (Saymaz, 2012).

İkinci aşamada banka içerisinde kurulacak BGYS yapısında görev alacak ekipler ve rolleri belirlenir. Rollerin belirlenmesi sırasında dikkat edilmesi gereken iki husus vardır. Bunlar kurulacak ekipler arasında rollerin belirlenmesi esnasında görev, yetki ve sorumluluk paylaşımlarının net bir şekilde yapılması herhangi bir karışıklığa yol açmayacak şekilde düzenlenmesidir. Bir diğer önemli husus ise bilgi güvenliği yönetim sistemi kapsamında ihtiyaç

duyulan tüm görevlerin atlanmadan belirlenmesi ve görev atamalarının net bir şekilde yapılmasıdır. Banka içerisinde BGYS yapısında yer alacak tüm ekiplerin görev ve sorumluluklarından haberdar olması sistem başarımı için son derece önemlidir (Saymaz, 2012).

Üçüncü aşamada banka içerisinde kurulacak BGYS' nin hangi alanlarda uygulanacağı, kapsamının ne olacağı belirlenir. Kapsam belirleme aşamasında kurumlar için dikkat edilmesi gereken husus kapsamın çok geniş tutulmaması, gerçekten gerekli alanlar için BGYS' nin kurulmasıdır. Çünkü BGYS kurulacak alanlar için kapsamlı olarak varlık envanteri oluşturulur ve risk analizi işlemleri gerçekleştirilir. Kapsamın kurum içerisinde geniş tutulması risk analizlerinin tekrar tekrar yapılmasına ve gereksiz dosya yığınlarına neden olabilir. Bunun için bankada kritik iş süreçleri ve bilgi varlıkları için BGYS'nin kurulması ve kapsamın bu bakış açısı ile belirlenmesi, kurumun zaman kaybı yaşamasını ve gereksiz maliyetlere katlanmasını önler (Saymaz, 2012).

Dördüncü aşamada banka içerisinde kurulacak BGYS için varlık envanteri oluşturulur. Sektörde varlık envanterinin oluşturulmasında kullanılan genel yapı kurum varlıklarının "Donanım", "Yazılım" ve "Bilgi" olarak temel üç sınıfa ayrılmasıdır (Sağıroğlu ve Ersoy, 2007).

Donanım Varlığı: Donanım varlık envanterinin oluşturulmasında BGYS kurulacak kurumun bilgi sistemleri ile ilgili tüm donanım varlıklarının listesi çıkarılır. Çıkarılan bilgi sistemleri donanım varlıklarının bilgi güvenliğinin temel üç ilkesi olan (CIA-Confident-Integrity-Avability) gizlilik, bütünlük ve erişebilirlik seviyeleri belirlenerek her bir donanım varlığının kritiklik ve gizlilik dereceleri yani puanları belirlenir. Kritiklik derecesinin belirlenmesinde bütünlük ve erişebilirlik kıstasları temel alınır (Saymaz, 2012).

Donanım Varlığı Kritiklik Seviyesi (Bütünlük + Erişebilirlik): Donanım varlıklarının kritikliği üç seviyede belirlenir. Bunlar yüksek, orta ve düşüktür.

Donanım Varlığı Gizlilik Seviyesi: Donanım varlıklarının gizliliği üç seviyede belirlenir. Bunlar çok gizli, gizli ve önemsizdir. Donanım varlıklarının gizlik derecesi, donamın üzerindeki bilgilerin yetkisiz kişiler tarafından ele geçmesi durumunda sistem güvenliğinin düşeceği duruma göre belirlenir (Sağıroğlu ve Ersoy, 2007).

Yazılım sınıfı ve Bilgi sınıfı ise yukarıda detaylı olarak yer alan Donanım sınıfı için bahsedildiği şekliyle aynı olarak değerlendirilir.

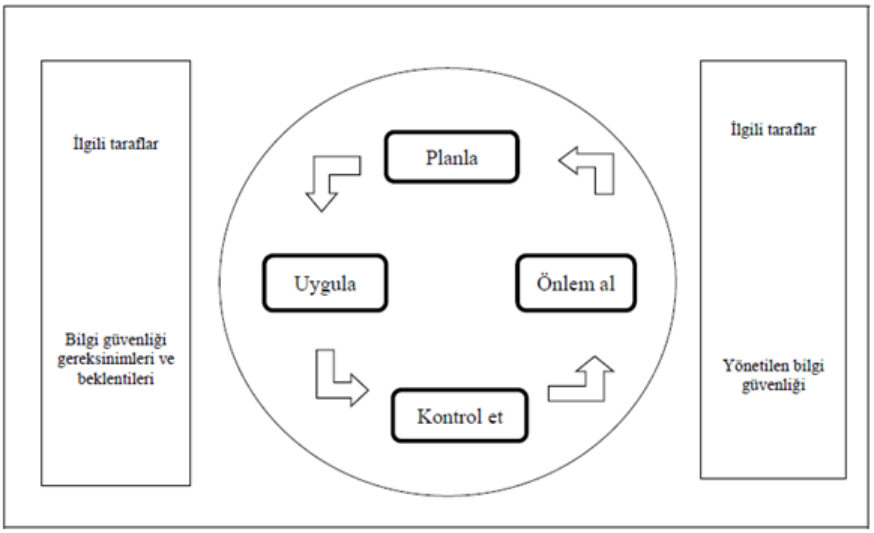
Beşinci aşamada kurulan BGYS'nin değerlendirmesi yapılarak sistemin etkinliği, yeterliliği ve yasal mevzuatlara uygunluğu değerlendirilmektedir. Süreç içerisinde iş etki analizleri, risk etki değerleri belirlenir.

Altıncı aşamada banka içerisinde yapılacak BGYS testlerin amacı kurumun bilgi güvenliği yönetiminde ne kadar etkili olduğunu belirlemektir. Bu testler sonucunda hangi bölümlerde eksikliğin olduğu belirlenerek ilgililere raporlanır. Ayrıca eksiklik sebepleri kök neden analiziyle araştırılarak bulunmaya çalışılır. Etkin bir bilgi güvenliği yapısının sağlanabilmesi için sadece teknik önlem almanın yetersiz olması sebebiyle bu aşama içerisinde banka çalışanlarının bilgi güvenliliği ile ilgili konularda farkındalık kazanması için eğitimlerin verilmesi de planlanır (Saymaz, 2012).

Yedinci aşamada banka içerisinde kurulan BGYS'nin etkin ve verimli bir şekilde uygulanması, sürdürülebilirliğinin sağlanması, kurum kültürü içerisine yerleştirilmesi için gerekli çalışmaların yapılması gerekmektedir. Sürekli iyileştirme yapısının sağlanabilmesi için etkin bir dokümantasyon sisteminin banka içinde kurulması, performans ve hedef yönetiminin belirlenmesi, bankanın belli periyotlarda BGYS bakımından denetlenmesi, banka süreçleri içerisine

BGYS için düzeltici ve önleyici faaliyetlerin yerleştirilmesi ve üst yönetim tarafından desteklenerek sürekli güncellenmesi gerekmektedir (Saymaz, 2012).

ISO/IEC 27001 standardının temel aldığı model ise PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) yaklaşımıdır. Planlama aşamasında standart içerisinde geçen Madde 4 - Kuruşun Bağlamı, Madde 5 - Liderlik, Madde 6 – Planlama, Madde 7 - Destek içerisinde yer alan gereksinimler karşılanırken, Uygulama aşamasında Madde 8 - İşletim, Kontrol Et aşamasında Madde 9 – Performans Değerlendirme ve son olarak Önlem Al aşamasında Madde 10 - İyileştirme içerisinde yer alan gereksinimler karşılanır. Bu modele göre belirlenecek döngünün, düzenli aralıklarla kurum, kuruluş ve işletmelerde gözden geçirilmesi gerekmektedir (Ersoy, 2012). PUKÖ döngüsünün özet yapısı Şekil 1.' de gösterilmiştir.



Şekil 1. PUKÖ Döngüsü

Planlama (BGYS'nin Kurulması, Hedef ve Önlemlerin Planlaması) PUKÖ modelinin ilk ve en önemli aşamasıdır. Bu aşamada güvenlik politikasının kurulması, amaçların, hedeflerin, süreçlerin ve prosedürlerin belirlenmesi işlemleri gerçekleştirilir. Planlama aşamasında konulan hedeflerin kurumun tüm amaç ve politikalarına uygun olması başarının sağlanması için en önemli gereksinimdir. Planlama aşamasında her noktanın düşünülmesi, görev dağılımlarının ve hedeflerin düzgün olarak belirlenmesi PUKÖ modelinin son adımı olan Önlem Al aşamasında yapılacak işlemleri en aza indirecektir. PUKÖ modeli her ne kadar eşit parçalıymış gibi sunulsa da Planlama safhası aslında döngünün en büyük alanını göstermektedir. Planlama aşaması içerisinde Kapsam, Politika, Risk Değerlendirme, Risk İyileştirme Planı ve Uygulanabilirlik Beyanı işlemleri tanımlanır (Çalık, 2013; Ersoy, 2012; Inform, 2016; TK01, 2013a; TK01, 2013b).

•Kapsamın belirlenmesi aşamasında BGYS'nin kapsadığı alanlar, donanım, yazılım, bilgi varlıkları ve teknolojiler belirlenir.

•İşin karakteristiğine, organizasyona, organizasyon varlıklarına ve teknolojilerine göre BGYS politikaları tanımlanır.

•Risk Değerlendirme aşamasında belirlenen politikalar dahilinde hedefler, oluşabilecek risk kriterleri tanımlanır. Risk Değerlendirme aşamasında BGYS kapsamında olan varlıkların karşılaşılabileceği tehlikeler, bu tehlikelerin olma olasılığı, riskin gerçekleştiğinde oluşturacağı zararlar varlık sahipleri tarafından belirlenir.

•Bu aşamada risklerin çözümlenmesi ve değerlendirilmesi işlemleri yapılır. Yapılan değerlendirilmelere göre, risk opsiyonları tanımlanmakta ve değerlendirilmektedir.

Risk iyileştirme aşamasında risklerin tanımlanması ile ilgili kullanılan üç temel kavram vardır. Bunlar "risk yönetimi", "riskin kabulü" ve "risk iyileştirme"dir.

*Risk yönetimi; risklerin tanımlanması, analizi, değerlendirmesi, risklere müdahale edilmesi ve kontrolü gibi işlevler için yönetim kültürü, politikası, prosedürleri ve uygulamalarının yapısal olarak geliştirilmesi ve yürütülmesidir.

*Riskin kabulü, belirli bir riskin etkisini hafifletmek için hiçbir harekette bulunmamaya ilişkin bir yönetim kararıdır.

*Risk iyileştirme, riski azaltamaya yönelik önlemlerin seçilmesi ve uygulanmasıdır.

Uygulama (Bilgi Güvenliği Yönetim Sisteminin Gerçekleştirilmesi ve İşletilmesi):PUKÖ döngüsünün Uygulama safhası, ilk aşamada planlanan faaliyetlerin gerçekleştirildiği aşamadır. Bu safhada genellikle bir deney düzeneğiyle ya da küçük ölçekli bir test gerçekleştirilir. Uygulama aşamasında, risk analizinde elde edilen sonuçlara göre standardın ön gördüğü kontrol maddeleri uygulanır. Uygulama aşamasında güvenlik politikasının, denetimlerin, süreçlerin ve prosedürlerin ayrıntıları oluşturularak işleme alınır. İşletim sırasında ortaya çıkan eksiklikler tespit edilerek dokümante edilir ve iyileştirme aşamasında bu tespitler kullanılır. Uygulama aşaması içerisinde "Kontrollerin İşletilmesi", "Farkındalık Eğitimi" ve "Kaynak Yönetimi" işlemleri gerçekleştirilir(Çalık, 2013; Ersoy, 2012; Inform, 2016; TK01, 2013a; TK01, 2013b).

•Kontrollerin işletilmesinde riskleri minimize etmek ve kontrol amaçlarını karşılamak için daha önce seçilen kontroller uygulanır.

•Farkındalık eğitimi aşamasında farkındalık eğitim programları geliştirilir ve uygulanır.

•Kaynak yönetiminde kurum içerisinde belirlenen risk yönetim planına uygun olarak yönetim aksiyonları, kaynaklar, sorumluluk ve öncelikler tanımlanır.

Kontrol Etme (Bilgi Güvenliği Yönetim Sisteminin İzlenmesi ve Gözden Geçirilmesi) başlığı altında güvenlik politikasının değerlendirilmesi, alınan önlemlerin ne kadar işe yaradığının ölçülmesi, hedeflerin ve amaçların gözden geçirilmesi ve raporların oluşturulması aşamasıdır. Böylece planlanan hedeflere ne kadar ulaşıldığı belirlenir. Eğer planlanan hedeflere ulaşıldıysa yapılan uygulama faaliyetleri standartlaştırılır. Kontrol Et aşamasında "BGYS'nin İç Denetimi" ve "BGYS' nin Yönetim Tarafından Gözden Geçirilmesi" işlemleri de gerçekleştirilir (Çalık, 2013; Ersoy, 2012; Inform, 2016; TK01, 2013a; TK01, 2013b).

•BGYS'nin iç denetimi aşamasında planlanan aralıklarla BGYS iç denetimi yapılır. İzleme ve gözden geçirme faaliyetlerindeki bulgular dikkate alınarak güvenlik planları güncellenir. İleride BGYS performansını ve etkinliğini etkileyecek eylemler ve olaylar kayıt altına alınır.

•BGYS'nin yönetim tarafından gözden geçirilmesinde yönetim, prosedürlerin ve diğer kontrollerin izlemesi ve gözden geçirilmesi işlemlerini yapar. Riskler ve kabul edilebilir risk derecelerinin işleyiş şekli gözden geçirilir.

Önlem alma (bilgi güvenliği yönetim sisteminin bakımının yapılması ve geliştirilmesi), gözden geçirme işlemlerinin sonucu esas alınarak Bilgi Güvenliği Yönetim Sisteminin düzeltilmesi, geliştirilmesi ve sürekliliğinin sağlanması için gerekli önlemlerin alınmasıdır. Uygulama aşamasında fark edilen aksaklıklar ve güvenlik zayıflıkları bu aşamada düzeltilmektedir. Önlem alma aşaması kendi içinde PUKÖ döngüsü içerir. Planlanan faaliyetler ile yapılan uygulamalar arasında ortaya çıkan farklılıkların, sapmaların nedenleri araştırılır ve bunların ortadan kaldırılmasına yönelik faaliyetler başlatılır. Önlem Al süreci, arzulanan etkiyi sağlamak ve değişimde yeni tanımlamalar yapabilmek için devamlı gözlemlenmelidir. Döngü

"Önlem Al" aşaması ile bitmez PUKÖ öğrenmek ve düzeltmek için sürekli bir döngüdür. Önlem Al aşamasında yapılan iki temel işlem BGYS' nin geliştirilmesi ve düzeltici faaliyetlerin uygulanmasıdır. Kazanılan tecrübeler doğrultusunda önleyici ve düzeltici adımlar atılır. İyileştirmelerin tasarlanan amaçlara ulaşması sağlanır. Eylemler ve iyileştirmeler tüm ilgili taraflara duruma uygun ayrıntı seviyesinde bildirilir ve gerekirse nasıl ilerleneceği konusunda anlaşmaya varılması sağlanır (Çalık, 2013; Ersoy, 2012; Inform, 2016; TK01, 2013a; TK01, 2013b). ISO/IEC 27001 standardının bileşenleri Tablo 1' de özetlenmiştir.

Tablo 1. ISO/IEC 27001 Bileşenleri

ISO 27001 BİLEŞENLERİNE GENEL BAKIŞ	
PLANLA	4 Kuruluşun İçeriği • İçeriği anlamak • İlgili tarafların beklentileri • Kapsam ve BGYS
	5 Liderlik • Yönetimin Katılımı • BG Politikası • Görevler, sorumluluklar ve yetkiler
	6 Planlama • Risk ve fırsatları ele almak için faaliyetler • BG amaçları
	7 Destek • Kaynaklar • Yetkinlik • Farkındalık • İletişim • Dokümante edilmiş bilgi
UYGULA	8 İşletim • Operasyonel planlama ve kontrol • Risk değerlendirme • Risk işleme
KONTROL ET	9 Performans ve Değerlendirme • İzleme, ölçme, analiz ve değerlendirme • İç tetkik • Yönetimin gözden geçirmesi
ÖNLEM AL	10 İyileştirme • Uygunsuzluklar ve düzeltici faaliyetler • Sürekli iyileştirme

Kaynak: (BGA, 2013)

Birinci Adım - Organizasyonun Tanınması: Bankacılık sektöründe yer alan ve İSYS kuracak bir kurumun ilk olarak gerçekleştirmesi gereken adım organizasyonun tanınmasıdır. Organizasyonun tanınması aşamasında banka, risk yönetiminin belirlenmesi, iş etki analizlerin yapılması, kapasite analizlerinin yapılması, yatırım analizlerin yapılması ve olay öncesi tüm hazırlık aşamalarının gerçekleştirilmesi işlemlerini tamamlamaktadır. Kısaca bu aşama da ilk olarak yapılması gerekenler;

•İSYS kurulacak bankanın verdiği bankacılık hizmetleri, ürün ve süreçlerinin tamamı,

•Teknolojik ve teknik altyapısı (hangi programlar kullanılıyor, hangi kuruluşlardan altyapı desteği alınıyor),

•Bankanın tüm çalışma lokasyonları (binalar, şubeler, ek hizmet binaları),

•Organizasyon şeması ve ayrıntıları,

•Personel sayısı ve personellerin hangi lokasyonlarda görev aldıkları,

•Paydaş yapısı,

•Bankanın uymakla yükümlü olduğu yasal müeyyidelerin neler olduğu BDDK 5411 Bankacılık Kanunu),

•Bankacılık hizmetlerinin durmasına sebep olabilecek olası riskler,

•Bankanın dışarıdan hizmet aldığı 3. Parti kuruluşların listesi temin edilmeli ve alınan hizmetlerin türü tanımlanmalıdır.

Risk kavramı "Bankanın amaç ve hedeflerini gerçekleştirmesini olumlu veya olumsuz etkileyecek, kayba ve kazanca yol açma ihtimali olan her türlü olay veya durum", İş Etki Analizi (İEA) ise "Olası kesintilerin ve iş aksamalarının iş süreçlerine ve kuruma olan etkilerinin analiz edilmesi" olarak tanımlanmaktadır(Dinçkan, 2008a; Altay, 2016). Risklerin belirlenmesi sırasında kullanılan en genel yaklaşımlardan biri risk değerlendirmesidir.

Risk Değerlendirmesi = "Olasılık"x"Etki"x"Mevcut Kontrollerin Yeterliliği"

şeklindedir. Burada bankanın mevcut risklerinin puanlama sistemiyle değerlendirmesi yapılır.

Tablo 2. Risk Değerlendirme Formu

Risk Değerlendirme Formu								
Tehdit	**Riskin Tanımı**	**Yasal**	**Etki**	**Olasılık**	**Mevcut Kontrol Yeterliliği**	**Puan**	**Mevcut Kontrol Tanımı**	**Aksiyon**
Sel	Sel sebebiyle BT altyapısının hizmet veremez hale gelmesi	Yok	3	2	1	6	Gerekli bariyer önlemleri alınmıştır.	Kritik Değil
Deprem	Deprem olması sonucu genel müdürlük binasının hizmet veremez hale gelmesi	Yok	4	3	1	12	Yedek bir bina deprem olasılığı az olan bir bölgede hazır halde bekletilmektedir.	Önemli

Örnek bir "Risk Değerlendirme Formu" Tablo 2'de gösterilmiştir (Altay, 2016).

Kaynak: (Altay, 2016)

Olasılıkların belirlenmesinde ise olayın olma ihtimaline göre olasılıklar "Düşük", "Orta" ya da "Yüksek" olarak sınıflandırılır. Sektörde kabul edilen olasılık tablosu yapısı Tablo 3'de gösterilmiştir.

Tablo 3. Olasılık Tablosu

Olasılık Tablosu		
Seviye	**Puan**	**Tanımı**
Yüksek	3	Olayın olma ihtimali yüksek ve gerçekleşme oranı %30'un üzerinde
Orta	2	Olayın olma ihtimali var ancak gerçekleşme oranı %30'un altında
Düşük	1	Olayın olma ihtimali çok düşük, gerçekleşme oranı %15' in altında

Etki değerinin belirlenmesinde ise olayın yaratacağı etki düzeyine göre "Düşük", "Orta" ya da "Yüksek" olarak sınıflandırılır. Sektörde kabul edilen etki tablosu yapısı Tablo 4'de gösterilmiştir.

Tablo 4. Etki Tablosu

Etki Tablosu		
Seviye	**Puan**	**Tanımı**
Yüksek	3	Kritik bankacılık süreçlerinde ciddi kesinti ve aksamalara sebep olur. Kesinti süresi 4 saati aşar. İtibar kaybı ve 50.000-TL üzerinde finansal kayba sebep olur.
Orta	2	Kritik bankacılık süreçlerinde kısmi kesintilere ve aksamalara sebep olur. Kesinti süresi 4 saati aşmaz. İtibar kaybı yaşanmaz fakat 0-50.000 arasında finansal kayıplar yaşanabilir.
Düşük	1	Kritik bankacılık süreçlerinde kesinti ve aksama yaşanmaz. Kesinti süresi 1 saati geçmez ve finansal ve itibari kayıp yaşanmaz.

Mevcut Kontrollerin Yeterliliği belirlenmesinde ise kontrollerin yeterlilik durumlarına göre "Düşük", "Orta" ya da "Yüksek" olarak sınıflandırılır. Sektörde kabul edilen kontrollerin yeterliliği tablosu yapısı Tablo 5.'de gösterilmiştir. Risk önceliklendirmesinde kullanılan yapı ise Etki * Olasılık şemalarında çeşitli kaynaklarda görülebilmektedir.

Tablo 5. Kontrollerin Yeterliliği Tablosu

Kontrollerin Yeterliliği Tablosu		
Seviye	**Puan**	**Tanımı**
Yüksek	1	Mevcut kontrol, riskin olma olasılığını ve/veya etkisini azaltmada yeterli ve etkin
Orta	2	Mevcut kontrol, riskin olma olasılığını ve/veya etkisini azaltmada kısmen yeterli ve etkin
Düşük	3	Mevcut kontrol, riskin olma olasılığını ve/veya etkisini azaltmada yetersiz

İkinci Adım-Senaryo ve Stratejilerin Belirlenmesi: İSYS' nin kurulmasındaki ikinci aşama senaryo ve stratejilerin belirlenmesidir. Senaryo ve stratejilerin belirlenmesinde risk analizi ve iş etki analizi çalışmaları sonucu elde edilen bilgiler kullanılır. Burada önemli olan senaryo ve strateji belirlerken her bir olay için ayrı ayrı senaryo ve stratejinin oluşturulmamasıdır. Çünkü böyle bir yapının banka gibi büyük bir kurumda yönetilmesi oldukça zordur. Örneğin yangın çıkması, siber saldırıların yaşanması, terör saldırıları gibi bankacılık faaliyetlerini etkileyecek sayısız olay ve senaryo yazmak mümkündür. Bu nedenle sayısız olay ve senaryo yazmak yerine genellikle bankacılık sektöründe kullanılan yapı olası yaşanacak olumsuz olayların etkileyebileceği temel alanları belirlemek ve bunlara karşı strateji geliştirmektir. Bankacılık sektörü içinde 4 temel alan sınıflandırılması yapılmaktadır. Bunlar çalışan yani insan kaynağı, çalışma yani üretim ortamı, kullanılan bilgi teknolojileri (Yazılım+donanım) ve son olarak üçüncü parti taraflardan yani tedarikçilerden alınan hizmetlerdir. Yaşanabilecek tüm olumsuz olaylar bankanın temel yapısını oluşturan bu 4 ana faktörden birini ya da birilerini etkileyecektir (Saymaz, 2012; Dinçkan, 2008a; Altay, 2016; ISO 22301, 2012). Bu nedenle oluşturulacak senaryo ve stratejilerin bu 4 ana faktörün çalışmaz hale gelmesi üzerine kurulmalıdır.

Bankacılık sektöründe kullanılan temel 10 senaryo örneği aşağıdaki gibidir (Saymaz, 2012; Dinçkan, 2008a; Altay, 2016; ISO 22301, 2012):

1. Senaryo, olaydan çalışma ortamının, BT sisteminin ve banka personelinin etkilenmemesi

2. Senaryo, olaydan çalışma ortamı, BT sisteminin etkilenmemesi ancak banka personelinin etkilenerek iş gücü kaybına yol açılması

3. Senaryo, olaydan çalışma ortamının ve banka personelinin etkilenmemesi ancak BT sistemlerinin etkilenmesi

4. Senaryo, olaydan çalışma ortamının etkilenmemesi ancak banka personelinin ve BT sistemlerinin etkilenmesi

5. Senaryo, olaydan çalışma ortamının etkilenmesi, BT sistemlerinin ve banka personelinin etkilenmemesi

6. Senaryo, olaydan çalışma ortamının ve banka personelinin etkilenmesi ancak BT sistemlerinin etkilenmemesi

7. Senaryo, olaydan çalışma ortamının ve BT sistemlerinin etkilenmesi ancak banka personelinin etkilenmemesi

8. Senaryo olaydan çalışma ortamının, BT sistemlerinin ve banka personelinin etkilenmesi

9. Senaryo, olayın firma itibarını ve imajını olumsuz etkilemesi

10. Senaryo, olayın banka için kritik olan tedarikçileri etkilemesi ve bu tedarikçilerin hizmet veremez hale gelmesi

Yukarıda belirtilen bu temel 10 senaryoya göre banka iş sürekliliği stratejileri geliştirilir. Bu stratejilerin her biri üzerinde çalışma planları yapılmalı süreç içerisinden meydana gelecek değişimlere göre dinamik B planları hazırlanmalıdır. Ele alınan tüm değerlendirme kriterleri tabii ki çeşitli hükümler ve standartların kısıtlaması altında olacaktır fakat kurumların farklı durumlar için senaryolar geliştirmesi çalışmaya konu olan bilgi güvenirliliği ve sürdürülebilirliğin teşkilinde esastır.

Üçüncü Adım-Rollerin Belirlenmesi: Bu aşamada banka içerisinde kurulacak İSYS yapısında görev alacak ekipler ve rolleri belirlenir. Rollerin belirlenmesi sırasında dikkat edilmesi gereken iki husus vardır. Bunlar kurulacak ekipler arasında rollerin belirlenmesi esnasında görev, yetki ve sorumluluk paylaşımlarının net bir şekilde yapılması herhangi bir karışıklığa yol açmayacak şekilde düzenlenmesidir. Bir diğer önemli husus ise İSYS kapsamında ihtiyaç duyulan tüm görevlerin atlanmadan belirlenmesi ve görev atamalarının net bir şekilde yapılmasıdır. Bankacılık sektöründe İş Sürekliliği Yönetim Sistemi için rollerin belirlenmesinde kullanılan temel yapı üç ana ekip oluşturmaktır. Bunlar Özel Amaçlı Ekipler, İş Sürekliliği Yönetim Ekibi ve İş Birimi Ekipleridir.

Dördüncü Adım-Planların Hazırlanması: İş kesintisine sebebiyet verecek herhangi bir olayın meydana gelmesi durumunda İş Sürekliliği Planları devreye alınır. Olayların büyüklüğü ve etkisine göre farklı planlar uygulanabilir. Banka içerisinde birden fazla iş sürekliliği planı hazırlanabileceği gibi tüm bankayı kapsayacak genel bir iş sürekliliği planı da hazırlanabilir. Önemli olan banka içerisinde birden fazla iş sürekliliği planı olması durumunda her bir planın diğer planlarla uyumlu olması, çatışma ve karmaşıklığa yol açmamasıdır.

İş Sürekliliği Planlarının temel iki amacı vardır. Bunlar;

•Finansal ve finansal olmayan kayıpların asgari düzeye indirilmesi

•İş etki analizleri sonucunda belirlenen iş kurtarma süreleri içerisinde ve iş öncelikleri doğrultusunda süreçlerin ayağa kaldırılmasıdır.

Beşinci Adım-Eğitim Ve Yetkinliklerin Yönetilmesi: İSYS kapsamında yer alan tüm personele, planlanan görevlerini tam, doğru ve zamanında yerine getirilmelerini sağlamak için

belli periyotlarda eğitim verilmesi gerekmektedir. İki ana grup olarak değerlendirilebilir. Birinci grupta genellikle İş Sürekliliği Yönetim yapısının sağlanmasında aktif görev alan kişiler yer alırken, ikinci grupta İş sürekliliği Yönetim Sisteminde aktif rol üstlenmeyen ancak bankada oluşabilecek olağanüstü bir durumdan etkilenecek diğer tüm personel yer almaktadır.

Altıncı Adım-Testlerin Yapılması: Banka içerisinde yapılacak iş sürekliliği tatbikatının (testlerin) amacı, kurumun hedeflenen sürelerde toparlanarak kritik bankacılık süreçlerinin, ürünlerinin, hizmetlerinin tekrar ayağa kaldırılabileceğini tetkik etmektir (Dinçkan, 2010).

Bankada uygulanacak iş sürekliliği yönetim kapsamının oldukça geniş olmasından dolayı, tek bir seferde iş sürekliliğinin test edilmesi oldukça zordur. Bundan dolayı testler genelde belirli bir program ve plan çerçevesinde birbirini destekleyen ve tamamlayan ancak nihai olarak tüm sistemin test edilmesini sağlayacak şekilde birden fazla tatbikatı içerebilir. Genelde sektörde kullanılan yapı belirlenen temel senaryolar bazında tatbikat, çalışma alanları bazında tatbikat, planlar ve prosedürler bazında tatbikat, bankacılık ürün ve hizmetleri bazında tatbikat, BT sistemleri bazında tatbikat ve son olarak iş birimleri bazında tatbikattır (Dinçkan, 2010).

- Belirlenen Senaryolar Bazında Tatbikat
- Çalışma Alanları Bazında Tatbikat
- Planlar ve Prosedürler Bazında Tatbikat
- Bankacılık Ürün ve Hizmetleri Bazında Tatbikat
- BT Sistemleri Bazında Tatbikat

o Tolere Edilebilir Maksimum Kesinti Süresi (MTPoD)

o Kurtarma Zamanı Hedefi (Response Time Objective/(RTO))

**Hedeflenen toparlanma süresi tolere edilebilir maksimum kesinti süresinden (MTPoD) kısa olmalıdır

o Tolere Edilebilir Maksimum Veri Kaybı Süresi (MTDL)

o Kurtarma Noktası Hedefi (RPO)

**Hedeflenen veri kurtarma süresi tolere edilebilir maksimum veri kaybı süresinden (MTDL) kısa olmak zorundadır.

- İş Birimleri Bazında Tatbikatı

Yedinci Adım-Sürekli İyileştirmenin Sağlanması: Banka içerisinde kurulan İSYS' nin etkin ve verimli bir şekilde uygulanması, sürdürülebilirliğinin sağlanması, kurum kültürü içerisine yerleştirilmesi için gerekli çalışmaların yapılması gerekmektedir. Sürekli iyileştirme yapısının sağlanabilmesi için etkin bir dokümantasyon sisteminin banka içinde kurulması, performans ve hedef yönetiminin belirlenmesi, bankanın belli periyotlarda İSYS bakımından denetlenmesi, banka süreçleri içerisine İSYS için düzeltici ve önleyici faaliyetlerin yerleştirilmesi ve üst yönetim tarafından desteklenerek sürekli güncellenmesi gerekmektedir (Dinçkan, 2008b).

3. SONUÇLARIN DEĞERLENDİRİLMESİ

Bu çalışmada, bankacılık sektöründe etkin bir "Bilgi Güvenliği Yönetim Sistemi" ve "İş Sürekliliği Yönetim Sistemi" yapısını kurmak için izlenecek adımlar ve durum gerçek sistem üzerinden önceki kısımlarda kurgulanarak ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı ve ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Standardı incelenmiştir. Çağımızın

popüler konusunu haline gelen bilgi güvenliği kavramı özellikle bankalar için hayati öneme sahip bir kavramdır ve teknolojinin gelişmesi ile de günden güne önemi daha fazla artmaktadır. Bankalar bilgi ve iletişim teknolojilerinin gelişmesiyle günümüzde artık tüm bankacılık faaliyetlerini bilişim sistemleri aracığıyla gerçekleştirmektedirler. Bankalara büyük kolaylık ve hız sağlayan bilişim teknolojisindeki gelişmeler aynı zamanda bilişim suçlarını da beraberinde getirmiştir. Bu sebeple etkin bir BGYSne sahip olmayan bir bankanın siber tehditlere maruz kalması ve bu saldırılardan etkilenmemesi olası değildir. Bankalar kurumsal hedeflerini gerçekleştirmek için çok sayıda bilgi varlığına gerek duyarlar. Bankaların elde ettikleri bilgilerin gizliliğinin uygun şekilde korunması, içeriğinin doğru olması ve gerek duyulduğu anda ulaşılması bankalarının yükümlülükleri, karlılığı, rekabetteki konumu ve imajı açısından son derece önemlidir. ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı bankalarda yer alan risklerin daha somut bir şekilde ölçülebilmesini ve değerlendirmesini sağlayarak bilgi güvenliği konusunda daha etkin önemlerin alınmasını sağlar. Sağlıklı bir şekilde standardı uygulayan bankalar hangi bilgi varlıklarının olduğunun ve değerinin farkına vararak, varlıklarını rakiplerine göre daha etkili korur ve kendilerine rekabet avantajı sağlarlar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardının uygulanması sonucu oluşacak faydalar aşağıdaki gibidir:

•Banka hangi bilgi varlıklarının olduğunu ve bunların değerinin farkına varır.

•Sahip olduğu varlıkları kuracağı kontroller ile etkin bir şekilde korur.

•Başta tedarikçileri olmak üzere, müşteriler bilgilerinin korunacağından emin olduklarından bankaya olan güven artar.

•Banka etkin bir BGYS sayesinde bilgiyi bir sistem sayesinde korur.

Banka, müşterileri tarafından rakiplerine göre daha iyi değerlendirilir.

• Çalışanların motivasyonunu arttırır.

•Yasal takipler önlenir.

•Yüksek prestij sağlar.

•Etkin bir BGYS sayesinde müşteri ve banka bilgilerinin korunması için fazladan iş yükü gerekmez ve zaman kaybının önüne geçilir.

•Bankanın karşı karşıya kalabileceği güvenlik riskleri minimize edilir.

•Etkin bir bilgi güvenliği yönetim sistemi yapısıyla iş sürekliliği de sağlanır.

•Banka çalışanlarının bilgi güvenliği konusunda farkındalıkları artar.

•Kurum müşterileri, kişisel bilgilerinin sağlıklı korunduğundan emin olur ve bankaya olsan güven duygusu artar.

•Banka bilgi güvenliği yönetimini etkin olarak gerçekleştirdiğinden, olası güvenlik ihlallerinin ve bu ihlaller sonucu bankanın maruz kalabileceği maddi kayıplarının önüne geçilmesini sağlanır.

•Bankanın uğrayabileceği tehdit ve riskler belirlenerek etkin bir risk yönetiminin kurulmasını sağlar.

•Bankanın oluşabilecek her türlü yeni riske karşı uyanık kalmasını sağlar.

•Banka, tüm bilgi sistemleri ve varlıklarının kapsamlı bir envanterine sahip olur.

•Banka ile çalışan müşterilerinin ve üçüncü parti kuruluşlarının bilgi güvenliği konusunda farkındalıklarının artmasını sağlar.

•Elde edilen ve sahip olunan tüm bilgi varlıklarının gizliliği, bütünlüğü ve erişebilirliği garanti altına alınır.

•Banka çalışanlarının, müşterilerinin ve üçüncü parti kuruluşların görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötüye kullanmaları engellenir.

•Etkin bir kimliklendirme ve loglama çalışmaları sayesinde yetkisiz erişimler engellenir ve tüm banka çalışanlarının yaptıkları işlemler kayıt altına alınır.

•ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Sistemi Standardının etkin şekilde uygulanması sonucu karşılaşılabilecek faydalar aşağıdaki gibidir:

•Herhangi bir uygulama kesintisinin etkileri proaktif olarak tespit edebilir ve erken müdahale edilebilir.

•İş Sürekliliği Yönetim Sisteminin uygulanması sürecinde yapılan tatbikatlar aracılığıyla bankanın güvenirliği kanıtlanır.

•Bankanın diğer rakiplerine karşı saygınlığı, marka değeri ve prestiji artar.

•Bankanın zor durum ve şartlarda iş sürekliliği sağlaması, bankacılık hizmetlerini vermeye devam etmesi sonucu rakiplerine karşı rekabet avantajı sağlanmış olur.

•Bankanın temel bankacılık hizmetlerini verememesinden dolayı uğrayabileceği yasal cezalar ve maddi kayıpların engellenmesini sağlar.

•Bankanın yasalara ve yönetmeliklere uygunluğu korunur ve objektif olarak uygunluğu kanıtlanır.

Günümüzde bilgi güvenliği kadar önemli bir diğer konu da iş sürekliliğidir. Bankalar gerçekleştirdikleri işlemlerin önemi sebebiyle, iş sürekliliğinin sağlanması gereken kurumlar arasında önde gelen kurumlardandır. Bankaların yaşayacağı iş kesintileri hem bankalara hem müşterilere hem de ülkemize büyük zararlara yol açmaktadır. Bilgi güvenliği yönetiminde de olduğu gibi etkin bir İş Sürekliliği Yönetim Sistemine sahip olmayan bankalar hem yasal (kanuni) hem de itibari olarak büyük zararlara uğramaktadır. Çalışma içerisinde ISO 22301 Toplumsal Güvenlik ve İş Sürekliliği Yönetim Standardının bankalarda uygulanması halinde bankaların yaşayabileceği herhangi bir sistem kesintisinin etkilerinden asgari düzeyde etkileneceği, bankaların temel bankacılık hizmetlerini verememesinden dolayı uğrayabileceği yasal cezalar ve maddi kayıpların engellenmesinin sağlanacağı ve kesintisiz hizmet sayesinde rakiplerine karşı rekabet avantajı sağlayacağı belirtilmiştir. Çalışma sonucunda bankaların "Bilgi Güvenliği Yönetim Sistemi" ve "İş Sürekliliği Yönetim Sistem"lerini kurarken geleceğe dair önerileri de barındıran ve dikkat etmesi gereken hususlar

•Bankalarda kurumsal bilgi güvenliğini sağlamanın dinamik bir süreç olduğu ve süreklilik arz ettiği,

•Bankalarda kurumsal bilgi güvenliğinin sadece teknolojiyle sağlanamayacağının unutulmaması gerektiği,

•Kurumsal bilgi güvenliğinin ancak ve ancak personel, eğitim ve teknoloji üçlüsü ile birlikte sağlanabileceği,

•Kurulan bilgi güvenliği sisteminin uluslararası standartlara uygun olarak yapılması ve uygulanması gerektiği,

•Kurulan bilgi güvenliği sisteminin belli periyotlarda iç ve dış denetime tabi tutularak etkinliğinin, uygunluğunun ve yeterliliğinin denetlenmesinin sağlanması gerektiği,

•Kurumsal bilgi güvenliğinin yönetilmesinin zorunlu bir süreç olduğu ve her zaman iyileştirmelere ihtiyaç duyulduğu,

•Bilgi güvenliği yönetiminde en zayıf halkanın insan olduğunun unutulmayarak kurum içinde verilen bilgi güvenliği eğitimlerinin öneminin farkına varılması gerektiği,

•İSYS için oluşturulan tüm dokümanlar sade ve anlaşılır bir dille yazılması gerektiği,

•İSYS' deki başarımın sağlanmasında en önemli etkenin yapılan tatbikatlar ve verilen eğitim olduğu,

•SYS için oluşturulan tüm dokümanların ve süreçlerin güncel olması gerektiği,

•İSYS' de aynı BGYS gibi dinamik ve yaşayan bir süreç olduğunun unutulmaması gerektiğidir.

Çalışmaya esas olan konuda bilgi güvenliği ve sürekliliği uzun bir süredir bilişim ayağında üzerinde durulan ve tartışılan bir konudur. Süreç genel olarak akla gelen siber saldırılar ve doğal afetler ağırlığında yürütülür iken bunlar haricinde halen yaşadığımız COVID19 gibi afet olaylarının da dikkate alınması adına dinamik yapı ve çevik felsefenin yer alması gerekmektedir. Pandemi sürecinde hayatın her alanında hızlı ve zorunlu dijital dönüşümün önemi en üst düzeye çıkmıştır. Bu dönüşüm anahtar kelimeler olan iş sürekliliği yönetim sistemi, bilgi güvenliği yönetim sistemi, bilgi güvenliği ve iş sürekliliği, süreç yönetimi ile birlikte değerlendirilmelidir.

KAYNAKÇA

Akpınar, H. (2009). Enformasyon Teknolojilerinde İş Sürekliliği Yönetimi ve Felaket Planlaması, Risk Yönetiminde Başarı Faktörü "İş Sürekliliği Yönetimi", 175-185, Marmara Üniversitesi İ.İ.B.F. 01 Mart 2016 tarihinde http://haldunakpinar.com/felaket_planlamasi.pdf adresinden erişildi.

Altay, O. (2016). Risklere Hazırlıklı Olmak için İş Sürekliliği Yönetimi. 01 Mayıs 2016 tarihinde http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/risklere-hazirlikli-olmak-icin-is-surekligi-yonetimi.html adresinden erişildi.

Aydemir, Z. (2013). İstanbul Metrosunda İş Sürekliliği, *Yüksek Lisans Tezi*, Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü.

BGA Security, (2013). ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi, Mart 2016 tarihinde https://www.bgasecurity.com/2013/10/iso-270012013-bilgi-guvenligi-yoneti/ adresinden erişildi.

Bingöl, C. (2010). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu, *Yüksek Lisans Tezi*, Sakarya Üniversitesi, Sosyal Bilimleri Enstitüsü.

Canbek, G., Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, *Politeknik Dergisi* Cilt: 9 Sayı: 3 s. 165-174.

Çalık, O. (2013). ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardındaki Değişiklikler ve Yenilikler, Aralık. 15 Mart 2016 tarihinde http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html adresinden erişildi.

Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması, *Akademik Bilişim 2008*, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak - 01 Şubat 2008.

Chouikha, M. Ben. (2016). Organizational Design for Knowledge Management. *ISTE and Wiley*, 173.

Dinçkan, A. (2008a). İş Sürekliliği Yönetim Sistemi Kurulumu, *Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü*, Sürüm 1.00, Ekim 2008a, ss. 5-21.

Dinçkan, A. (2008b) İş Sürekliliği Yönetimde Hatalı Yaklaşımlar, Ekim 2008b. 19 Mayıs 2016 tarihinde http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-yonetiminde-hatali-yaklasimlar.html adresinden erişildi.

Dinçkan, A. (2010). İş Sürekliliği Tatbikatları İçin Örnek Bir Model, Kasım 2010. 01 Mayıs 2016 tarihinde http://www.bilgiguvenligi.gov.tr/is-surekliligi/is-surekliligi-tatbikatlari-icin-ornek-bir-model.html adresinden erişildi.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management, *Journal of Information Security*, Vol.4, No.2, Article ID:30059.

Eren, C. (2013). İş Süreklilik Planlarının Test Edilmesi Örnek Vaka Çalışması, *İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi Dergisi*, No:49. ss.143-152.

Ersoy, E. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı- Tanımlar ve Örnek Uygulamalar, Türkiye: ODTÜ Yayıncılık- Şubat 2012.

Ganbat, O. (2013). Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması, *Yüksek Lisans Tezi*, Ege Üniversitesi, Fen Bilimleri Enstitüsü.

Gencer, K. (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım, *Yüksek Lisans Tezi*, Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü.

Haklı, T. (2012). Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi, *Yüksek Lisans Tezi*, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü.

Inform Danışmanlık ve Eğitim, (2016). Bilgi Güvenliği Yönetim Sistemi Nedir?, http://www.informdanismanlik.com/bilgi_guvenligi.html, Erişim Tarihi:01.03.2016.

ISO 22301 Standardı Komitesi, (2012). ISO 22301 Toplumsal Güvenlik-İş Sürekliliği Yönetim Sistemi-Gereksinimler-Birinci Versiyon, Mayıs, 2012. 01 Mayıs 2016 tarihinde https://www.pea.co.th/BCM/DocLib/ISO_22301_2012.pdf adresinden erişildi.

Karaağaç, T. (2013). Kriz Yönetimi ve İletişim, *İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi Dergisi*, No:49.,117-132.

Komut, M. (2013). İş Sürekliliği Organizasyonu, *İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi Dergisi*, No:49., 101-116.

Mittal, M., Goel, V. (2005). Business Continuity Information Management System, *United States, Patent Application Publication*, US20050144062 A1,30 June.

Önaçan, M. B. K. (2015). Organizasyonlar İçin Bilgi Yönetimi Çerçevesi ve Bilgi Yönetim Sistemi Mimarisi Önerisi: dOBLYN (Döküman ve Bilgi Yönetimi). *Ankara Üniversitesi*, s. 404.

Önel, Ö., Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu, *Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü*, Sürüm 1.00, Ağustos2007, ss. 2-15.

Özbilgin, İ. G., Özlü, M. (2010). Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi, *Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri* 10 - 12 Şubat 2010, Muğla Üniversitesi, ss. 221-228.

Özgen, B. (2013). İş Sürekliliğinde Strateji, *İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi Dergisi* No:49. ss.83-99.

Reynolds, W. J. (2004). Business Continuity Management, *GIAC Security Essentials Certification (GSEC)*,Version 1.4b, Option,February 20, SANS Institute.

Sağıroğlu, Ş., Ersoy, E., Alkan, M. (2007). Bilgi Güvenliğinin Kurumsal Bazda Uygulanması, *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, 13-14 Aralık, Ankara-2007.

Saymaz, Ö. (2012). *İş Sürekliliği Yönetim Sistemi*, Cinius Yayınları, s.42.

Susanto, H., Almunawar, M. N., Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of theBigFive, *International Journal of Electrical&ComputerSciences* IJECS-IJENS Vol: 11 No: 05, s.23-29.

Şahinaslan, E. Kandemir, R., Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitim Örneği, *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri* 11-13 Şubat 2009 Harran Üniversitesi.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi, *Kahramanmaraş Sütçü İmam Üniversitesi, Fen ve Mühendislik Dergisi*, 11(1), 2008.

TK01 Bilişim Teknolojileri Komitesi, (2013a). TS ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler, *Türk Standartları Enstitüsü*, Aralık.

TK01 Bilişim Teknolojileri Komitesi, (2013b). TS ISO/IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri- Bilgi Güvenliği Kontrolleri için Uygulama Prensipleri, *Türk Standartları Enstitüsü*, Aralık.

Vural, Y., Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", *Gazi Üniversitesi Müh. Mim. Fak. Der.* Cilt 23, No 2, 507-522.