T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ VE KALİTE YÖNETİM SİSTEMLERİ ARASINDAKİ İLİŞKİNİN İNCELENMESİ VE BİR UYGULAMA

YÜKSEK LİSANS TEZİ
Necati ALASULU

Anabilim Dalı: İstatistik
Programı: Olasılık Teorisi ve Olasılık Süreçleri
Danışman: Yrd. Doç. Dr. Nurhan HALİSDEMİR

ŞUBAT-2012

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ VE KALİTE YÖNETİM SİSTEMLERİ ARASINDAKİ İLİŞKİNİN İNCELENMESİ VE BİR UYGULAMA

YÜKSEK LİSANS TEZİ
Necati ALASULU
(091133102)

Tezin Enstitüye Verildiği Tarih: 15 Şubat 2012
Tezin Savunulduğu Tarih: 29 Şubat 2012

Tez Danışman : Yrd. Doç. Dr. Nurhan HALİSDEMİR (F.Ü)
Diğer Jüri Üyeleri : Doç. Dr. Cemil ÇOLAK (İ.Ü)
Doç. Dr. Sinan ÇALIK (İ.Ü)

ŞUBAT-2012

ÖNSÖZ

Tez konusunun belirlenmesi ve yürütülmesi aşamasında, her türlü yardımı ve desteği esirgemeyen kıymetli danışman hocam Yrd. Doç. Dr. Nurhan HALİSDEMİR' e, tezi oluşturmamda bana fikir kaynağı olan ve bilgilerinden yararlandığım değerli hocam Doç. Dr. Cemil ÇOLAK'a, bilgilerini benimle paylaşan değerli hocalarım, Doç. Dr. Sinan ÇALIK'a, Yrd. Doç. Dr. Mehmet GÜRCAN'a, ve Yrd. Doç. Dr. Mahmut IŞIK'a, uygulama aşamasında bizlere her türlü desteği veren firma yöneticilerine ve tezi hazırlama aşamasında bana destek olan değerli arkadaşlarım Ali ZOBİ'ye ve Mehmet Onur KAYA'ya teşekkür eder, saygılarımı sunarım.

Necati ALASULU

ELAZIĞ- 2012

İÇİNDEKİLER

Sayfa No

ÖNSÖZ. II
İÇİNDEKİLER III
ÖZET… VI
SUMMARY VII
ŞEKİLLER LİSTESİ VIII
TABLOLAR LİSTESİ IX
KISALTMALAR LİSTESİ X
1. GİRİŞ 1
1.1. Temel Kalite Kavramları 1
1.2. Kalite Yönetim Sistemi 1
1.2.1. Yönetim 1
1.2.2. Kalite Sistemi 2
1.2.3. Kalite Yönetim Sistemi 2
1.2.4. Kalite Yönetim Sistemi Standartları 3
1.2.5. Kalite Yönetim Sistemi Prensipleri 4
1.2.5.1. Müşteri Odaklılık 4
1.2.5.2. Liderlik 4
1.2.5.3. Çalışanların Katılımı 4
1.2.5.4. Proses Yaklaşımı 5
1.2.5.5. Yönetimde Sistem Yaklaşımı 6
1.2.5.6. Sürekli İyileştirme 6
1.2.5.7. Karar Vermede Gerçekçi Yaklaşım 7
1.2.5.8. Karşılıklı Yararlar Sağlayan Tedarikçi İlişkileri 7
1.3. Bilgi Güvenliği Yönetim Sistemi 7
1.3.1. Bilgi ve Varlık 7
1.3.2. Bilgi Yönetimi 8
1.3.3. Bilgi Güvenliği 9
1.3.3.1. Gizlilik 9
1.3.3.2. Bütünlük 10
1.3.3.3. Kullanılabilirlik 10
1.3.4. Bilgi Güvenliği Yönetim Sistemi 10

1.3.5. Bilgi Güvenliği Yönetim Sistemi Standartları 13
2. MATERYAL VE METOT 14
2.1. Uygulamada Kullanılan Standartlar 14
2.2. TS EN ISO 9001:2008 KYS ve TS ISO/IEC 27001:2005 BGYS Standartları İlişkisi 15
2.2.1. Genel Gereksinimler 17
2.2.2. Kapsam 17
2.2.3. Atıf Yapılan Standartlar ve/veya Dokümanlar ve Terimler ve Tarifler 17
2.2.4. Yönetim Sistemi Planlama ve Kurulum 18
2.2.5. Dokümantasyon Gereksinimleri 18
2.2.6. Yönetim Sorumluğu 19
2.2.7. Kaynak Yönetimi 19
2.2.8. İç Denetimleri(Tetkik) 20
2.2.9. Yönetimin Gözden Geçirmesi 21
2.2.10. Sürekli İyileştirme 21
2.2.11. Düzeltici Faaliyet 21
2.2.12. Önleyici Faaliyet 22
2.2.13. Kontrol Amaçları ve Kontroller 22
3. BULGULAR 23
3.1 Uygulama Yapılan İşletme Hakkında Genel Bilgiler 23
3.1.1. İşletmenin Kısa Tanımı 23
3.1.2. İşletmenin Vizyonu 23
3.1.3. İşletmenin Misyonu 23
3.1.4. İşletmesinin Organizasyon Şeması 24
3.2. Uygulama 24
3.2.1. Yönetim Sistemlerinin Tanımlanması ve Kurulum Süreci 24
3.2.1.1. Kapsam Belirleme 24
3.2.1.2. Prosesleri Tanımlama 25
3.2.2. Dokümantasyon Süreci 29
3.2.3. Yönetim Sorumluluğu Süreci 39
3.2.4. Kaynak Yönetim Süreci 40
3.2.5. Tetkik Süreci 42
3.2.6. Yönetimin Gözden Geçirmesi Süreci 44

3.2.7. İyileştirme Süreci 45
3.2.7.1. Düzeltici Faaliyet 47
3.2.7.1. Önleyici Faaliyet 49
4. SONUÇ VE TARTIŞMA 51
KAYNAKLAR 54
ÖZGEÇMİŞ 57

ÖZET

BİLGİ GÜVENLİĞİ VE KALİTE YÖNETİM SİSTEMLERİ ARASINDAKİ İLİŞKİNİN İNCELENMESİ VE BİR UYGULAMA

Bu çalışmada, Bilgi Güvenliği Yönetim Sistemi (BGYS) ile Kalite Yönetim Sistemleri (KYS) arasındaki ilişki incelenmiştir. Çalışmada ilk olarak temel kalite kavramları tanımlanmış ve KYS ile BGYS hakkında açıklamalar yapılmıştır. Daha sonra, Bilgi Güvenliği Yönetim Sistemi'nin standart maddeleri baz alınarak, KYS ile benzerlikleri incelenmiştir. BGYS ve KYS'nin çeşitli alanlarda uygulamaları için literatür araştırması yapılmıştır.

Uygulama aşamasında, bu çalışmada örnek olarak alınan işletmede KYS'nin kurulumu yapılmıştır. Bu sisteme ilave olarak sonradan Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve uygulaması incelenmiştir. BGYS ile KYS arasındaki ilişkiler ve benzerlikler ele alınmıştır. BGYS ile KYS'ye ilişkin veriler, Netsolutions firmasından temin edilmiştir. Sonuç olarak, BGYS'nin KYS ile entegre kurulması önerilmiş ve karşılaşılan problemlere çözüm getirilmiştir.

Şubat 2012, 70 Sayfa.

Anahtar Kelimeler: Kalite, Bilgi Güvenliği, Entegre Yönetim Sistemi.

SUMMARY

INVESTIGATION OF THE RELATIONSHIP BETWEEN INFORMATION SECURITY AND QUALITY MANAGEMENT SYSTEMS AND AN APPLICATION

In this study, the relationship between the Information Security Management System (ISMS) and the Quality Management Systems (QMS) was examined. Initially, the basic concepts of quality were described in this study, and explanations on QMS and ISMS were provided. Then, the similarities of ISMS and QMS were investigated on the basis of the standard substances of ISMS. The applications of ISMS and QMS in different fields were searched in literature.

In the application phase, QMS was established in the studied a company taken as an example. In addition to QMS, the establishment and implementation of ISMS were examined later. The similarities and the relationships between ISMS and QMS were taken into account. The data on ISMS and QMS was obtained from Netsolutions company. Eventuallly, an integrated management system that integrates ISMS and QMS was proposed and the problems encountered in the establishment of QMS and ISMS were remedied.

February-2012, 70 Pages.

Key Words: Quality, Information Security, Integrated Management System.

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 1.1 Proses Tabanlı Kalite Yönetim Sistemi Modeli **6**
Şekil 1.2 Bilgi Yönetim Sistemi **9**
Şekil 1.3 BGYS Proseslerine uygulanan PUKÖ Modeli **12**
Şekil 2.1 Bilgi Güvenliği Altyapısı Oluşturma Süreci **14**
Şekil 3.1 Kuruluş Oranizasyon Şeması **24**
Şekil 3.2 KYS ve BGYS Planlama Prosedürü **27**
Şekil 3.3 Doküman Kontrol Prosedürü **31**
Şekil 3.4 Doküman Ana Listesi **36**
Şekil 3.5 KYS ve BGYS Eğitim Prosesi Akış Şeması **47**
Şekil 3.6 İç Tetkik Prosedürü **43**
Şekil 3.7 Sürekli İyileştirme Prosesi Şeması **46**
Şekil 3.8 Düzeltici Faaliyet Prosedürü **48**
Şekil 3.9 Önleyici Faaliyet Prosedürü **50**

TABLOLAR LİSTESİ

Sayfa No

Tablo 1.1 ISO 9000 Serisi Standartlarının Yıllar İtibariyle Gelişimi **3**
Tablo 1.2 ISO 27000 Serisi Standartlarının Yıllar İtibariyle Gelişimi **13**
Tablo 2.1 TS ISO/IEC 27001 ve TS EN ISO 9001 Standartları Arasındaki İlişki **15**
Tablo 3.1 Ölçme Analiz ve İyileştirme Prosesi Tablosu **45**

KISALTMALAR LİSTESİ

BGYS : Bilgi Güvenliği Yönetim Sistemi

EN : Europeane Norm (Avrupa Standartları)

IEC : International Electrotechnical Commission

ISMS : Information Security Management System

ISO : International Standarts of Organisation (Uluslararası Standartlar Organizasyonu)

IT : Information Technology

KYS : Kalite Yönetim Sistemi

PUKO : Planla - Uygula - Kontrol et - Önlem al

TS : Türk Standardı

TSE : Türk Standartları Enstitüsü

1. GİRİŞ

1.1. Temel Kalite Kavramları

Günümüze kadar kalitenin çeşitli tanımları yapılmıştır. Kalite, yapısal karakteristikler kümesinin şartları yerine getirme derecesi olarak tanımlanmaktadır [1].

Bazı kalite tanımları şu şekilde yapılmıştır;

Kalite, mükemmeli arayışın sistematik bir yaklaşımıdır.

Kalite, kullanıma uygunluktur.

Kalite, şartlara uygunluktur

Kalite, bir urun veya hizmetin belirlenen veya doğabilecek gereksinimleri karşılama yeteneğine dayanan özellikleri toplamıdır.

Kalite, urun veya hizmeti ekonomik bir yoldan üreten ve tüketici isteklerine cevap veren bir üretim sistemidir.

Kalite, kontrolü uygulamak, en ekonomik, en kullanışlı ve tüketiciyi daima tatmin eden kaliteli ürünü geliştirmek, tasarımını yapmak, üretmek ve satış sonrası hizmetlerini vermektir [2].

Kalite, ihtiyaçların zorladığı ve ihtiyacların anlam ve önemine göre değişen bir gerekliliktir. Kalite canlı bir süreçtir ve insanlıkla beraber gelişerek devam edecek ve var olacaktır [3].

En genel anlamı ile kalite, şartların yerine getirilmesidir.

Kalite, kar için çalışsın veya çalışmasın bir kurulusun çalışmalarının her yönüne nüfuz eden sürekli bir işlev, bir urunun (mal veya hizmetin) kullanıcının (müşterinin) beklentisini karşılamadaki uygunluğu ve müşteri tatminidir [2].

Kısaca özetlersek kalite; müşteri ihtiyaç ve beklentilerinin zamanında ve istenilen ölçüde karşılanmasıdır.

1.2. Kalite Yönetim Sistemi

1.2.1. Yönetim

Yönetimle ilgili çok çeşitli tanımlar yapılmıştır bu tanımlardan bazıları şöyledir; Yönetim, amaçların etkili bir şekilde gerçekleştirilmesi için çalışan arasında işbirliğini ve

koordinasyonu sağlamaya yönelik çalışmaları ifade eder. Bir diğer tanım da yönetim, insanların ortak amaçlar olarak belirlediği hedeflere en kısa zamanda ve istenilen biçimde ulaşmaları için topluca hareket etmeleridir [2].

Yönetim, belirli bir takım amaçlara ulaşmak için başta insanlar olmak üzere kaynakları, zamanı birbiriyle uyumlu, verimli ve etkin kullanabilecek kararlar alma ve uygulatma süreçlerinin toplamı olarak tanımlanabilir [2].

Yönetim sistemi; kuruluşun proseslerini ve faaliyetlerini yönetmek için neler yapacağını ve nasıl yöneteceğini amaçlamaktadır[4].

1.2.2. Kalite Sistemi

Kalite sistemi, bir kuruluşun kalite bakımından sevk ve idaresi için koordine edilmiş faaliyetleridir. Kalite bakımından sevk ve idare, genellikle Kalite politikasının oluşturulması ve kalite hedefleri, kalite planlaması, kalite kontrol, kalite güvence ve kalite iyileştirmesini içerir [1].

1.2.3. Kalite Yönetim Sistemi

Kalite Yönetim Sistemi, bir kuruluşu kalite açısından yönlendiren ve kontrol eden yönetim sistemidir [1].

Kalite Yönetim Sistemi standartları olan ISO 9000 serisi standartlar kuruluşun faaliyetlerini kontrol altında tutarak müşterinin şartlarını karşılayan ürün üretmeyi amaçlamaktadır[4].

Kuruluş tarafından Kalite Yönetim Sistemi'nin benimsenmesi, kuruluşun stratejik bir kararı olmalıdır. Kuruluşun Kalite Yönetim Sistemi'nin tasarımı ve uygulanmasına aşağıdakiler etki eder:

Kuruluşun organizasyonel ortamı, bu ortamdaki değişiklikler ve bu ortamın beraberinde gelen riskler;

Kuruluşun değişen ihtiyaçları,

Kuruluşa özel amaçlar,

Kuruluşun sağladığı ürünler,

Kuruluşun prosesleri,

Kuruluşun büyüklüğü ve organizasyon yapısı etki etmektedir [5].

TS EN ISO 9001:2008 standardı ile Kalite Yönetim Sistemlerinin yapısında tek tiplilik veya dokümantasyonun tek tipliliği amaçlanmamaktadır. Belirtilen Kalite Yönetim Sistemi şartları, ürün şartlarını tamamlayıcıdır. Bu standardı, belgelendirme kuruluşları dâhil iç ve dış taraflarca kuruluşun; müşteri şartları, ürüne uygulanabilir birincil ve ikincil mevzuat şartları ve kendi şartlarını karşılamadaki yeterliliğini değerlendirmek için kullanılabilir [5].

1.2.4. Kalite Yönetim Sistemi Standartları

Kalite Yönetim Sistemi standartları ilk oluşturulmasından günümüze çeşitli revizyonlar geçirmiştir. Bunlar Tablo 2.1'de verilmiştir.

Çalışmadaki bu standartların uygulamada olanlarının güncel revizyonları göz önüne alınarak hazırlanmıştır.

Tablo: 2.1 ISO 9000 Serisi Standartlarının Yıllar İtibariyle Gelişimi

Yıllar	**Standartların Gelişimi**	**Açıklama**
1963	MIL/Q/9858	ABD'de savunma teknolojisinde
1968	AQAP Standartları	NATO üyesi ülkelerde
1979	BS 5750	British Standards
1987	ISO 9000 serisi	ISO tarafından
1988	EN 29000 standartları	CEN tarafından
1988	TS 6000 KGS standardı	(KGS) Kalite Güvence Sistem
1991	TS EN ISO 9000	TSE tarafından yayımlandı
1994	TS EN ISO 9001:1994 / TS EN ISO 9002:1994 / TS EN ISO 9003:1994	ISO tarafından revize edildi
1996	EN 29000 serisi	ISO Tarafından EN ISO 9000 olarak yayınlandı
2000	TS EN ISO 9001:2000	ISO Tarafından 1994 Versiyonu Revize Edildi
2007	TS EN ISO 9000:2007	ISO Tarafından 2000 Versiyonu Revize Edildi
2008	TS EN ISO 9001:2008 olarak yayınlandı	ISO Tarafından 2008 Versiyonu Revize Edildi

Güncel olarak Kalite Yönetim Sistemi standardı TS EN ISO 9001:2008 revizyonu kullanılmaktadır.

1.2.5. Kalite Yönetim Sistemi Prensipleri

Kalite Yönetim Sistemi prensipler üzerine kurulmuştur. Bu prensipler kuruluşu başarılı bir şekilde çalıştırmak için, kuruluşu sistematik ve şeffaf bir şekilde yönetmek ve kontrol etmek gereklidir. Başarı, bütün ilgili tarafların ihtiyaçları karşılanırken, performansı sürekli iyileştirilecek şekilde tasarlanan bir Yönetim Sistemi'nin uygulanması ve sürdürülmesinin sonucunda elde edilir. Bir kuruluşun yönetilmesi, diğer yönetim sistemleri yanında Kalite Yönetim Sistemi'ni de içerir.

Kuruluşu performans iyileştirmeye yöneltmek amacıyla üst yönetim tarafından kullanılabilecek olan kalite prensibi aşağıdaki gibi tanımlanmıştır [1].

1.2.5.1. Müşteri Odaklılık

Kuruluşlar müşterilerine bağlıdır. Bu nedenle kuruluşlar, mevcut ve gelecekteki müşteri ihtiyaçlarını anlamalı, müşteri şartlarını karşılamalı ve müşteri isteklerini aşmaya istekli olmalıdır.

1.2.5.2. Liderlik

Liderler kuruluşta amaç ve yönetim birliğini oluşturur. Liderler, kuruluşun hedeflerine ulaşılması için çalışanların tam katılımının sağlandığı kuruluş içi ortam oluşturmalı ve sürdürmelidirler.

Liderler, görev ve yetkileri çalışanlara açık bir biçimde bildirirler, yol gösterirler ve denetim faaliyetlerini gerçekleştirirler [2].

1.2.5.3. Çalışanların Katılımı

Her seviyedeki çalışanlar kuruluşun temelini oluşturur. Onların tam katılımı, yeteneklerinin kuruluş yararına kullanılmasını sağlar.

1.2.5.4. Proses Yaklaşımı

Girdileri çıktılara dönüştürmek üzere kaynakları kullanan her faaliyet veya faaliyetler dizisi bir proses olarak kabul edilebilir.

Kuruluşlar etkin çalışabilmeleri için birbirleri ile ilgili olan ve etkileşimde bulunan çok sayıda prosesini tanımlamalı ve yönetmelidir.

ISO 9001, Kalite Yönetim Sistemi proseslerin tanımlanması, sıralaması ve etkileşimlerinin belirlenmesini zorunlu kılmıştır. Yani proseslerin birbirinden ayrı birer faaliyet olarak ele alınmasını istemiyor [6]. Çoğunlukla bir prosesin çıktısı, bir sonraki prosesin girdisini oluşturur. Bir kuruluşta kullanılan proseslerin ve özellikle bu prosesler arasındaki etkileşimlerin sistematik bir şekilde tanımlanması ve yönetilmesine "proses yaklaşımı" adı verilir [1].

Bu standardın amacı, bir kuruluşun yönetilmesinde proses yaklaşımının benimsenmesini teşvik etmektir (Şekil 1.1). ISO 9000 serisi standartlarda açıklanan proses tabanlı Kalite Yönetim Sistemi'ni göstermektedir. Şekil1.1'de kuruluşun girdilerinin temininde ilgili tarafların önemli bir rol oynadığını göstermektedir. İlgili tarafların memnuniyetinin izlenmesi, ilgili tarafların ihtiyaç ve beklentilerinin ne derecede karşılandığına dair algılamalarıyla ilgili bilginin değerlendirilmesini gerektirir [1, 5].

Proseslerin tanımlanması ve yönetilebilmesinde Deming, PUKO çevrimi olarak da adlandırılan sistemi yönetim biliminin hizmetine sunmuştur [1, 5].

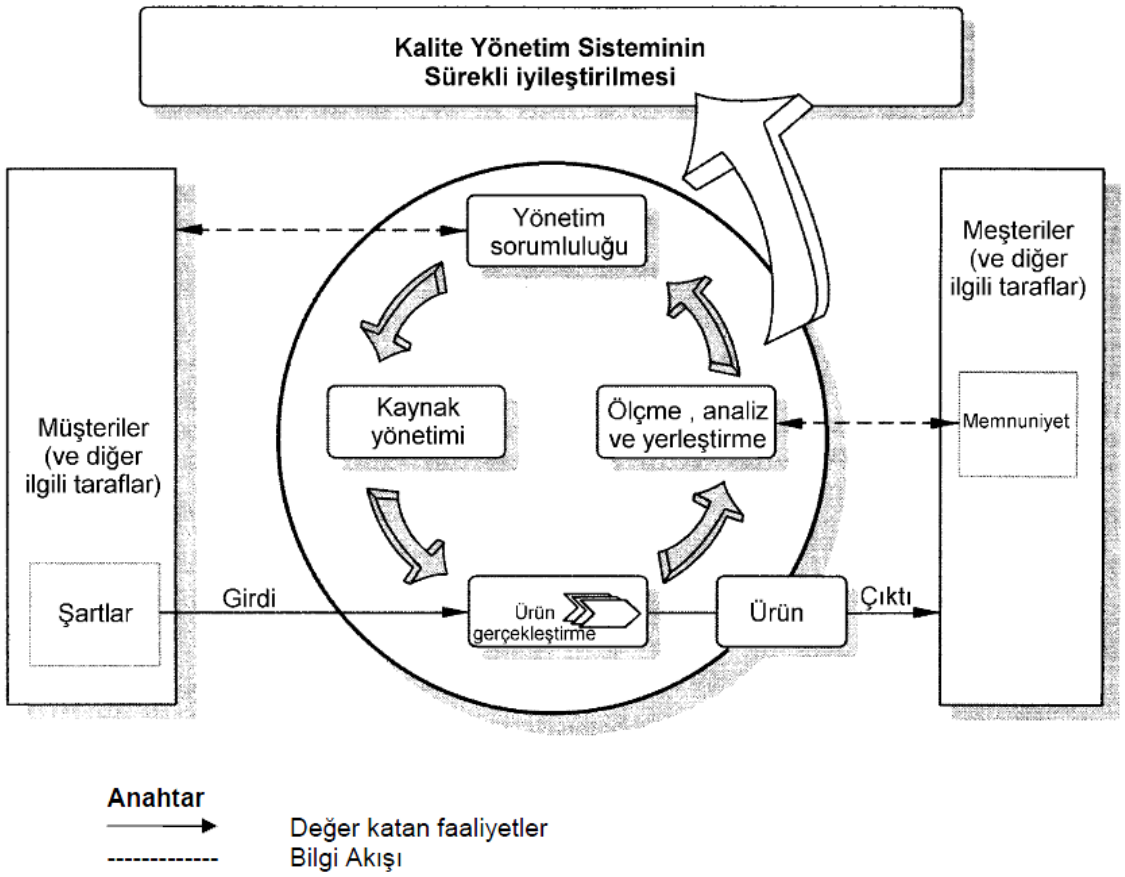
"Plânla - Uygula - Kontrol et - Önlem al" olarak bilinen (PUKO) metodolojisi, bütün proseslere uygulanabilir. PUKO kısaca şöyle açıklanabilir;

Plânla : Müşteri şartlarına ve kuruluşun politikasına uygun sonuçların ortaya çıkması için gerekli hedefleri ve prosesleri oluştur,

Uygula : Prosesleri uygula,

Kontrol et : Prosesleri ve ürünü; politikalara, hedeflere ve ürün şartlarına göre izle, ölç ve sonuçları rapor et,

Önlem al : Proses performansını sürekli iyileştirmek için tedbirler al.



Şekil 1.1 Proses Tabanlı Kalite Sistemi Modeli [1, 5].

1.2.5.5. Yönetimde Sistem Yaklaşımı

Birbirleri ile ilgili proseslerin bir sistem olarak tanımlanması, anlaşılması ve yönetilmesi, hedeflerin gerçekleştirilmesinde kuruluşun etkinliğine ve verimliliğine katkıda bulunur [1].

Sistem yaklaşımının temelinde verimlilik, kavramı bulunmaktadır. Verimlilik; doğru olan işleri, doğru bir biçimde ve ekonomik bir çalışmayla gerçekleştirmeyi hedefleyen akılcı bir yaşam biçimi olarak tanımlanabilir [2].

1.2.5.6. Sürekli İyileştirme

Kuruluşun toplam performansının sürekli iyileştirilmesi kuruluşun sürekli hedefi olmalıdır. Sürekli iyileştirme kalite sisteminin bir parçası değil onu yönetme şekli olarak ele alınmıştır [6].

1.2.5.7. Karar Vermede Gerçekçi Yaklaşım

Etkin kararlar verilerin ve bilginin analizine dayanır. Kararlar tecrübe ve sezgisel olarak alınmaz. Böylece alınan kararlara ilişkin inceleme ve geriye dönük analizlerin yapılmasına olanak tanır.

1.2.5.8. Karşılıklı Yararlar Sağlayan Tedarikçi İlişkileri

Kuruluş ve tedarikçileri birbirlerine bağımlıdır. Karşılıklı yararların gözetildiği bir ilişki her iki tarafın da değer yaratma yeteneğini artırır.

Tedarikçiden gelen malzemeler müşteriye sunulan ürünlerin en önemli parçalarını oluşturmaktadır. Kuruluş ile tedarikçisi arasındaki ilişkilerin artırılması ve geliştirilmesi; müşterinin kalite ve güvenilirlik acısından yararına olduğu söylenebilir. Üretim surecinde, oluşturulan müşteri ile tedarikçi arasındaki ilişkisi sayesinde son mamulde arzulanan kalitenin çıkma olasılığı yükselmektedir [2].

Bu sekiz Kalite Yönetim Sistemi ilkesi ISO 9000 standart serisi içindeki kalite yönetimi standartlarının temelini oluşturur [1, 5].

1.3. Bilgi Güvenliği Yönetim Sistemi

1.3.1. Bilgi ve Varlık

Bilgi, kurumdaki diğer varlıklar gibi, kuruluşlar için önem taşıyan ve bu nedenle de en korunması gereken bir varlıktır [7]. Bilgi günümüzde en basit manada, bir kavramın ne olduğunu, fiziksel olarak nasıl hareket ettiğini, ne işe yaradığını, varlığını nasıl koruduğu çok çeşitli anlamlar içeren karmaşık bir kavramdır. Bir bilginin değerli olması için odaklanmış, test edilmiş, geçerli kılınmış ve paylaşılmış olması gerekmektedir [8].

Kuruluşların ömrü boyunca ihtiyaç duyduğu ve yaşamını şekillendiren en önemli unsur bilgidir. Doğru, gerçek, zamanında istenilen bilgiye sahip olmayan yönetimlerin isabetli karar veremeyeceği bilinen bir gerçektir. Buda kurumsal faaliyetlerin karar verme aşamasında yaşanılan problemlerin çözümü, en doğru kararı verebilme kabiliyeti yönetimin sahip olduğu bilgi ile olacaktır [8].

Varlık, kuruluş için değeri olan herhangi bir şey olarak tanımlamaktadır [9, 10].

Yine varlık, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır. İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Kurum çalışanlarının zihinlerinde, konuşmalarında bulunur. Varlıklara çeşitli örnekler verilebilir. Bu örnekler kuruluşun yapısına, büyüklüğüne, proseslerinin karmaşıklığına ve personelinin yetkinliğine göre değişmektedir. Aşağıda birkaç tane örnek verilmiştir [11].

a) Bilgi varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir;

b) Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları;

c) Fiziksel varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni;

d) Servisler (Hizmetler): Bilgi işleme ve haberleşme servisleri (web servisi, e-ticaret servisi, ftp servisi), genel faydalar; örneğin ısınma, ışıklandırma, elektrik, havalandırma.

e) İnsan: Kurum çalışanları da kurum varlığı olarak düşünülmelidir

Yukarıdaki varlıklara ilave yapılabilir [11].

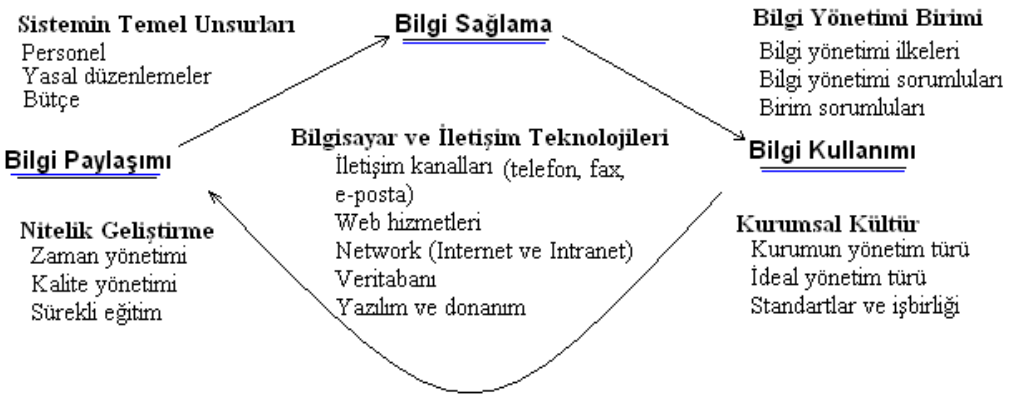
1.3.2. Bilgi Yönetimi

21. Yüzyıl, bilginin organizasyonlar için öneminin giderek arttığı bir asır olma özelliği taşır. Kuruluşlar, etkinliklerinde bilgiyi, stratejik bir kaynak olarak kullanmaktadır. Bilginin kullanımının yaygınlaşması ve bir değer yaratma aracı olarak bilginin öneminin artması, bilgi yönetimini önemli kılmaktadır. Bilgi yönetimi; bilgisayar ortamında verilerin korunması, bilgi mühendisliği, dijital ağlarla ilgili ve organizasyondaki bir yatırım değildir [8].

Bilgi varlıklarının yönetilebilmesi, kurumların karşılaşabileceği risklerin en aza indirmesi ve iş sürekliliğinin sağlanması ancak üst yönetim desteğiyle mümkün olmaktadır. Üst yönetim kilit rol oynamaktadır [12].

Bilgi yönetimi için çeşitli tanımlamalar yapılmış olup kısaca; bilginin gizlilik bütünlük, kullanılabilirliğinin sağlanmasıdır.

Günümüzde bilgi yönetimi, net olarak tanımlanmış bilgi yönetimi stratejisi ve hedefleri doğrultusunda; insanların/ çalışanların bilgi, yetenek ve yaratıcılıklarını ortaya koyulmasıdır. Bilginin ilgili personele dengeli ve zamanında iletilmesini sağlayan, aynı zamanda personel, bütçe, bilgisayar ve iletişim teknolojileri gibi çok farklı unsurları barındıran bir sistemi de ifade etmektedir. Bilgi yönetimi sistemi Şekil 1.2,'de bilgi yönetimi disiplininin tasarımı, kurulması, uygulanması ve yenilenmesi sırasında personel, bütçe, yasal düzenlemeler, bilgisayar ve iletişim teknolojilerini oluşturan iletişim kanalları, web sayfaları, ağlar, veri tabanları, zaman, kalite, bilgi güvenliği ve sürekli eğitim gibi çok çeşitli unsurların bir arada ve uyum içerisinde kullanıldığı sistemi ifade etmektedir [8].



Şekil 1.2 Bilgi Yönetim Sistemi [8]

1.3.3. Bilgi Güvenliği

Bilgi Güvenliği, bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özelliklerini de kapsar [13, 14].

1.3.3.1. Gizlilik

Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği [9, 10].

Gizlilik, bilgiye, varlığa sadece yetkili insan ve organizasyonların ulaşılabilmesidir. Bugün şifreleme altyapılarının olmasının sebebi temel olarak gizlilik ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için önemlidir [8].

1.3.3.2. Bütünlük

Varlıkların doğruluğunu ve tamlığını koruma özelliği olarak bilinmektedir[9, 10]. Bütünlük özetle verinin yahut bilginin yetkisiz kişilerce değiştirilmesine, tahrip edilmesine veya yok edilmesine karşı korunmasıdır[8].

Bilgi varlığının bozulması kasten yahut kaza ile olabilir bu durum bütünlük özelliğinin bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü; kesinlik, doğruluk ve geçerlilik kıstaslarını sağlaması gerekmektedir [8].

1.3.3.3. Kullanılabilirlik

Varlığın kullanılabilirlik özelliği birçok kaynakta "Erişilebilirlik" olarak geçmekte ise de TS ISO/IEC 27001:2005 Standardında "Kullanılabilirlik" olarak ifade edildiğinden tezde kullanılabilirlik olarak tanımlayacağız.

Kullanılabilirlik, bilginin yani varlığın yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir[9, 10].

Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Başka bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır [11].

1.3.4. Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı bir yönetim sistemidir [13].

Bilgi Güvenliği Yönetim Sistemi kurumun iç verimliğinin artmasında da önemli paya sahiptir [15]. Bu sebeple BGYS, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içermelidir.

Bilgi Güvenliği Yönetim Sistemi'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek isteyen kuruluşlar TS ISO/IEC 27001:2005 Standardı gereklerini yerine getirmelidirler. Bu standartta ISO tarafından hazırlanmış ve TSE tarafından Türkçe 'ye tercümesi yapılarak Türk Standardı olarak kabul edilmiştir [13].

Bilgi Güvenliği Yönetim Sistemi'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. BGYS'nin benimsenmesi kuruluşun stratejik bir kararı olmalıdır. BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısına birebirinden farklılıklar gösterecektir [13].

TS ISO/IEC 27001:2005 Standardı, kuruşun kurmuş olduğu BGYS'nin akredite belgelendirme kuruluşları tarafından uygunluk değerlendirmesine esas teşkil eder. Kuruluş Bilgi Güvenliği Yönetim Sistemi'nin etkin şekilde işlev görmesi sağlamak için, birçok faaliyetini tanımlaması ve yönetmesi gerekir [13].

Bu standarda diğer tüm ISO standartları gibi "Proses Yaklaşımını" benimsemiştir. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünülebilir. Çoğunlukla, bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur. Kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir. Bu standarda sunulan bilgi güvenliği yönetimi proses yaklaşımı, kullanıcılarını aşağıdakilerin öneminin vurgulanmasına özendirir [13, 16, 17];

- İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,
- Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
- Nesnel ölçmeye dayalı olarak sürekli iyileştirmek.

Bu standart, tüm BGYS proseslerini yapılandırmaya uygulanan "Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modelini benimser [1, 13].

BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir (Şekil 1.3), Ayrıca, standart maddelerine atıfta bulunur [13].

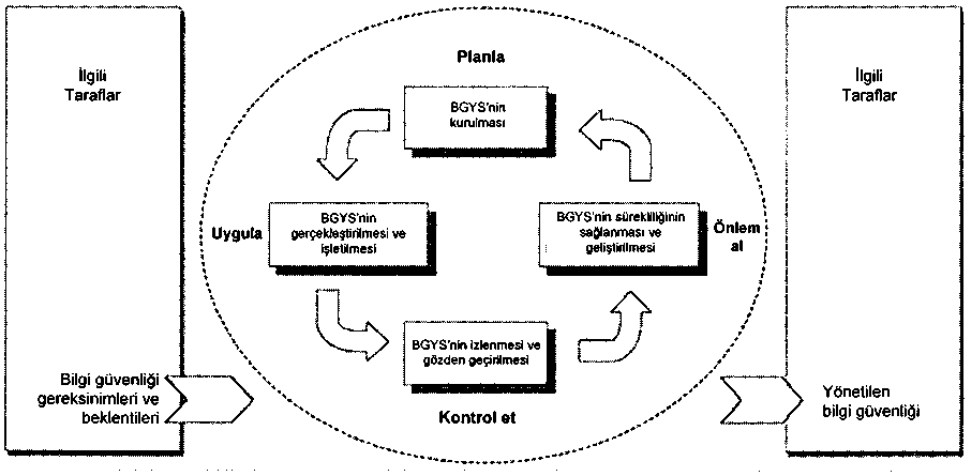
Bilgi Güvenliği Yönetim Sistemi proses tabanlı bir sistemdir. "Plânla - Uygula - Kontrol et - Önlem al" olarak bilinen (PUKO) metodolojisi, bütün proseslere uygulanabilir. PUKO kısaca şöyle açıklanabilir [13];

Planla (BGYS'nin kurulması): Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin

Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi): BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.

Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi) : BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.

Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi) : BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi.



Şekil 1.3 BGYS Proseslerine Uygulanan PUKO Modeli [13].

1.3.5. Bilgi Güvenliği Yönetim Sistemi Standartları

Bilgi Güvenliği Yönetim Sistemi standartları ilk oluşturulmasından günümüze çeşitli revizyonlar geçirmiştir. Bunlar Tablo 2.2'de verilmiştir [18].

Çalışmadaki bu standartların uygulamada olanlarının güncel revizyonları göz önüne alınarak hazırlanmıştır.

Tablo: 2.2 ISO 27000 Serisi Standartlarının Yıllar İtibariyle Gelişimi [18, 19].

Yıllar	**Standartların Gelişimi**	**Açıklama**
1999	BS 7799-1	British Standards Institute
1999	BS 7799-2	British Standards Institute
2000	ISO/IEC 17799:2000	ISO tarafından yayınlandı.
2005	ISO/IEC 17799:2005	BS 7799-1 ISO tarafından code of practice for infomation security management olarak yayınlanmıştır
2005	ISO/IEC 27001:2005	ISO tarafından BGYS belgelendirme standardı olarak yayınlanmıştır.
2005	ISO TR 13569:2005	Finansal Hizmet- Bilgi Güvenliği Kılavuzu
2007	ISO/IEC 27002:2005	ISO/IEC 17799:2005 standardı ISO standart numarası değiştirildi BGYS Uygulama Prensipleri olarak kullanılmaya başlandı. ISO/IEC 27001:2005' Ek A daki kontrolleridir.
2008	ISO/IEC 27005:2008	Bilgi Güvenliği Risk Yönetimi
2008	ISO/IEC 27011:2008	Telekomünikasyon kuruluşları için ISO/IEC 27002 bazlı bilgi güvenliği kılavuzu
2008	ISO/IEC 27799:2008	Tıbbi Bilişim ISO/IEC 27002' yi kullanarak Bilgi Güvenliği Yönetim Sistemi
2009	ISO/IEC 27000:2009	Genel Bakış ve Sözlük
2009	ISO/IEC 27004:2009	Bilgi Güvenliği Yönetim Ölçümü
2010	ISO/IEC 27003:2010	Bilgi Güvenliği Yönetim Sistemi uygulama kılavuzu
2011	ISO/IEC 27007:2011	Tetkik için kılavuz

Güncel olarak Bilgi Güvenliği Yönetim Sistemi standardı ISO/IEC 27001:2005 revizyonu kullanılmaktadır.

2. MATERYAL VE METOT

2.1. Uygulamada Kullanılan Standartlar

TS EN ISO 9001:2008 Standardı, bir kuruluşun kendi Kalite Yönetim Sistemi'ni; ilgili diğer yönetim sistem şartları ile bir araya getirmesini veya bütünleştirmesini sağlar. Bir kuruluşun, bu Standard‟ ın şartlarına uygun bir Kalite Yönetim Sistemi oluşturmak amacıyla, kendisinde mevcut yönetim sistemlerini uyarlaması mümkündür [5].

TS ISO /IEC 27001:2005 Standardı, ilgili yönetim standartlarıyla tutarlı ve tümleşik gerçekleştirme ve işletimi desteklemek için TS EN ISO 9001:2008 ile uyumludur. Bu nedenle, uygun şekilde tasarlanmış bir yönetim sistemi tüm bu standartların gereksinimlerini karşılayabilir ve kuruluşun BGYS'ni ilgili yönetim sistemi gereksinimleriyle uyumlu yapabilmesi yada bütünleştirebilmesine imkan sağlar [13].

Bilgi Güvenliği Yönetim Sistemi uzmanlar tarafından bilinçlendirme çalışmasıyla başlar. Yapılması gereken ilk adım; konuyla ilgili bir bilgi güvenliği ve risk yönetim ekibi, bilgi güvenliği ve risk yönetim lideri belirleyerek bu tür bir koordinasyonu sağlayabilecek ortam oturuşturulmalıdır. Genel olarak bilginin yönetilmesi ve güvenlik konusunda gidişata bakıldığımızda; ISO 9001(Kalite Yönetim Sistemi), ISO 27001 (Bilgi Güvenliği Yönetim Sistemi) ve ISO/IEC 20000 (ITIL- Bilgi Teknolojileri Hizmet Yönetimi Sistemi) gibi standartlar global düzeyde uygulanmaktadır [20]. Şekil 2.1 de Bilgi güvenliği yönetim sistemlerinin kurulum ve iyileştirme yapısı verilmiştir.

Şekil 2.1 Güvenliği Altyapısı Oluşturma Süreci [20].

Bu çalışmada Kalite Yönetim Sistemi için TS EN ISO 9001:2008 Standart maddeleri, Bilgi Güvenliği Yönetim Sistemi için de TS ISO /IEC 27001:2005 Standardı maddeleri temel alınarak açıklanmaya çalışılacaktır.

Çalışmadaki tüm dokümanlar bu standartların güncel revizyonları göz önüne alınarak hazırlanmıştır.

Uluslararası standartların hazırlanması, ISO teknik komitelerince, alt komiteler oluşturularak; üye kuruluşların, standartların kullanıcılarının ve diğer ilgili kişi ve kuruluşların görüşleri alınarak gerçekleştirilmektedir. Standartların teknoloji ve piyasa gelişmeleri ışığında, kullanıcı ihtiyaçları doğrultusunda periyodik olarak ISO tarafından revize edilirler [17].

2.2. TS EN ISO 9001:2008 KYS ve TS ISO/IEC 27001:2005 BGYS Standartları İlişkisi

Bilgi Güvenliği Yönetim Sistemi Standardı ile Kalite Yönetim Sistemi Standardı arasında ilişki Tablo 2.1.'de verilmiştir [13].

Tablo 2.1 TS ISO/IEC 27001:2005 ve TS EN ISO 9001:2008 Standartları Arasındaki İlişki

TS ISO/IEC 27001:2005	**TS EN ISO 9001:2008**
0 Giriş 0.1 Genel 0.2 Proses yaklaşımı 0.3 Diğer yönetim sistemleriyle uyumluluk	0 Giriş 0.1 Genel 0.2 Proses yaklaşımı 0.3 ISO 9004 ile ilişkiler 0.4 Diğer yönetim sistemleriyle uyumluluk
1 Kapsam 1.1 Genel 1.2 Uygulama	1 Kapsam 1.1 Genel 1.2 Uygulama
2 Atıf yapılan standardlar ve/veya dokümanlar	2 Atıf yapılan standard ve/veya dokümanlar
3 Terimler ve tarifler	3 Terimler ve tarifler
4 Bilgi Güvenliği Yönetim Sistemi 4.1 Genel gereksinimler 4.2 BGYS'nin kurulması ve yönetilmesi 4.2.1 BGYS'nin kurulması 4.2.2 BGYS'nin gerçekleştirilmesi ve işletilmesi 4.2.3 BGYS'nin izlenmesi ve gözden geçirilmesi	4 Kalite ve Bilgi Güvenliği sistemi 4.1 Genel şartlar 8.2.3 Proseslerin izlenmesi ve ölçülmesi 8.2.4 Ürünün izlenmesi ve ölçülmesi

4.3 Dokümantasyon gereksinimleri 4.3.1 Genel 4.3.2 Dokümanların kontrolü 4.3.3 Kayıtların kontrolü	4.2 Dokümantasyon şartları 4.2.1 Genel 4.2.2 Kalite el kitabı 4.2.3 Dokümanların kontrolü 4.2.4 Kayıtların kontrolü
5 Yönetim sorumluluğu 5.1 Yönetimin bağlılığı	5 Yönetim sorumluluğu 5.1 Yönetimin taahhüdü 5.2 Müşteri odaklılık 5.3 Kalite ve Bilgi Güvenliği Politikası 5.4 Planlama 5.5 Sorumluluk, yetki ve iletişim
5.2 Kaynak yönetimi 5.2.1 Kaynakların sağlanması 5.2.2 Eğitim, farkında olma ve yeterlilik	6 Kaynak yönetimi 6.1 Kaynakların sağlanması 6.2 İnsan kaynakları 6.2.2 Yeterlilik, farkında olma (bilinç) ve eğitim 6.3 Alt yapı 6.4 Çalışma ortamı
6 BGYS iç denetimleri	8.2.2 İç tetkik
7 BGYS'yi yönetimin gözden geçirmesi 7.1 Genel 7.2 Gözden geçirme girdisi 7.3 Gözden geçirme çıktısı	5.6 Yönetimin gözden geçirmesi 5.6.1 Genel 5.6.2 Gözden geçirme girdisi 5.6.3 Gözden geçirme çıktısı
8 BGYS iyileştirme 8.1 Sürekli iyileştirme 8.2 Düzeltici faaliyet 8.3 Önleyici faaliyet	8.5 İyileştirme 8.5.1 Sürekli iyileştirme 8.5.2 Düzeltici faaliyet 8.5.3 Önleyici faaliyetler
Ek A Kontrol amaçları ve kontroller Ek B OECD prensipleri ve bu standard Ek C TS EN ISO 9001:2008, TS EN ISO 14001 ve bu standard arasındaki benzerlikler	Ek A TS EN ISO 9001:2008:2000 ve ISO 14001:1996 arasındaki eşleme

Bilgi Güvenliği Yönetim Sistemi ve Kalite Yönetim Sistemi arasında standart maddeleri baz alınarak aşağıdaki gibi açıklanacaktır.

Tablo 2.1 incelendiğinde TS EN ISO 9001:2008 ve TS ISO/IEC 27001:2005 standartları arasında ilişki ve maddelerinin birbirlerine karşılık gelenleri görülebilmektedir. Bununla birlikte madde karşılık olmasa da aralarında işlev bakımında bir benzerlik oluşturulabilir.

2.2.1. Genel Gereksinimler

Gerek KYS, gerekse BGYS standartları genel olarak proses yaklaşımını benimsemiş ve uygulamada bu çerçevede yapılandırılmıştır. Proses yaklaşımı standartların ana yapı taşlarıdır. Şekil 1.1'de KYS ve Şekil 1.3'de BGYS sistemleri proses yapıları görülmektedir. Bu standartların tamamı diğer yönetim sistemleri standartlarıyla da uyumluk gösterebilirler.

2.2.2. Kapsam

Yönetim sistemleri kurulum öncesi bilinmesi gereken en önemli basamak kapsamdır. Kapsam her Yönetim Sistemi'nin çerçevesinin oluşturmaktadır. Kuruluşlar yaptıkları faaliyetleri ve proseslerini tanımlamak zorundadırlar. Bu faaliyetlere kapsam denilmektedir. Kurulacak sistemlerde kapsam sistemin sınırlarını göstereceği için yönetim sistemleri bu kapsam çerçevesinde dokümante edecektir.

Kuruluşlar isterlerse her yönetim sistemi için ayrı ayrı kapsam oluşturabildikleri gibi entegre bir kapsamda oluşturabilirler. Sistemlerin her birinde kuruluş isterse uygulamadığı yani ürettiği ürün ve hizmeti dolaylı veya direk olarak etkilemeyen Standart maddelerinin şartlarını kapsam dışı bırakmayı talep edebilir [6]. Bunu ilgili standart maddesinin altında açıklamak zorundadır. Kapsamın dışına çıkarılan faaliyet kuruluşun yapmak zorunda olduğu faaliyetlerinden olmamalıdır.

Entegre olarak belirlenen bir kapsamda standartların birbiriyle eşleşmeyen maddeleri ilave olarak belirlenmelidir. Burada KYS den farklı olarak sadece BGYS kapsamında, güvenlik ile ilgili kontroller, kontrol amaçları ve kontroller altında toplanmıştır [21].

2.2.3. Atıf Yapılan Standartlar ve/veya Dokümanlar ve Terimler ve Tarifler

Bu bölüm her iki yönetim sisteminde mevcuttur. Dokümantasyon ilgili atıflar yapılmaktadır.

Her standarda kullanılan terim ve tarifler mevcuttur. Birçok terim ortak olarak kullanılmaktadır. KYS ve BGYS den oluşan bir entegre sistemde terimlerin tüm standart maddeleri için kullanıldığı unutulmamalıdır.

2.2.4. Yönetim Sistemi Planlama ve Kurulum

Yönetim sistemlerinin planlanması ve kurulumu her yönetim sisteminde mevcuttur. Gerek KYS ve gerekse BGYS yapılandırıldığı bölümdür ve iki sistemin planlaması ve kurulumu entegre olarak ele alınmalıdır.

Kalite Yönetim Sistemi'nde olduğu gibi BGYS'nin de kurulum isteği kurumun üst yönetimi tarafından benimsenmeli, gerekliliğine ve faydasına inanılmalıdır. Üst yönetim desteği BGYS'nin başarıya ulaşması açısından hayati öneme sahiptir [7].

BGYS genel gereksinimler maddesi altında sistemin gereklerini tanımlamaktadır. KYS de genel şartlar altında sistemin genel durumunu tanımlamaktadır. Her iki sistemde de sistemlerin planlanması ve kurulumu için Planla, Uygula, Kontrol et ve Önlem al döngüsü temel alınmaktadır. Buda bilgi güvenliğinin de kalite gibi yasayan bir süreç olarak ele alınmasını ve yönetilebilirlik ihtiyacını ortaya koymaktadır[22].

BGYS'nin kurulması ve yönetilmesi bilgi teknolojisi ürünü veya sistemi ile karıştırılmamalıdır [7]. BGYS öncelikle bir yönetim sistemidir ve diğer yönetim sistemleri ile birlikte düşünülmelidir.

2.2.5. Dokümantasyon Gereksinimleri

KYS ve BGYS proseslerinin etkin olarak planlanması, uygulanması ve kontrolünün sağlanması amacıyla kuruluşun ihtiyaç duyduğu dokümantasyon şart koşulmaktadır. Dokümantasyon gerek BGYS gerekse KYS gereksinimleri dikkate alınarak yapılmalıdır. Gereğinden fazla dokümantasyon sistemin yürütülmesinden ziyada dokümantasyonun yürütülmesi sorunu ortaya çıkar. Sistemlerin kendine özgü spesifik dokümanları oluşturulabilir. Ancak BGYS ve KYS proseslerinin etkin planlanmasını, işlemesini ve kontrolünü sağlamak için gereksinim duyulan dokümante edilmiş prosedürleri, politikalar, el kitapları, hedefler birlikte oluşturulmalıdır. Sistemin yürütülmesi uygulanacak dokümantasyon sistemi kâğıt üzerinde olabileceği gibi, elektronik ortamda da gerekli yetkiler tanımlanarak uygulanabilir [23].

BGYS'nin spesifik politikaları, kontrolleri, BGYS kapsamını, kontrolleri, Risk değerlendirme metodolojisinin bir tanımı, Risk değerlendirme raporu, Risk iyileştirme planı ve Uygulanabilirlik Bildirgesi gibi kuruluşun spesifik dokümanları da

oluşturulacaktır. Ancak bu dokümanların kontrolü doküman kontrolü kapsamına alınmalıdır [8, 13].

2.2.6. Yönetim Sorumluğu

Bilindiği üzere üst yönetimin desteği yönetim sistemlerinin olmazsa olmazıdır. Sistemlerin kuruluşta uygulanması, yerleşmesi ve sürekliliği ancak yönetimin desteği ile mümkündür. Yönetim bir işletmenin başarısı veya başarısızlığında önemli rol oynamaktadır [24]. Kuruluşun politikalarını ancak üst yönetim belirleyebilir. Çalışanlar bu politikalara uyar ve uygularlar. Pek çok yönetici bu tür çalışmalar konusunda desteğini dile getirse de, desteğin gerçekleşmesi söylemek kadar kolay olmamaktadır. Bu durum yöneticilerin kendi iş ve sorumluluklarının bulunmasından kaynaklanmaktadır [8, 13].

Üst yönetim KYS ve BGYS oluşan entegre sistemin temsilcisi olarak yönetim kademesinden birini belirlemelidir. Yönetim Temsilcisi'nin üst yönetim adına işletmede sistemin kurulması uygulanması ve gerekli kontrollerin yapılması için her iki standartta da ortak ve zorunlu olan yönetimin gözden geçirmelerini birlikte yapabilmesine imkân verilmiştir.

Yönetimim gözden geçirme toplantıları entegre olarak planlamalı, gündem maddelerinin birleştirmeli ve toplantıda alınan kararların her iki sistem için alındığına dikkat edilmelidir. Yönetim temsilcilerinin görevleri arasında çoğu zaman eksik olan müşteriye verilen önemin, müşterinin isteklerini yerine getirmek için tüm çalışanları bilgilendirmek ve muhtemel müşteri memnuniyetsizliklerini engellemek için sistematik çalışmalar yapılarak desteklenmesi entegre sistem açısından da gereklidir [25].

2.2.7. Kaynak Yönetimi

Standartlarda kaynak terimi her ne kadar insan kaynağını öne çıkmışsa da entegre sistemi'nin ihtiyaç duyduğu tüm kaynakları kapsar. Bu kaynaklar standartlarda açıkça belirtilmiş olmasa da, personel, donanım, makine, teçhizat, bina, zaman, malzeme, ekipman, yazılım vb.dir [6]. Üst yönetim KYS ve BGYS sistemlerinin kaynakların kapsamını, belirlenmesini, sağlanmasını ve tanımlanmış nitelikte insan kaynakları temin etmelidir. Personelin eğitim ihtiyaçları tespit etmeli ve gerekirse nitelikli personel istihdam etmelidir [5, 13]. Çalışanların kalite ve bilgi güvenliği konusunda bilinçli olmaları

gerekirken, kurumların bilgi güvenliği konusunda kurumsal önlemler almaları ise mutlaka yapılması gereken görevler arasındadır [26]. Burada önemli olan her çalışanın sadece ihtiyaçları kadar bilgiye erişim izni olmalıdır [27]. Daha fazla yetki güvenlik ve denetim açıklarına sebep olmaktadır.

Kuruluşlar tarafından kalite ile birlikte uygulanacak bilgi güvenliği bilinçlendirme çalışması, bilgi güvenliğinin önemini anlamaları ve eğitim eksikliğinin giderilmesinde kritik öneme sahiptir. İyi planlanmış, tasarlanmış ve yürütülmüş çalışan bilinçlendirme çalışması bilgi güvenliğinde en zayıf halkasının güçlendirilmesinde büyük öneme haizdir [28].

KYS üzerine BGYS oluşturmanın zamandan ve kaynaklardan önemli ölçüde tasarruf sağladığı, ayrıca mevcut sistemi geliştirdiği görülecektir [29].

2.2.8. İç Denetimleri(Tetkik)

İç tetkik, tetkik delili elde etmek ve tetkik kriterlerinin karşılanma derecesini objektif olarak değerlendirmek için yapılan sistematik, bağımsız ve belgelendirilmiş prosestir [30].

Kurulan ve uygulanan KYS ve BGYS planlamaları, prosedürleri, standardın şartları, etkin olarak uygulanıp uygulanmadığı ve sürekliliğinin sağlanıp sağlanmadığını belirlemek için planlı periyotlarda iç tetkikler yapılmalıdır [5, 13]. Yapılan iç tetkiklerin kayıtları muhafaza edilmelidir. Bir iç tetkik denetleme programı iç tetkik eğitimi almış personel tarafından, bir önceki denetim sonuçlarının yanı sıra denetlenecek proseslerin ve alanların durumu ve önemi dikkate alınarak planlanmalıdır. Tetkik kriterleri, kapsamı, sıklık ve yöntemler tanımlanmalıdır. Tetkikçilerin seçiminde ve tetkiklerin gerçekleştirilmesinde, tetkik prosesinin objektif ve tarafsız olması sağlanmalıdır [8, 31].

Entegre sistem tetkiklerin planlanması ve yürütülmesi ve sonuçların raporlanması ve kayıtların tutulmasındaki sorumluluklar ve gereksinimler, yazılı hale getirilmiş iç tetkik prosedürü içinde tanımlanmalıdır [5, 13, 31].

Tetkiklerin planlanması ve uygulaması KYS ve BGYS sistemi iç tetkik eğitimi almış tetkikçiler tarafından yapılmalıdır. Tetkikler zamanında ve tetkik programına göre yapılmalı gerekirse takip tetkikleri de yapılmalıdır.

2.2.9. Yönetimin Gözden Geçirmesi

Üst yönetim, kuruluşun KYS ve BGYS sistem planlamalarına uygunluk, yeterlilik ve etkinliğinin sürekliliğini sağlamak için planlanmış aralıklarla gözden geçirmelidir. Bu gözden geçirme iyileştirme fırsatlarının ve kalite ve bilgi güvenliği politikası ve hedeflerini içeren bir değerlendirme yapması sağlanmalıdır [5, 8, 13].

Yönetimim gözden geçirmeleri birlikte planlamalı, gündem maddeleri birleştirmelidir. Yönetimin gözden geçirme toplantılarının gündemini BGYS ve KYS politikaları, iç tetkik sonuçları, müşteri ihtiyaç ve beklentileri, proseslerin performans uygunluğu, düzeltici ve önleyici faaliyetler ve iyileştirme önerileri gibi standartların zorunlu maddeleri mutlaka gündem arasında olmalıdır.

Yönetimim gözden geçirme toplantılarında alınan entegre sistemi etkileyebilecek değişiklikler ve kaynak planlamalarına ilişkin kararların her iki sitem için olduğu bilinmelidir.

2.2.10. Sürekli İyileştirme

Sürekli iyileştirme, kuruluşun ürettiği ürün veya hizmetin müşteri şartları, kalite gereksinimleri ve yasal şartların yerine getirilmesi yeteneğinin artırmak için tekrar eden faaliyetlerdir[1]. Kuruluşlar aşağıdakiler için gerekli olan izleme, ölçme, analiz ve iyileştirme proseslerini plânlamalı ve uygulanmalıdır. Bunlar:

Ürün ve hizmet şartlarına uygunluğu göstermek,

BGYS ve KYS sistemlerinin uygunluğunu güvence altına almak ve bu sistemlerin etkinliğini sürekli iyileştirmektir [5, 13].

Kuruluş sürekli iyileşmeyi kalıcı ve bağlılık ilkesi olarak kabul ederler. Anlaşılması amacıyla oluşturduğu kalite ve bilgi güvenliği politikalarına yazarak bu taahhüdünü sürekli kılar. Yönetimin gözden geçirmesi kapsamında yapılan toplantılarda, belirli aralıklarla ölçülen ve sürekli izlenen hedefler ve sürekli iyileşme faaliyetleri görüşülür [31].

2.2.11. Düzeltici Faaliyet

Düzeltici faaliyet, saptanan bir uygunsuzluğun sebebini veya diğer istenmeyen durumu ortadan kaldırma için yapılan faaliyettir[1]. Kuruluş, meydana gelen

uygunsuzlukların nedenlerini gidermek ve tekrarlarını önlemek için karşılaşılan uygunsuzlukların etkilerine uygun tedbirler ve düzeltici faaliyetler planlanmalıdır. Düzeltici faaliyetler uygunsuzluğun büyüklüğüne ve etkilerine göre entegre olarak planlanmalıdır[5, 13]. Böylece kaynaklar etkin olarak kullanılmış olacaktır.

Yapılan düzeltici faaliyetler müşteri şikâyetlerini, uygunsuzlukların nedenlerinin belirlenmesi için düzeltici faaliyet ihtiyacının tespiti ve uygulanan düzeltici faaliyetlerin sonuçlarının kayıtlarının tutulmasını düzeltici faaliyetlerin etkinliklerinin gözden geçirilmesi amacıyla Düzeltici Faaliyetler Prosedürü BGYS ve KYS için ortak dokümante edilmelidir.

2.2.12. Önleyici Faaliyet

Önleyici faaliyet, potansiyel bir uygunsuzluğun sebebinin veya istenmeyen diğer potansiyel durumların ortadan kaldırılması için yapılan faaliyetlerdir[1,13]. Kuruluş, potansiyel uygunsuzlukların nedenlerini gidermek, uygunsuzluk oluşumunu engellemek, önleyici faaliyet ihtiyacının değerlendirilmesi ve bu önleyici faaliyetlerin sonuçlarının kayıtlarının tutulması ve etkinliklerinin gözden geçirilmesi için Önleyici Faaliyetler Prosedürü BGYS ve KYS için ortak dokümante edilmelidir[5, 13].

Önleyici faaliyetler potansiyel uygunsuzluğun büyüklüğüne ve etkilerine göre entegre olarak planlanmalı böylece kaynaklar etkin olarak kullanılmış olsun [5, 13].

2.2.13. Kontrol Amaçları ve Kontroller

Kontrol amaçları ve kontroller, ISO/IEC 17799 Standardının madde 5 ile madde 15, TS ISO/IEC 27001:2005 Standardında Ek-A olarak madde A.5 ile madde A.15'te belirtilen kontrollerin desteğiyle gerçekleştirme önerisi ve en iyi uygulamaya ilişkin kılavuzluk sağlar[13]. Kontrol amaçları ve kontroller BGYS'ye ait kontrol dokümanı olup, uygunluk bildirgesi altına hazırlanması gereken zorunlu bir dokümandır. Bu doküman sadece BGYS sistemi ait olup sadece BGYS maddeleri dikkate alınarak hazırlanmalıdır. Bu dokümanın kontrolü de diğer tüm dokümantasyon gibi entegre sistem doküman kontrolü altında olmalıdır.

3. BULGULAR

3.1 Uygulama Yapılan İşletme Hakkında Genel Bilgiler

3.1.1. İşletmenin Kısa Tanımı

Netsolution Limited Şirketi 2006 Şubat ayından itibaren Teknoloji Geliştirme Merkezi'nde faaliyetlilerine devam etmektedir.

Firmanın başlıca hizmetleri; Yazılım, Entegrasyon, Danışmanlık ve İnteraktif web hizmetleri sunmaktadır.

Kuruluşta TS EN ISO 9001:2008 Standartları uygulanmaktadır ve Bu kuruluşun Kalite Yönetim Sistemi akredite belgelendirme bir kuruluşundan belgesi mevcuttur.

Yazılım otomasyonu temelde aşağıdaki özellikleri içermektedir. Bunlarla birlikte kamera sistemi, otomatik plaka okuma modülü, plaka okuma ile entegre bariyer kontrol modülü, ülkemizde yaygın olarak kullanılan elektronik kantarlar ile tam entegre tartım modülü, otomatik araç tanıma modülü, giriş çıkış kayıtlarının loglama modülü, entegre gelir, muhasebe tahakkuk ve tahsilat yönetim modülü, ürün birim dara yönetimi modülü, kullanıcı ve personel yönetim modülü, yazıhane yönetim modülü, peron yönetim modülü, nakliyeci modülü, rayiç bedel yönetim modülü ve vardiya yönetim modülü gibi ürünleri mevcuttur.

3.1.2. İşletmenin Vizyonu

Bilişim sektöründe Türkiye ekonomisine katkıda bulunmak, müşteri memnuniyetini sağlamak, yurt içinde ve yurt dışında öncü firma olmaktır.

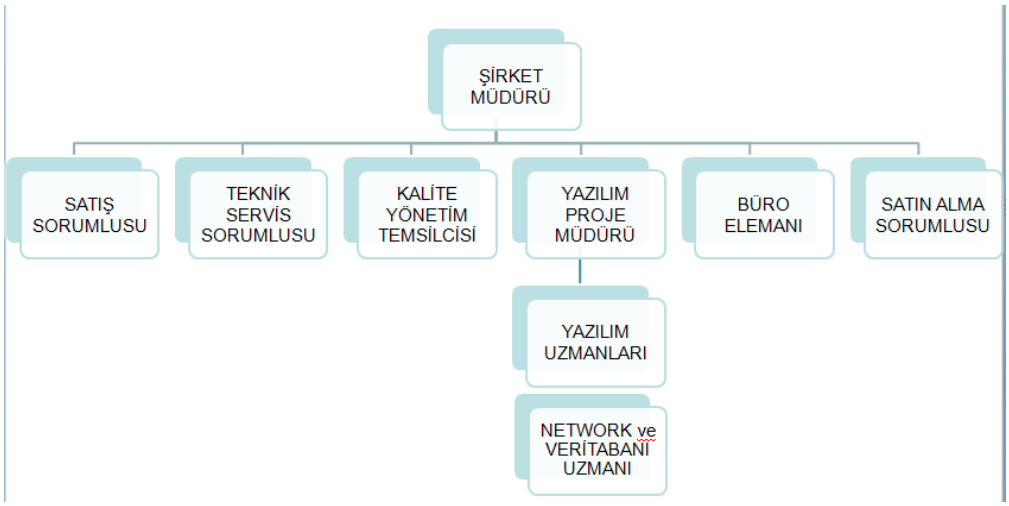
3.1.3. İşletmenin Misyonu

Başarıya odaklanarak,
Aynı amaca yönelerek,
İleri teknolojiyi takip ederek,
Takım ruhuyla hareket ederek,
Müşteri memnuniyetini en üst seviyede tutarak,

Mühendislik prensiplerini uygulayarak,

Müşterilerimize katma değer sağlamaktır.

3.1.4. İşletmesinin Organizasyon Şeması



Şekil 3.1 Kuruluş Organizasyon Şeması

3.2. Uygulama

Bilgi Güvenliği Yönetim Sistemi ile Kalite Yönetim Sistemi için her iki standartta da zorunlu ve ortak maddeler ana bölümlere ilişkin bulgular aktarılacaktır.

3.2.1. Yönetim Sistemlerinin Tanımlanması ve Kurulum Süreci

3.2.1.1. Kapsam Belirleme

Kuruluşta TS EN ISO 9001:2008 ve TS ISO /IEC 27001:2005 standartlarının öngördüğü şartlara uygun olarak. KYS ve BGYS sistemlerinin sınırlarını belirleyen ve uygulama alanlarını tanımlayan ortak ve tekbir kapsam belirlenmiştir.

“Bilgisayar yazılımı, donanım, kablolama, taahhüt, veri girişi ve bilgi işlem destek hizmetleri”

Burada uygulayıcılar olarak her iki sistem için tek kapsam belirleneceği gibi ayrı ayrı kapsam belirlenebilir. Entegre yönetim sistemi her iki sistemi azami ölçüde içine alan işletmenin ana faaliyetlerini kapsayan bir kapsam hazırlanmış buda sistemin planlanmasında paralellik sağlamıştır.

BGYS sınırlarının belirlenmesinde aşağıda faaliyetler ele alınmıştır.

- Sistem analizi, kuruluş lokasyonu içindeki yerel / geniş alan ağlarının yönetimi, izlenmesi, kontrol ve denetimini,
- Kuruluş lokasyonu için bilgi güvenlik hizmetlerini (yedekleme, felaket senaryoları, aynalama -mirroring- vb.),
- Kuruluş lokasyonu içindeki yerel / geniş ağ altyapısının sürekliliğinin (kablolama, sunucu odası, router, switch, sunucular vb.) sağlanması,
- Kuruluş lokasyonu içinde gerektiğinde yerel / geniş alan ağlarının yeniden kurulması ve yapılandırmasını (donanım, yazılım, işletim sistemi vb.

sağlamak veya gerçekleştirmek olarak belirlenmiştir.

3.2.1.2. Prosesleri Tanımlama

TS EN ISO 9001:2008 ve TS ISO /IEC 27001:2005 için ihtiyaç duyulan prosesler ve uygulamaları tanımlanmış olup yazılı hale getirilmiştir. Prosedürler, talimatlar, veri toplama formları gibi ihtiyaç duyulan dokümanlar entegre olarak hazırlanarak yürürlüğe konulmuştur.

Kuruluşta ortak olarak; Satın alma Prosesi, Sürekli İyileştirme Prosesi, Eğitim Prosesi, Teknik Servis Prosesi, Tasarım Prosesi ve Sürekli İyileştirme Prosesleri oluşturulmuştur.

Oluşturulan iş proseslerinin sırası ve etkileşimleri prosedürler ve talimatlar ile belirlenmiştir.

Proseslerin sırası, birbirileriyle olan etkileşimleri, yürütülmesi, izlenmesi, ölçme ve analiz edilip değerlendirilmesi sağlanmaktadır. Prosesler için gerekli kaynaklar temin edilmekte ve bilgiler hazır bulundurulmaktadır. KYS ve BGYS proses etkileşimi, Proses Etkileşim Şeması (Şekil 3.3) de standardize edilmiştir.

KYS sistemine ilave olarak BGYS proseslerinin belirlenmesinde Sistem analizi, yerel / geniş alan ağlarının yönetimi, izlenmesi, kontrol ve denetimi prosesi.

Kuruluş lokasyonu için bilgi güvenlik hizmetlerini (yedekleme, felaket senaryoları, aynalama -mirroring- vb.) prosesi.

Kuruluş lokasyonu içindeki yerel / geniş ağ altyapısının sürekliliğinin (kablolama, sunucu odası, router, switch, sunucular vb.) sağlanması ve gerçekleştirilmesi prosesi olarak belirlenmiştir.

Oluşturulan sistemin etkin olarak işletilmesi sağlanmakta ve iş proseslerinin çıktıları ölçülerek uygun olduğunda sürekli iyileştirme çalışmaları yapılmaktadır.

Proseslerin Entegre olarak oluşturulması yapılan işlemlerin hem KYS hem de BGYS sistemi tarafından sürekli olarak kontrol edilmesine ve sistemlerin birinde yapılan bir değişikliğin etkisi ölçüsünde diğer yönetim sistemine de yansıtılması mümkün olmuştur.

Kalite Yönetim Sistemi ve Bilgi Güvenliği Yönetim Sistemi'nin entegre olarak anlaşılması ve uygulanması için KYS ve BGYS Planlama Prosedürü (Şekil 3.2) deki gibi oluşturulmuştur.

AMAÇ : Bu prosedürün amacı; yapılan veya yapılacak faaliyetlerde, KYS ve BGYS boyutlarının ve etkilerinin belirlenmesi, kanuni ve diğer şartların tespit edilmesi, yapılan çalışmaların belirlenen şartlara uygunluğunun sağlanması, BGYS amaç ve hedeflerinin belirlenmesi, bu amaç ve hedefleri gerçekleştirmek üzere KYS ve BGYS programların ve yıllık planlarının oluşturulmasını sağlamaktır.

SORUMLULUKLAR

Bu prosedürün uygulattırılmasından

- Üst Yönetim,
- Yapılan planlama ve diğer sistem uygulamalarının gerçekleştirilmesinden KYS ve KYS ve BGYS Yönetim Temsilcisi ve BGYS Koordinasyon Grubu, sorumludur.

TANIMLAR

Üst Yönetim	:	ÜY	:
Bölüm / Birim Sorumlusu	:	BS	:
BGYS Koordinasyon Grubu	:	BGYS-KG	:

UYGULAMA

1. KYS ve BGYS Boyutlarının Belirlenmesi:

I. BGYS, kurumun altyapı, personel, kullanılan teknolojiler, donanım ve yazılımlarla yürüttüğü faaliyetler sonucunda oluşan etkilere odaklanır. Bu etkilerin kaynakları iki kategoriye ayrılır.

1. Altyapı, personel, teknoloji, donanım, yazılım zaafiyetleri
2. Yangın, sel, deprem, savaş hali, saldırı ve terör olayları gibi önceden bilinemeyen oluşumlar.

BGYS öncelikle;

a. 1. Maddede yer alan zaafiyetler ve bu zaafiyetlerden kaynaklanan tehditlere odaklanır. Tehditlerin ortaya çıkma olasılıklarına göre "Risk Analizi ve Yönetimi Raporu"na göre çalışmalarını yürütür.

b. 2. Madde için genel tedbirler "BGYS Yıllık Plan" içinde tanımlanır.

II. İşletme bünyesinde, BGYS için gerekli olan riskler; Risk Analiz ve Yönetim Raporu içinde yer alan Risk Hafifletme Planı üzerinden izlenir.

III. Risk Hafifletme Planı ile tanımlanan her faaliyet veya faaliyet grubu için Risk Planlama Formu.xls doldurulur.

IV. Risk Planlama formunda ilgili birim faaliyetleri için kullanılan girdiler belirtilerek bu girdiler kapsamında oluşan riskler olay ihlal kayıtlarına göre forma işlenir.

V. Bu form yönetimin gözden geçirme toplantısının girdisidir.

VI. Her birime ait formlar birim yöneticisi sorumluluğundadır.

VII. İlgili birim yöneticileri tarafından bu faaliyetlerin olası BGY boyutu, etkileri ve tabi olduğu mevzuata ilişkin bilgiler, Riski Olan Faaliyetler Formu.xls ile tespit edilir.

VIII. Yapılan bu çalışmaların sonuçları, BGYS koordinasyon grubu tarafından değerlendirilerek oluşan her riskin etkilerinin analizi yapılarak önem sırası Risk Öncelikleri Formu.xls ile derecelendirilir ve sayısallaştırılır.

2. Amaç ve Hedefler:

I. BGYS koordinasyon grubu tarafından, risk değerleri ortaya çıkarıldıktan sonra Kalite ve BGYS politikaları yönetimce belirlenir.

II. Hedefler Üst Yönetim, KYS ve KYS ve BGYS Yönetim Temsilcisi tarafından onaylanır.

III. Onaylanan hedefler ilan panolarına asılır veya ilgili personele dağıtılır.

IV. Böylece hedef ve amaçların tüm personel tarafından bilinmesi sağlanır.

V. Yönetimin gözden geçirmesi toplantılarında amaç ve hedefler yönetimce gözden geçirilir ve gerekli ise revize edilir.

VI. Amaç ve hedefler yönetim tarafından Gözden Geçirme Talimatı uyarınca gözden geçirilir.

3. Kanuni Ve Diğer Şartlar:

I. Tespit edilen faaliyetlerin ve etkilerinin tabi olduğu kanun, yönetmelik, mevzuat KYS ve BGYS Yönetim Temsilcisi tarafından temin edilir ve bu mevzuat veya teknik gereklilikler doğrultusunda çalışmalar başlatılır.

II. Dış Kaynaklı Doküman Listesi ile kayıt altına alınarak sistem içerisinde yürürlüğe girmesi sağlanır.

III. Mevzuattaki değişiklik ve gelişmelerin takibi KYS ve BGYS Yönetim Temsilcisi ve BGYS Koordinasyon Grubu tarafından yapılır.

IV. İlgili mevzuatlarda değişiklik olması durumunda eski mevzuat bilgisi listeden çıkarılır ve güncel olan yeni bilgi, dış kaynaklı doküman listesine eklenir.

4. BGYS Etki Önem Analizi ile BGYS Etki Önem Puanının Belirlenmesi:

I. Risk Öncelikleri Formu.xls ile tespit edilen ve sayısallaştırılan risklerin **Risk Puanı** ve derecesi (düşük, orta, yüksek) form üzerinde değerlendirilir.

II. En yüksek puanı olan etkiler önem sırasında öncelikli olarak ele alınır.

III. Risk değeri "yüksek (high)" olanlar derhal ve risk değeri "orta (medium)" olanlar BGYS Planı çerçevesinde bertaraf edilmek üzere çalışma başlatılır.

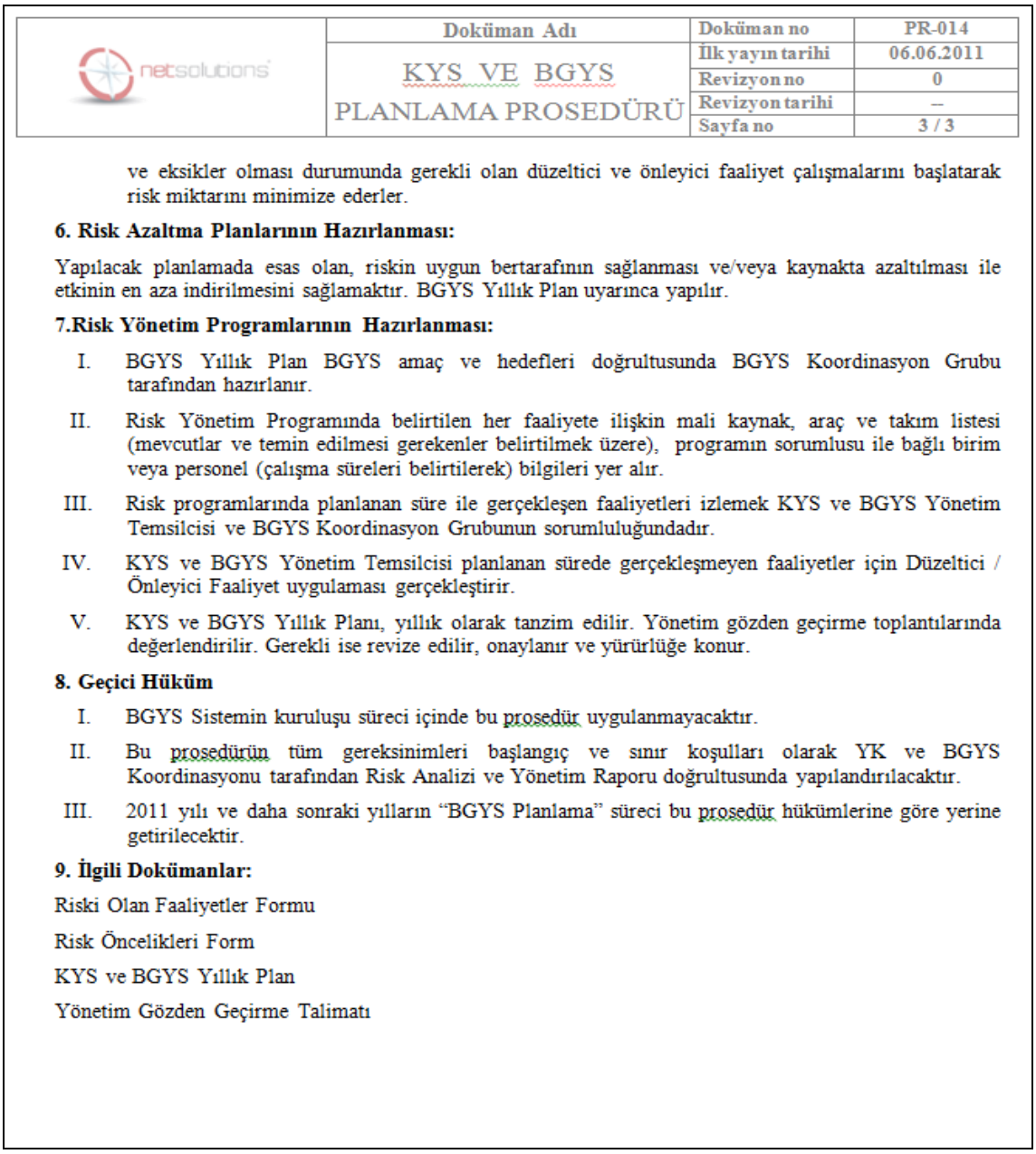
IV. Bu çalışmaların sonuçları, yapılacak olanlar, yapılması planlananlar BGYS Yıllık Plan içinde tanımlanır.

5.Uygunluğun Değerlendirilmesi:

I. İşletmede riskli olan faaliyetler için ya da mevcutta bulunan rutin faaliyetlere riski olan yeni bir faaliyet eklenmesi durumunda BGYS Koordinasyon Grubu ve KYS ve BGYS Yönetim Temsilcisi tarafından Risk Etki Değerlendirmeleri gerçekleştirilir.

II. Yapılan tüm bu faaliyetlerin neticesinde elde edilen sonuçlar BGYS Koordinasyon Grubu ve KYS ve BGYS Yönetim Temsilcisi tarafından ISO 9001 standardı 8.2.4 maddesine uygun şekilde izler ve ölçer.

III. Elde edilen veriler BGYS Koordinasyon Grubunca ve KYS ve BGYS Yönetim Temsilcisi tarafından BGYS faaliyetlerin izlendiği formlar üzerinden istatistiksel analizlerle değerlendirilir



	Doküman Adı	Doküman no	PR-014
netsolutions	KYS VE BGYS PLANLAMA PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	0
		Revizyon tarihi	–
		Sayfa no	3 / 3

ve eksikler olması durumunda gerekli olan düzeltici ve önleyici faaliyet çalışmalarını başlatarak risk miktarını minimize ederler.

6. Risk Azaltma Planlarının Hazırlanması:

Yapılacak planlamada esas olan, riskin uygun bertarafının sağlanması ve/veya kaynakta azaltılması ile etkinin en aza indirilmesini sağlamaktır. BGYS Yıllık Plan uyarınca yapılır.

7.Risk Yönetim Programlarının Hazırlanması:

I. BGYS Yıllık Plan BGYS amaç ve hedefleri doğrultusunda BGYS Koordinasyon Grubu tarafından hazırlanır.

II. Risk Yönetim Programında belirtilen her faaliyete ilişkin mali kaynak, araç ve takım listesi (mevcutlar ve temin edilmesi gerekenler belirtilmek üzere), programın sorumlusu ile bağlı birim veya personel (çalışma süreleri belirtilerek) bilgileri yer alır.

III. Risk programlarında planlanan süre ile gerçekleşen faaliyetleri izlemek KYS ve BGYS Yönetim Temsilcisi ve BGYS Koordinasyon Grubunun sorumluluğundadır.

IV. KYS ve BGYS Yönetim Temsilcisi planlanan sürede gerçekleşmeyen faaliyetler için Düzeltici / Önleyici Faaliyet uygulaması gerçekleştirir.

V. KYS ve BGYS Yıllık Planı, yıllık olarak tanzim edilir. Yönetim gözden geçirme toplantılarında değerlendirilir. Gerekli ise revize edilir, onaylanır ve yürürlüğe konur.

8. Geçici Hüküm

I. BGYS Sistemin kuruluşu süreci içinde bu prosedür uygulanmayacaktır.

II. Bu prosedürün tüm gereksinimleri başlangıç ve sınır koşulları olarak YK ve BGYS Koordinasyonu tarafından Risk Analizi ve Yönetim Raporu doğrultusunda yapılandırılacaktır.

III. 2011 yılı ve daha sonraki yılların "BGYS Planlama" süreci bu prosedür hükümlerine göre yerine getirilecektir.

9. İlgili Dokümanlar:

Riski Olan Faaliyetler Formu

Risk Öncelikleri Form

KYS ve BGYS Yıllık Plan

Yönetim Gözden Geçirme Talimatı

Şekil 3.2 KYS ve BGYS Planlama Prosedürü

3.2.2. Dokümantasyon Süreci

TS EN ISO 9001:2008 ve TS ISO /IEC 27001:2005 dokümantasyonu; kuruluşun büyüklüğü, fiziksel uzaklıklar, yaptığımız faaliyetler ve personelimizin yetkinliği dikkate alınarak hazırlanmıştır.

Kuruluşun dokümantasyon yapısı aşağıdaki gibidir;

Kalite ve Bilgi Güvenliği Politikası ve Hedefleri Vizyonu: Kuruluş politikası ortak olarak hazırlanmıştır. Buda çalışanların kuruluşun politikasına olan algılarının tam

olmasına ve her iki sisteminde çalışanlar ve kuruluş tarafından ortak olarak yürütüldüğüne yönelik bilinçlendirmeyi sağlamıştır.

El Kitabı: KYS ve BGYS el kitabı her sistem için entegre el kitabı olarak oluşturulmuştur. BGYS kapsamında her ne kadar el kitabı zorunluğu olmasa da sistemin bütünlüğü göz önüne alınmıştır. TS EN ISO 9001:2008 ve TS ISO /IEC 27001:2005 Standartları paralelinde ve entegre el kitabı oluşturulmuş ve sürekliliği sağlanmaktadır.
Bu el kitabı KYS ve BGYS sistemlerini kapsar. Entegre sisteme göre hazırlanmış olan prosedürleri atıfta bulunur. Entegre yönetim sistemi proseslerini açıklar.

Prosedürler: KYS ve BGYS standartlarının zorunlu olan ve kuruluşun ihtiyaç duyduğu prosedürler entegre olarak dokümante edilmiştir. Prosedürler, sistemimizin uygulama safhalarını ve işleyişini anlatır. Gerektiğinde yetki ve sorumlulukları da ortaya koyar. KYS ve BGYS Yönetim Sistemi'ni oluşturan diğer dokümanlara atıf yapar. Kuruluşta KYS ve BGYS kapsamında prosedürler hazırlanmıştır. Kuruluşta dokümanların hazırlanması, kontrolü, yürürlüğü girmesi ve değişikliklerin kontörlü ve dağıtımını sağlamak için Doküman Kontrol Prosedürü oluşturulmuştur (Şekil 3.3). Entegre hazırlanan bu prosedürler ile sistemlerin dokümantasyon yapısı ve uygulaması kolaylaştırılmıştır.

1.AMAÇ:

KALİTE VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ kapsamındaki dokümanların hazırlanması onaylanması ve kontrollü şartlar altında uygulanması ve gözden geçirilerek güncelliğinin sağlanması.

2.KAPSAM

KYS VE BGYS sistemi içinde yer alan dokümantasyonu kapsar.

3.SORUMLULAR:

1- Şirket Müdürü
2- Kalite ve Bilgi Güvenliği Yönetim temsilcisi
3- Birim Sorumluları
4- KYS VE BGYS kapsamında çalışan tüm personel

4.TANIMLAR:

KYS VE BGYS : Kalite ve Bilgi Güvenliği Yönetim Sistemi
KONTROLLU DOKÜMAN: Güncelliğinin takip edilmesi zorunlu olan kırmızı renkli "KONTROLLU DOKÜMAN" kaşesi bulunan dokümanlardır.
KONTROLSÜZ DOKÜMAN: Güncelliğinin takip edilmesine gerek olmayan ve bilgi amaçlı dağıtılan dokümanlardır.
STANDART SAYFA: Kalite ve Bilgi Güvenliği El Kitabı, Prosedürler, Talimatlar, Akış Şemaları ve Görev Tanımlarında kullanılan şablon form **(FR-001),** bunlarında dışında kalan dokümanlarda (FR-PL-RP-LS vb.) standart sayfa şartı aranmaz

5. PROSEDÜR:

1- DOKÜMAN HAZIRLAMA VE ONAYLAMA

1.1 -KYS VE BGYS kapsamındaki doküman adları ve hazırlama ve onaylama yetkilisi aşağıdaki tabloda belirtilmiştir. Bu dokümanlar Kontrole Tabi Olan Dokümanlar;

DÖKÜMANIN ADI	HAZIRLAYAN	ONAYLAYAN
Kalite ve Bilgi Güvenliği El Kitabı (KE)	KYT	GM
Kalite ve Bilgi Güvenliği Politikası / Kalite ve Bilgi Güvenliği Hedefleri –PO/KH	KYT	GM
Proses Akış Şemaları (PS)	KYT	GM
KYS ve BGYS Zorunlu Prosedürleri (PR)	KYT	GM
Diğer Prosedürler (PR)	KYT	GM
Diğer Dokümanlar (TL-FR-LS-PL-TB-RP)	KYT	GM
Satın alma Şartnameleri (SŞ)	SAT.S	KYT
Girdi, Proses ve Ürün Kalite ve Bilgi Güvenliği Planı(PL)	TSS	KYT
Görev Tanımları (GT)	KYT	GM
Ürün Akış Şemaları (AŞ)	KYT	GM
Organizasyon Şeması (OŞ)	KYT	GM

1.2-Kalite ve Bilgi Güvenliği Yönetim Sistemi Dokümanları Madde–1 de tanımlanan şekilde hazırlanır ve onaylanır.
1.3-Dokümanlardan KE, AŞ, PR, TL, GT "Standart Sayfa" formatında hazırlanır **(FR-001).** PS-FR-LS-TB-PL-RP-ŞT-OŞ-YP- ve benzeri dokümanlarda standart sayfanın başlık kısmı şartı aranır hazırlayan ve onaylayan kısım şartı aranmaz.

1.4 Bu dokuman, orijinal doküman olarak tanımlanır ve ıslak imza ile geçerli olur. Orijinalinden kopyalanarak dağıtılanlara ise, ıslak KIRMIZI renkli "KONTROLLÜ DÖKÜMAN" kaşesi basılarak dağıtım listesine göre ve imza karşılığı yapılır. **(Kayıt olarak kullanılan dokümanlarda "kontrollü doküman" kaşesi şartı aranmaz fakat ilgili birimde örnek olarak "kontrollü doküman" kaşeli bir sureti saklanır.)** Bilgi amaçlı olarak dağıtılan dokümanlara ise, her bir sayfasına ıslak MAVİ renkli "BİLGİ İÇİNDİR" kaşesi basılarak, dağıtım listesi kaydı yapılmadan verilebilir.

2-DÖKÜMANLARDA BULUNMASI GEREKEN ASGARİ BİLGİLER

(Doküman Formatları)

K.E. : Kalite ve Bilgi Güvenliği El Kitabında en az TS ISO 9001-2008 standardının 4.2.2 maddesindeki ve ISO/TR 10013-2001 4.4 maddesindeki bilgiler bulunur.

Kalite ve Bilgi Güvenliği Yönetim Sistemi (KYS VE BGYS) Prosedürleri (PR) : ISO/TR 10013–2000 4.5 maddesindeki formata uygun olarak hazırlanır

Talimat (TL) : Yapılan her iş(lem) için yapacak kişinin anlayacağı dille ayrıntılı olarak yazılmış kontrollü dokümanlardır. Eğitim ve uygulama amaçlı hazırlanmıştır. İş yapılan noktalara kadar dağıtımları yapılır ve takipleri yapılır.

Satın alma Şartnamesi (SŞ) : Satın alınacak malzemeler için oluşturulur. Ürüne yönelik temel bilgiler yer alır.

Hammadde, Proses ve Ürün Kalite ve Bilgi Güvenliği Planı (KP) : Firmamızda yapılması gereken kontrollerin neler olduğunu bu kontrollerin hangi sıklıkta yapıldığını, kabul kriterlerini, sorumluluklarını varsa ölçüm cihazlarını ve sonuçlarının kayıt yerlerini tanımlayan kontrollü dokümanlardır. Eğitim ve uygulama amaçlı hazırlanmıştır.

Formlar (FR) : Firmamızda yapılan Kalite ve Bilgi Güvenliği yönetim sistemine ait faaliyetlerin kayıt altına almak amacıyla matbu olarak hazırlatılmış dokümanlardır.

Görev Tanımları (GT) : Firmamızda çalışan, tüm departmanlardaki çalışanların yapmış oldukları işleri kayıt altına almak için hazırlanmış dokümanlardır.

3-KALİTE VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ DOKÜMAN KODLAMA SİSTEMİ

6.3.1 DOKÜMAN KISALTMALARI			6.3.2 BÖLÜMLER KISALTMALARI	
Kalite ve Bilgi Güvenliği El Kitabı	KE		Şirket Müdürü	GM
Proses	PS		Kalite ve Bilgi Güvenliği Yönetin Temsilcisi	KYT
Prosedür	PR		İdari Mali İşler Sorumlusu	İMS
Görev Tanımı	GT		Satış Sorumlusu	SS
Talimat	TL		Satınalma Sorumlusu	SAT.S.
Plan	PL		Teknik Servis Sor.	TSS
Politika	PO			
Form, Fiş, Program,	FR			
Tablo	TB			

Rapor	RP			
Liste	LS			
Organizasyon Şeması	OŞ			
Yerleşim Planı	YP			
Şartname	SŞ			
Kalite ve Bilgi Güvenliği Hedefleri	KH			
Kalite ve Bilgi Güvenliği Planı	KP			
Akış Şeması	AŞ			

3.2 DOKÜMAN VE KALİTE VE BİLGİ GÜVENLİĞİ KAYDI KODLAMASI

-- XXX

Doküman/Kalite ve Bilgi Güvenliği Kaydı No

Doküman ve Kalite ve Bilgi Güvenliği Kaydı Kısaltması

SAYFA NO: a/b a : Sayfa Numarasını, b : Toplam Sayfa sayısını gösterir.

4. DOKÜMAN DAĞITIMI GÜNCELİĞİNİN TAKİBİ VE DEĞİŞİKLİK KONTROLÜ

4.1 Tüm dokümanların ilk yayınlarına ve revizyonlarına ait dağıtımlar İlgili Birimlere Yön. Tem. tarafından imza karşılığı dağıtılır **(FR-002)**. Revizyona uğramış dokümanlar kullanım yerinden toplanır sadece orijinal dokümana iptal kaşesi vurularak Kayıtların Kontrolü Prosedürüne göre saklanır, diğerleri anında yakılarak veya yırtılarak imha edilir.

4.2 KYS VE BGYS içersisinde yer alan tüm dokümanlar, doküman ana listesi **(LS-001)** aracılığıyla Yön. Tem. tarafından takibi yapılır. (Doküman ana listesinde dokümanın adı ilk yayını, revizyon durumu Revizyon tarihi ve kullanıldığı alanlar hakkında bilgiler bulunur).

4.3 Dış kaynaklı dokümanlar dış kaynaklı dokümanlar listesi **(LS-002)** aracılığıyla Yön. Temsilcisi tarafından takip edilir. Dış kaynaklı dokümanlarda değişiklik olduğunda ilgililere Yön. Temsilcisi tarafından yenisi verilerek eskileri toplanır. Bir sureti bilgi amaçlı olarak İPTAL KAŞESİ (KIRMIZI RENKLİ) vurularak saklanır.

4.4 Dış kaynaklı dokümanların güncelliği Yönetim Temsilcisi tarafından ilgili kuruluşun yayınları, web sayfası ve/veya gerektiğinde abonelik sistemi (Standart aboneliği, resmi gazete aboneliği) v.b. metotlar ile takip edilir

4.5 Dokümanlar yılda bir kez hazırlayan birimlerce gözden geçirilir ve herhangi bir değişiklik ihtiyacı olduğunda değişiklikler 4.6/4.7/4.8 maddelerine göre yapılır.

4.6 Revizyonlar, "**Revizyon İstek Formu" (FR-003)** ile talep edilir ve revizyon isteğinde bulunan birim gerekçelerini belirtir. Ayrıca; talep edilen revizyon diğer birimleri ilgilendiriyor ise ilgili birimlerin görüşleri alınır, revizyon uygun görüldüğü taktirde Yönetim Temsilcisi tarafından "Doküman Hazırlama Onaylama Yetkisi"ne göre yayınlanır.

4.7 Kalite ve Bilgi Güvenliği El Kitabındaki değişiklikler sayfa bazında yapılır. Yapılan değişiklikler sayfasına; değişiklik nedeni, sayfa numarası, revizyon numarası, tarihi yazılır ve Şirket Müdürü

	Doküman no	Doküman no	PR-001
netsolutions	DOKÜMAN KONTROL PROSEDÜRÜ	İlk Yayın Tarihi	06.06.2011
		Revizyon no	0
		Revizyon tarihi	–
		Sayfa	4 / 4

tarafından onaylanır. Kalite ve Bilgi Güvenliği El kitabında değişen sayfanın revizyonu bir arttırılır. Kalite ve Bilgi Güvenliği El Kitabında revizyon sayısı 10 olduğunda El Kitabı'nın tamamı revizyon edilir.

4.8 El Kitabı dışında kalan dokümanlarda revizyon ihtiyacı olduğunda Madde-1 de tanımlanan yetkililer tarafından gözden geçirilir ve değişiklik kararı verildiğinde yine ilgililer tarafından onaylanır. Dokümanların tamamı revize edilir. Revizyon numarası bir artırılır. Prosedürlerde değişiklik sebebi prosedürün ön sayfasına yazılır.

5-DOKÜMAN KULLANIM SORUMLULUĞU

5.1 Birim Sorumluları birim çalışanlarına KYS VE BGYS dokümantasyonunun amaç ve kullanım şartları için gerekli bilgilendirmeyi yapar. Tüm çalışanlar KYS VE BGYS dokümantasyonuna göre davranış gösterirler ve dokümantasyon ile uygulama arasında faklılıkları birim sorumlusuna ve/veya yönetim temsilcisine bildirirler.

6. REFERANSLAR :

- TS –ISO 9001–2008 Standartları
- ISO / TR 10013.2001
- Kalite ve Bilgi Güvenliği Kayıtları Prosedürü
- Toplantı Prosedürü

7. KAYITLAR:

- Ana Doküman Listesi **(LS-001)**
- Doküman Dağıtım Formu **(FR-002)**
- Dış kaynaklı Doküman Listesi **(LS-002)**
- Doküman Revizyon İzleme Listesi **(LS-003)**
- Revizyon İstek Formu **(FR-003)**

Rev. No	Sayfa No	Değişiklik Sebebi	Onay	Tarih
Rev 0	Tümü	İlk Yayın	G.M.	**16.09.2010**

Şekil 3.3 Doküman Kontrol Prosedürü

Ürün / Hizmet Gerçekleştirme Planı: Kuruluşun verdiği hizmetin gerçekleştirilmesi için KYS ve BGYS kapsamında gerekli proseslerin planlanması ve ilgili faaliyetlerin yerine getirilmesi amacıyla hazırlanan plandır. Ürünün ve hizmetin kontrolü, doğrulanması için yapılması gereken ölçmeler, kabul kriterlerini, sorumluları ve tutulacak kayıtları gösterir. Kuruluşta KYS ve BGYS Kapsamında entegre olarak planlar hazırlanmıştır. Bunlar; Hizmet Gerçekleştirme Planı, Yıllık İç Tetkik Planı, Eğitim Planı, Girdi Kalite

Planı, Bakım Onarım Planları, Tasarım Planları, BGYS Planıdır. Bu planlarda talimatlara ve diğer destek dokümanlara atıf yapılır.

Talimatlar: Talimatlar uygulamaların detayını yani, işin nasıl yapılacağını anlatan dokümanlar olup, KYS ve BGYS kapsamında entegre olarak başlıca; kullanma ve bakım talimatları, hizmet talimatları, iş talimatları ve sistem talimatları hazırlanmıştır. Talimatlar çalışanlara yani işi yapan kişilere yönelik yazılmıştır.

Diğer Dokümanlar: KYS ve BGYS Kapsamında entegre olarak başlıca diğer dokümanlar: kalite ve Bilgi Güvenliği Yönetim Sistemi dokümantasyonu ve kayıtlarının tutulmasında kullanılan; listeler, formlar, raporlar, projeler, tablolar v.b. dokümanlardır.

Dış Kaynaklı Dokümanlar: Dış kaynaklı dokümanlar, kuruluş bünyesinde hazırlanmayan ancak kullanılan dokümanlardır. Bunlar; Standartlar, müşteri tarafından gönderilen dokümanlar, şartnameler (idari ve teknik) ve yasal mevzuatlardır.

Kuruluşta gerçekleştirilen tüm entegre sistem uygulamalarını gösteren kayıtlar, uygulamayı yapan tüm birimler tarafından sürekli ve düzenli olarak tutulmaktadır. Kayıtların kontrolü ile ilgili olarak Kayıtların Kontrolü Prosedürü hazırlanmış ve uygulanmaktadır. Hazırlanan bu prosedür; kayıtlarının tutulması, muhafazası ve saklanması sırasında hasara ve bozulmaya uğramaması için gerekli önlemleri, ihtiyaç duyulduğunda eski kayıtlara rahatlıkla ulaşılabilmesi için kayıtlarda ve arşivleme sırasında izlenebilirlik metotlarını, kayıtların saklama sürelerini ve yetkileri tanımlamaktadır. Kalite kayıtlarının saklanması kayıtları tutan birimde ve arşivde yapılmaktadır. Saklama süresi dolan kayıtların elden çıkartılması için yöntemler ve sorumluluklar belirlenmiştir.

Entegre olarak oluşturulan dokümantasyon yapısı bütün kuruluşların sistemlerin en büyük sorunu olan dokümantasyon yükü azaltılmış ve uygulaması kolaylaştırılmıştır.

Kuruluşun ihtiyaç duyduğu diğer dokümanlar tanımlanmış ve kurumda entegre dokümantasyon kültürü oluşturulmuştur. Böylece her bir doküman çok amaçlı olarak hazırlanmakta olup kâğıt tasarrufu sağlanmıştır.

Kuruluşta hazırlanan dokümanların listesi (Şekil 3.4) de verilmiştir.

	Doküman Adı	Doküman No	LS-001
netsolutions	ANA DÖKÜMAN LİSTESİ	Yayın Tarihi	06.06.2011
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	1/4

ADI	KODU	BASLANGIÇ TARİHİ	REV.NO	REV. TARIHI
KALITE EL KITABI	KE-001	06.06.2011		
KALITE POLITIKASI	KP-001	06.06.2011		
KALITE HEDEFLERI	KH-001	06.06.2011		
ORGANIZASYON ŞEMASI	OŞ-001	06.06.2011		
PROSESLER				
SATIŞ PROSESI	PS-001	06.06.2011		
SATIN ALMA PROSESI	PS-002	06.06.2011		
SÜREKLI IYILEŞTIRME PROSESI	PS-003	06.06.2011		
EGITIM PROSESI	PS-004	06.06.2011		
TEKNIK SERVIS	PS-005	06.06.2011		
TASARIM PROSESI	PS-006	06.06.2011		
AKIŞ ŞEMALARI				
SATIN ALMA AŞ	AŞ-001	06.06.2011		
SIPARIŞ AŞ	AŞ-002	06.06.2011		
TEKNIK SERVIS AŞ	AŞ-003	06.06.2011		
EGITIM AŞ	AŞ-004	06.06.2011		
SÜREKLI IYILEŞTIRME AŞ	AŞ-005	06.06.2011		
TASARIM AŞ	AŞ-006	06.06.2011		
GOREV TANIMLARI				
ŞIRKET MUDURU GT	GT-001	06.06.2011		
KALITE VE BILGI GUVENLIGI YONETIM TEMSILCISI GT	GT-002	06.06.2011		
SATIN ALMA SORUMLUSU GT	GT-003	06.06.2011		
SATIŞ SORUMLUSU GT	GT-004	06.06.2011		
TEKNIK SERVIS SORUMLUSU GT	GT-005	06.06.2011		
BURO ELEMANI GT	GT-006	06.06.2011		
YAZILIM PROJE MUDURU	GT-007	06.06.2011		
YAZILIM UZMANI GT	GT-008	06.06.2011		
NETWORK UZMANI GT	GT-009	06.06.2011		
PROSEDURLER				
DOKUMAN KONTROL PR	PR-001	06.06.2011		
KAYITLARIN KONTROLU PR	PR-002	06.06.2011		
IÇ TETKIK PR	PR-003	06.06.2011		
UYG. OLM. URUN/HIZ. KONT. PR	PR-004	06.06.2011		
DUZELTICI FAAL. PR	PR-005	06.06.2011		
ONLEYICI FAALIYET PR	PR-006	06.06.2011		
IÇ ILETIŞIM PR	PR-007	06.06.2011		
EGITIM PR	PR-008	06.06.2011		
VERI ANALIZI PR	PR-009	06.06.2011		
TEKNIK SERVIS PR	PR-010	06.06.2011		
SATIN ALMA PR	PR-011	06.06.2011		
SATIŞ PR	PR-012	06.06.2011		
TASARIM PR	PR-013	06.06.2011		
BGYS PLANLAMA PROSEDURU	PR-014	06.06.2011		
DISIPLIN PROSEDURU	PR-015	06.06.2011		
RISK DEGERLENDIRME YAKLAŞIMI PROSEDURU	PR-016	06.06.2011		
UYGULANABILIRLIK BILDIRGESI HAZIRLAMA PROSEDURU	PR-017	06.06.2011		
RISKLERI TANIMLAMA PROSEDURU	PR-018	06.06.2011		
RISKLERI ÇOZUMLEME VE DERECELENDIRME PROSEDURU	PR-019	06.06.2011		

ADI	KODU	BASLANGIÇ TARİHİ	REV.NO	REV. TARIHI
TALIMATLAR				
TEDARIKÇI DEGERLENDIRME TL	TL-001	06.06.2011		
GIRDI KABUL TL	TL-002	06.06.2011		
BILGISAYAR KAYITLARI YEDEKLEME TL	TL-003	06.06.2011		
CIHAZ BAKIM TL	TL-004	06.06.2011		
ACTIVE DIRECTORY KURULUM TALIMATI	TL-005	06.06.2011		
SERVER YEDEKLEME TALIMATI	TL-006	06.06.2011		
KULLANICI ARAYUZ TALIMATI	TL-007	06.06.2011		
DATABASE STANDARTLARI TALIMATI	TL-008	06.06.2011		
WINDOWS 2003 SERVER KURULUM TALIMATI	TL-009	06.06.2011		
PROJE TAKIBI VE KODLARIN YEDEKLENMESI TALIMATI	TL-010	06.06.2011		
BGYS'NIN GOZDEN GEÇIRILMESI TALIMATI	TL-011	06.06.2011		
ISTIHDAMIN SONLANDIRILMASI TALIMATI	TL-012	06.06.2011		
YENI BILGI IŞLEME TESISLERI IÇIN YETKILENDIRME TALIMATI	TL-013	06.06.2011		
BGYS IÇIN IŞ SUREKLILIGI TALIMATI	TL-014	06.06.2011		
AG KONTROLLERI TALIMATI	TL-015	06.06.2011		
BILGI ELDE TUTMA TALIMATI	TL-016	06.06.2011		
ORTAMIN ELDEN ÇIKARILMASI TALIMATI	TL-017	06.06.2011		
FORMLAR				
STANDART SAYFA FORMATI	FR-001	06.06.2011		
DOKUMAN DAGITIM FORMU	FR-002	06.06.2011		
REVIZYON ISTEK FORMU	FR-003	06.06.2011		
IÇ TETKIK RAPORU	FR-004	06.06.2011		
MUŞTERI ŞIKAYET FORMU	FR-005	06.06.2011		
DUZELTICI/ONLEYICI FAALIYET FORMU	FR-006	06.06.2011		
UYGUNSUZLUK BILDIRIM FORMU	FR-007	06.06.2011		
EGITIM ETKINLIGININ DEG. FORMU	FR-008	06.06.2011		
ORYANTASYON EGITIM FORMU	FR-009	06.06.2011		
PERSONEL EGITIM TAKIP FORMU	FR-010	06.06.2011		
EGITIM KATILIM FORMU	FR-011	06.06.2011		
EGITIM IHTIYAÇ BILDIRIM FORMU	FR-012	06.06.2011		
HIZMET IÇI EGITIM ANKET FORMU	FR-013	06.06.2011		
MAKINA BAKIM KARTI FR	FR-014	06.06.2011		
TOPLANTI TUTANAGI FR	FR-015	06.06.2011		
PROGRAM BAKIM ANLAŞMASI FR	FR-016	06.06.2011		
IÇ ILETIŞIM FORMU	FR-017	06.06.2011		
GIRDI KONTROL FORMU	FR-018	06.06.2011		
MALZEME TALEP FORMU	FR-019	06.06.2011		
SATIN ALMA SIPARIŞ FORMU	FR-020	06.06.2011		
TEDARIKÇI INCELEME FR	FR-021	06.06.2011		
IHALE GOZDEN GEÇIRME FORMU	FR-022	06.06.2011		
PERSONEL DEG. TAKIP ANKET FR	FR-023	06.06.2011		
IŞ BAŞVURU FORMU	FR-024	06.06.2011		
ARIZA BILDIRIM FR	FR-025	06.06.2011		
MUŞTERI GORUŞME FR	FR-026	06.06.2011		
MUŞTERI ANKET FR	FR-027	06.06.2011		
PROGRAM BUTUNLEŞIK TEST FR	FR-028	06.06.2011		
PROGRAM GERI BILDIRIM TEST FR	FR-029	06.06.2011		
PROGRAM ARAYUZ OZELLIKLERI FR	FR-030	06.06.2011		
PROGRAM ÇATISI VE MODUL TANIMLARI FR	FR-031	06.06.2011		
TASARIM GOZDEN GEÇIRME FR	FR-032	06.06.2011		

ADI	KODU	BASLANGIÇ TARİHİ	REV.NO	REV. TARIHI
SISTEM ANALIZ FR	FR-033	06.06.2011		
ARGE SONUÇ FR	FR-034	06.06.2011		
SERVER BAKIM CHECKLIST	FR-035	06.06.2011		
KURULUM CHECKLIST	FR-036	06.06.2011		
SVN YETKILENDIRME FORMU	FR-037	06.06.2011		
SORUMLULUK USTLENME BEYANI	FR-038	06.06.2011		
IP TESLIM ALMA TUTANAGI	FR-039	06.06.2011		
VARLIK TESLIM TUTANAGI	FR-040	06.06.2011		
ŞIFRELEME POLITIKASI VE ŞIFRE BILDIRIM FORMU	FR-041	06.06.2011		
YEDEK IMHA TUTANAGI	FR-042	06.06.2011		
SERVER DATA AKTARIM CHECKLIST	FR-043	06.06.2011		
OLAY IHLAL FORMU	FR-044	06.06.2011		
ZAAFIYET TESPIT FORMU	FR-045	06.06.2011		
IHLAL OLAYI SONUÇ RAPORU FORMU	FR-046	06.06.2011		
BILGI SAKLAMA BEYANI FORMU	FR-047	06.06.2011		
YONETIMIN BILGI GUVENLIGI YONETIMI SISTEMINE BAGLILIK BEYANI FORMU	FR-048	06.06.2011		
BILGI GUVENLIGI SORUMLULUKLARININ TAHSISI FORMU	FR-049	06.06.2011		
SUNUCU ODASINA GIRIŞ FORMU	FR-050	06.06.2011		
AG KONTROLLERI CHECKLIST FORMU	FR-051	06.06.2011		
BINA TESLIM TUTANAGI FORMU	FR-052	06.06.2011		
TAŞINABILIR ORTAM YONETIMI POLITIKASI VE FORMU	FR-053	06.06.2011		
BINA TURU FORMU	FR-054	06.06.2011		
RISKI OLAN FAALIYETLER FORMU	FR-055	06.06.2011		
IP MAC ADRES FORMU	FR-056	06.06.2011		
YEDEK ALMA CHECKLIST	FR-057	06.06.2011		
SUNULAN ARTIK RISKLERE ILIŞKIN YONETIM ONAYI EDINME BEYANI FORMU	FR-058	06.06.2011		
BGYS IŞLETME BIRIMI IÇIN YETKI BEYANI FORMU	FR-059	06.06.2011		
PLANLAR				
HIZMET GERÇEKLEŞTIRME PL	PL-001	06.06.2011		
YILLIK IÇ TETKIK PL	PL-002	06.06.2011		
GIRDI KALITE PL	PL-003	06.06.2011		
YILLIK EGITIM PL	PL-004	06.06.2011		
TEÇHIZAT BAKIM PL	PL-005	06.06.2011		
MUŞTERI GORUŞME PL	PL-006	06.06.2011		
TASARIM GELIŞTIRME PL	PL-007	06.06.2011		
TASARIM IŞ ZAMANI PL	PL-008	06.06.2011		
PERIYODIK BAKIM ÇIZELGESI	PL-009	06.06.2011		
BGYS PLANI	PL-010	06.06.2011		
KAPASITE PLANI	PL-011	06.06.2011		
LISTELER				
ANA DOKUMAN LISTESI	LS-001	06.06.2011		
DIŞ KAYNAKLI DOK. TAKIP LISTESI	LS-002	06.06.2011		
DOKUMAN REV. IZLEME LISTESI	LS-003	06.06.2011		
ONAYLI TEDARIKÇI LISTESI	LS-004	06.06.2011		
IÇ TETKIK SORU LISTESI	LS-005	06.06.2011		
DUZELTICI FAALIYET LISTESI	LS-006	06.06.2011		
UYGUNSUZLUK TAKIP LISTESI	LS-007	06.06.2011		
ONLEYICI FAALIYET LISTESI	LS-008	06.06.2011		

netsolutions	Doküman Adı	Doküman No	LS-001
	ANA DÖKÜMAN LİSTESİ	Yayın Tarihi	06.06.2011
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	4/4

ADI	KODU	BASLANGIÇ TARİHİ	REV.NO	REV. TARIHI
PROSES HEDEF IZLEME TABLOSU	LS-009	06.06.2011		
MUŞTERI ŞIKAYET TAKIP LISTESI	LS-010	06.06.2011		
TEDARIKÇI SORU LISTESI	LS-011	06.06.2011		
TEDARIKÇI PERF. IZLEME LS	LS-012	06.06.2011		
KAYITLAR LISTESI	LS-013	06.06.2011		
POLITIKALAR				
BGYS IÇIN IŞ SUREKLILIGI POLITIKASI	PLK-001	06.06.2011		
BILGI GÜVENLIGI YÖNETIM SISTEMI POLITIKASI	PLK-002	06.06.2011		
E-POSTA POLITIKASI	PLK-003	06.06.2011		
ERIŞIM POLITIKASI	PLK-004	06.06.2011		
GENEL INTERNET ERIŞIM POLITIKASI	PLK-005	06.06.2011		
MOBIL BILGI IŞLEME ve UZAKTAN ÇALIŞMA POLITIKASI	PLK-006	06.06.2011		
SINIFLANDIRMA VE ETIKETLEME POLITIKASI	PLK-007	06.06.2011		
TEMIZ MASA TEMIZ EKRAN POLITIKASI	PLK-008	06.06.2011		
ŞEMALAR				
AG TOPOLOJISI ŞEMASI	Ş-001	06.06.2011		
BINA ŞEMASI	Ş-002	06.06.2011		

Şekil 3.4 Doküman Ana Listesi

3.2.3. Yönetim Sorumluluğu Süreci

Kuruluş üst yönetimi, KYS ve BGYS sistemlerinin uygulanması, geliştirilmesi ve etkinliğinin sürekli iyileştirilmesi, müşteri ihtiyaç ve beklentilerinin alınması ve karşılanması için gerekli yöntemleri belirlemiş olup, uygulanmasını sağlamaktadır. Bu kapsamda yönetim gerekli kaynakları oluşturmuş ve uygulanmaktadır. Yönetimin taahhüdü içerisine aşağıdakiler yapılmıştır;

- Kuruluşu ilgilendiren yasal şartları ve müşteri şartlarının yerine getirilmesi ve bu şartların güncelliğinin takibi,

-Kalite ve bilgi güvenliği politikasının oluşturulması; kalite ve bilgi güvenliği politikası yönetim tarafından yazılı olarak tespit edilmiş ve üst yönetim tarafından imzalanarak yayınlanmıştır.

-Kuruluş, kalitenin müşteri odaklı olduğunun bilincinde olup, tüm çalışanlar bu anlayışla uygulamaları sağlar. Çalışanlarımızın kalite bilincinin geliştirilmesi amacıyla planlı, programlı olarak iç ve dış eğitimler düzenlenmektedir. Bu eğitimlerde çalışanlara kalite uygulamaları, standart uygulamaları ile kuruluş kültürü vb. konularda bilgilendirilmeleri sağlanmaktadır.

-Kalite ve bilgi güvenliği hedefleri; kuruluşun yapısı ve organizasyonuna uygun şekilde kurulan kalite ve bilgi güvenliği sisteminde hedeflerle yönetim ve verilere dayalı

karar verme yönetim ilkeleri benimsenmiş olup, kalite ve bilgi güvenliği hedefleri her yıl periyodik aralıklarla yapılan toplantılarda yazılı olarak tespit edilmektedir. Bu hedefler prosesler, ürünler, kalite ve bilgi güvenliği sistemi uygulamaları olarak birimler bazında oluşturulmaktadır. Kalite ve bilgi güvenliği hedeflerine ulaşılabilmesi için gerekli olan faaliyetler ve stratejiler tespit edilerek uygulanmaktadır. Kalite ve bilgi güvenliği hedefleri ilgili birimler ve yönetim tarafından belli aralıklarla değerlendirilmekte, hedeflerin gerçekleşmesi takip edilmektedir.

-Görev yetki ve sorunlulukların tayini; Kuruluş kalite ve bilgi güvenliği etkileyen işleri yöneten, uygulayan ve doğrulayan tüm çalışanların görev, yetki sorumluluklar ve karşılıklı ilişkilerinin, kime bağlı çalıştığının ve kime vekalet edeceğinin yazılı olduğu görev tanımları hazırlanmıştır. Görev tanımları organizasyon şemasında yer alan ve kaliteyi etkileyen tüm personel için hazırlanmış ve ilgili personelin bilgisine sunulmuştur. Görev tanımlarındaki kişiler bulunmadığında yerine kimin bakacağı vekalet sistemi ile belirlenmiştir.

-Yönetim Temsilci; KYS ve BGYS kuruluşta kurulması uygulaması ve etkinliğinin sürekli iyileştirilmesinden sorumlu olan personel, Yönetim Temsilcisi olarak şirket müdürü tarafından atanmıştır. Kalite ve bilgi güvenliği sistemin kurulması uygulanması devam ettirilmesi ve sürekli iyileştirilmesinden sorumludur. Yönetimin gözden geçirme toplantılarını organize eder

3.2.4. Kaynak Yönetim Süreci

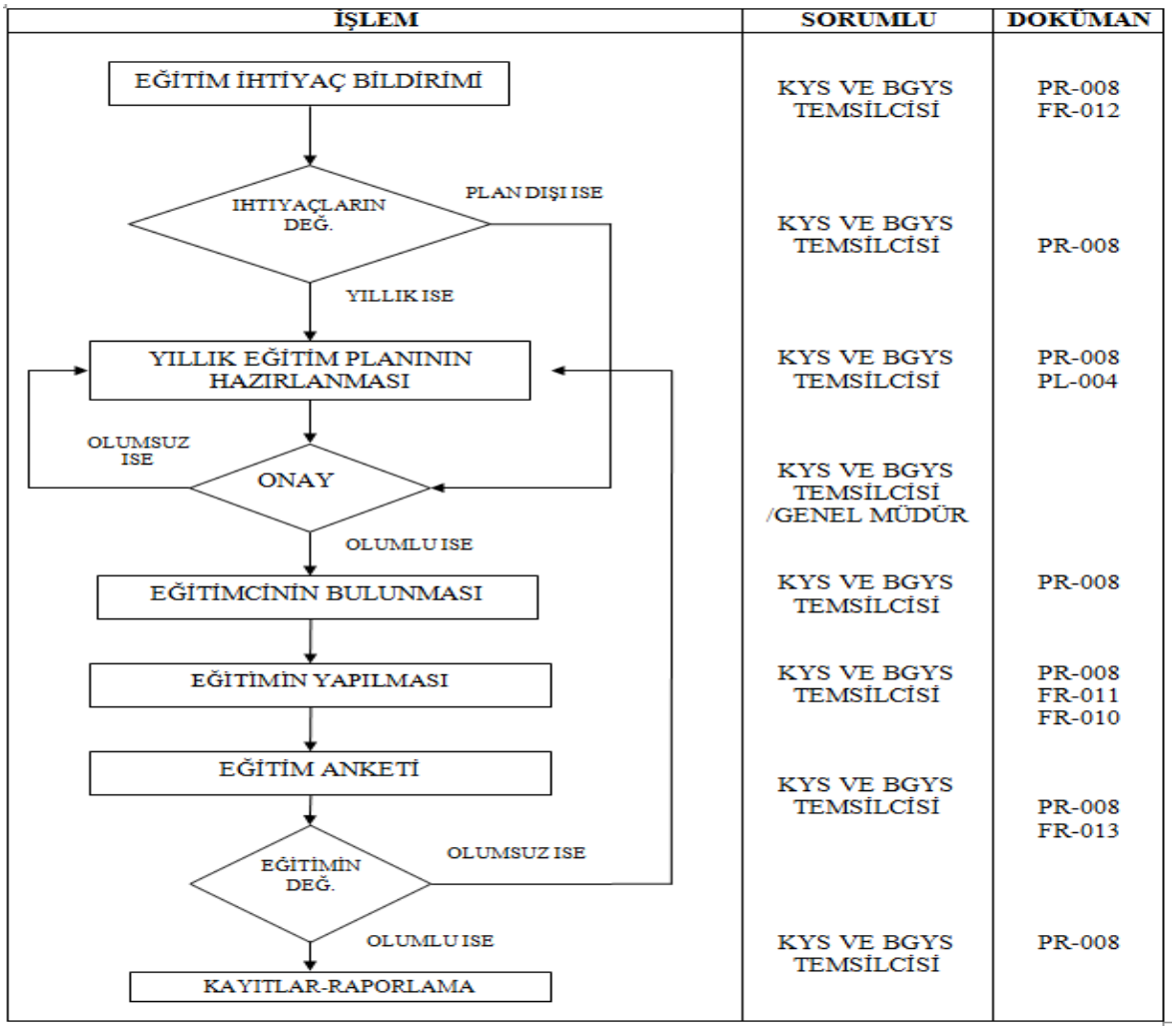
Kuruluş üst yönetimi KYS ve BGYS Yönetim Sistemi'ni uygulamak, devam ettirmek, sürekli geliştirmek için gerekli olan kaynakları sağlamaktadır. Yönetimin gözden geçirme toplantılarında her iki sisteminde ortak kaynak ihtiyaçları belirlenmektedir. Gerçekleştirilen tüm kontrollerin doğru uygulanmasıyla ürün ve hizmetin güvenliği sürdürmek için gerekli olan altyapıyı insan kaynakları, altyapı ve çalışma koşulları her iki sistem için entegre olarak gerçekleştirilmektedir. Bu sayede her sistem için ayrı bir kaynak tahsisine gerek kalmamıştır.

KYS ile BGYS sistemini entegre olarak tasarlamanın kaynaklardan önemli ölçüde tasarruf sağladığı, ayrıca mevcut sistemi geliştirdiği görülmüştür[29].

Kuruluşta ihtiyaç duyulduğunda kalifiyeli personele yönelik istihdamlar yapılmaktadır. Personelin unvanları göz önünde bulundurularak sahip olması gereken

eğitim, öğretim, tecrübe ve diğer nitelikleri tespit edilmiştir. Personel alımlarında bu nitelikler dikkate alınmaktadır. İşe yeni başlayan personele KYS ve BGYS Sistemi kapsamında uyum eğitimi olarak tanımlanan eğitim faaliyetleri uygulanır.

KYS ve BGYS sistemi kapsamında eğitim ihtiyaçları, Yönetim Temsilcisi tarafından tüm birimlerden gelen talepler doğrultusunda tespit edilir. Planda kuruluş içerisinde ve kuruluş dışında alınacak eğitimler saptanır. Eğitim programının duyurulması, takibi ve kayıtlarının düzenli olarak tutulması kalite ve bilgi güvenliği Yönetimi Temsilcisi tarafından yapılır. Böylece eğitim talepleri ve planlaması ve yürütülmesi tek elden entegre olarak yapılması sağlanmıştır. Eğitim prosesi akışı Şekil 3.5 deki gibi yapılmış ve uygulanmıştır.



Şekil 3.5 KYS ve BGYS Eğitim Prosesi Akış Şeması

3.2.5. Tetkik Süreci

Kuruluşun KYS ve BGYS'nin planlanan düzenlemelere uygunluğunun, yeterliliğinin, etkinliğinin ve devamlılığının sağlanması, eksiklerin ve uygunsuzlukların tespit edilerek giderilmesi ve sistemin hedeflere ulaşmada yeterli olup olmadığının takibi için her iki sistemin ayrı ayrı olan iç tetkik prosedürleri birleştirilmiş ve tek bir İç Tetkik Prosedürü (Şekil 3.6) oluşturulmuştur. Bu prosedür kapsamında Yönetim Temsilcisi tarafından hazırlanan ve her iki sistemin iç tetkikini kapsan bir yıllık iç tetkik planı oluşturulmuştur.

İç tetkikler, hazırlık, planlama, uygulama ve değerlendirme aşamalarını içerecek şekilde dokümante edilmiştir. Yapılan bu iç tetkikler; kalite ve bilgi güvenliği sisteminin geliştirilmesi, sisteminin uygunluk ve etkinliğinin tespiti, hedeflere ulaşılması, uygunsuzlukların azaltılması, ortadan kaldırılması ve önlenmesi için faydalanılan bir proses olarak değerlendirilir. İç tetkikler sonunda hazırlanan raporlar yönetimin gözden geçirme toplantılarında görüşülür ve değerlendirilir.

Firma Logosu	Doküman Adı	Doküman no	PR-003
	İÇ TETKİK PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	0
		Revizyon tarihi	--
		Sayfa no	1 / 2

1.AMAÇ:

Kalite ve Bilgi Güvenliği Yönetim Sistemlerinin planlanmış düzenlemelere ve KYS ve BGYS standart şartlarına uyup uymadığını ve etkin olarak uygulanıp uygulanmadığını ve sürekliliğinin sağlanıp sağlanmadığını planlı aralıklarla tespit etmek.

2.KAPSAM

Kalite ve Bilgi Güvenliği Yönetim Sistemlerindeki tüm fonksiyon ve prosesleri kapsar

3.SORUMLULAR:

- Şirket Müdürü
- Kalite ve Bilgi Güveliği Yönetim Temsilcisi
- Birim Sorumluları
- İç tetkikçiler

4.TANIMLAR

5.PROSEDÜR:

1) Yıllık iç tetkik planları Kalite ve Bilgi Güveliği Yönetim Temsilcisi tarafından kalite hedeflerine ulaşma seviyelerine, uygun olmayan ürün miktarına, müşteri şikayetlerine, iç ve dış tetkik sonuçlarına göre ilgili birim veya prosesteki tetkiklerin adedi, süresi ve tetkikçi özellikleri dikkate alınarak planlanır. (Yılda en az bir defa tüm birim ve proseslerde tetkik gerçekleştirilir). Yıllık plan Şirket Müdürünün onayından sonra Kalite ve Bilgi Güveliği Yönetim Temsilcisi tarafından tetkikten 15 gün önce tetkik edilecek birim sorumlularına ve tetkikçilere dağıtılır.

2) Tetkikler, KYS ve BGYS dokümanları, TS ISO 9001, TS ISO/IEC 27001 ve TS En ISO 19011 Standartları, kalite ve Bilgi Güvenliği politikaları ve hedefler göz önüne alınarak gerçekleştirilir.

3)Tetkikçiler tetkik yapabilme yeteneğine sahip (eğitilmiş personel) olan personel tarafından gerçekleştirilir. Tetkikçiler sorumlu olduğu ve veya ardışık proseslerde yer alanlardan (çıkar çatışması olabilecek) seçilmez.

4) Tetkiklerde önceden hazırlanan tetkik soru listesi (LS-005) kullanılır (tetkikin şartlarına göre ilave sorular sorabilir).

5) Tetkik edilecek birimler ve tetkikçiler acil durumlarda programdan sapmaları halinde 7 gün öncesinden Kalite ve Bilgi Güveliği Yönetim Temsilcisine bildirmelidirler.

6) Tetkikçiler tetkike hazırlık olarak ilgili KYS ve BGYS dokümanlarını (bir önceki iç ve dış tetkike ait kayıtlar dahil) inceleyerek hazırlık yaparlar. Tetkikçiler sözlü veya yazılı iletişim metoduyla kesin tetkik programını gün ve/veya saat olarak belirlerler.

7) Her tetkikten önce soru listeleri güncellenir. Tetkik edilecek birim sorumlusu kendi birimini ve çalışanlarını tetkikten haberdar ederek tetkikin en verimli olarak yapılması için gerekli hazırlıkları yapmakla sorumludur.

8)Tetkikçiler tetkik programına uygun olarak tetkik yapılacak bölümde tetkiki gerçekleştirir. Gerektiğinde rehber kullanabilir. Tetkik sonucunda tetkikçiler bulgularını değerlendirir ve söz konusu bulguları ilgili birimlerle paylaştıktan sonra tetkik raporuna kaydeder.

9) Tetkik sırasında uygunsuzluk tespit edildiğinde düzeltici faaliyet talebinde bulunur. Düzeltici faaliyet raporunda uygunsuzluğu objektif delillerle belirler ve birim sorumlularıyla yapılacak

Firma Logosu	Doküman Adı	Doküman no	PR-003
	İÇ TETKİK PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	0
		Revizyon tarihi	–
		Sayfa no	2 / 2

düzenleyici faaliyetler belirlenir ve gereksiz gecikmelerden kaçınılarak bitiş tarihi tespit edilir. Birim sorumlusu belirlenen uygunsuzlukların süratli şekilde giderilmesinden sorumludur. Tetkikçi süresi sonunda uygunsuzluğun giderip giderilmediği kontrol edilir giderilmişse kapatılır, giderilmemişse sebepleriyle beraber Kalite ve Bilgi Güveliği Yönetim Temsilcisi bilgilendirir.

10) Tetkik sonrasında iki suret olarak hazırlanan tetkik raporunun bir sureti birimde muhafaza edilirken diğer sureti Kalite ve Bilgi Güveliği Yönetim Temsilcisine teslim edilir. Kalite ve Bilgi Güveliği Yönetim Temsilcisi tetkikte açılan düzeltici faaliyet listesini kayıt eder. Kayıtlar kalite kayıtları prosedürüne göre muhafaza edilir.

11) Kalite ve Bilgi Güveliği Yönetim Temsilcisi tetkiklerle ilgili değerlendirme raporunu üst yönetime ve yönetimin gözden geçirme toplantısına sunar.

REFERANSLAR:
TS-ISO 9001:2008

KAYITLAR

- Yıllık İç Tetkik Planı **(PL-002)**
- İç Tetkik Raporu **(FR-004)**
- Düzeltici/Önleyici Faaliyet İstek Formu **(FR-005)**
- İç Tetkik Soru Listesi **(LS-005)**

Rev. No	Sayfa No	Değişiklik Sebebi	Onay	Tarih
Rev 0	Tümü	İlk Yayın	G.M.	16.09.2010

Şekil 3.6 İç Tetkik Prosedürü

3.2.6. Yönetimin Gözden Geçirmesi Süreci

Kuruluşta KYS ve BGYS'nin değerlendirilmesi için yönetimin gözden geçirmesi toplantısı yapılır. KYS ve BGYS gözden geçirme faaliyetleri hazırlanan entegre yönetimin gözden geçirmesi talimatlarıyla dokümante edilmiştir.

Yönetim Temsilcisi KYS ve BGYS yönetimi gözden geçirme gündemini belirler. Yönetimin Gözden Geçirme Prosedürü paralelinde toplantıları organize eder, toplantı raporlarını hazırlar, tutanakları katılımcılara dağıtır, alınan kararların takibini yapar, kalite ve bilgi güvenliği sistemiyle ilgili üst yönetime, belirlenen periyotlarda rapor sunar ve dış kuruluşlarla iletişimi sağlar.

Yönetim Temsilcisi; toplantının gündemi, görüşülecek konuların tespiti, alınan kararların kayıtlarının tutulması ve ilgili birimlere duyurulması gibi konulardan sorumludur. Ayrıca alınan kararların takibi, koordinasyonu ve kontrolünü de üstlenmiştir.

KYS ve BGYS için yönetimin gözden geçirme toplantılarının girdisi aşağıdaki gibi oluşturulmuştur.

-KYS ve BGYS Tetkiklerin sonuçları,

-Müşteri (ilgili taraflardan edinilen) geri beslemeleri,

-Önceki yönetim gözden geçirmesine ait takip faaliyetleri,

-Proses performansı ve ürün uygunluğu,

-Önleyici, düzeltici ve uygunsuzluk(BGYS İhlalleri) faaliyetlerin durumu,

-Kalite ve Bilgi Güvenliği Yönetim Sistemi'ni etkileyebilecek değişiklikler,

-İyileştirme için öneriler.

Böylece her iki yönetim Sistemi için tek bir yönetimin gözden geçirme toplantısı yapılarak standardın şartları sağlanmış ve kuruluş gereksiz maliyetlerden kurtarılmıştır.

Toplantıda alınan kararlar her iki Sistemin birlikte yürütülmesi yönünde olmuştur

3.2.7. İyileştirme Süreci

Kuruluş KYS ve BGYS yönetim sistemleri için gerekli olan izleme, ölçme, analiz ve iyileştirme prosesleri ortak olarak planlamıştır. Kalite ve bilgi güvenliği sistemlerinin uygunluğunu sağlamak ve bu sistemlerin etkinliğini sürekli iyileştirmek istatistiksel ve yönetimsel metotlar kullanılmıştır.

Sürekli iyileştirme kapsamında; Ölçme, izleme ve verilerin analizi ile iyileşme sağlamak için tutulan veriler kullanılır.

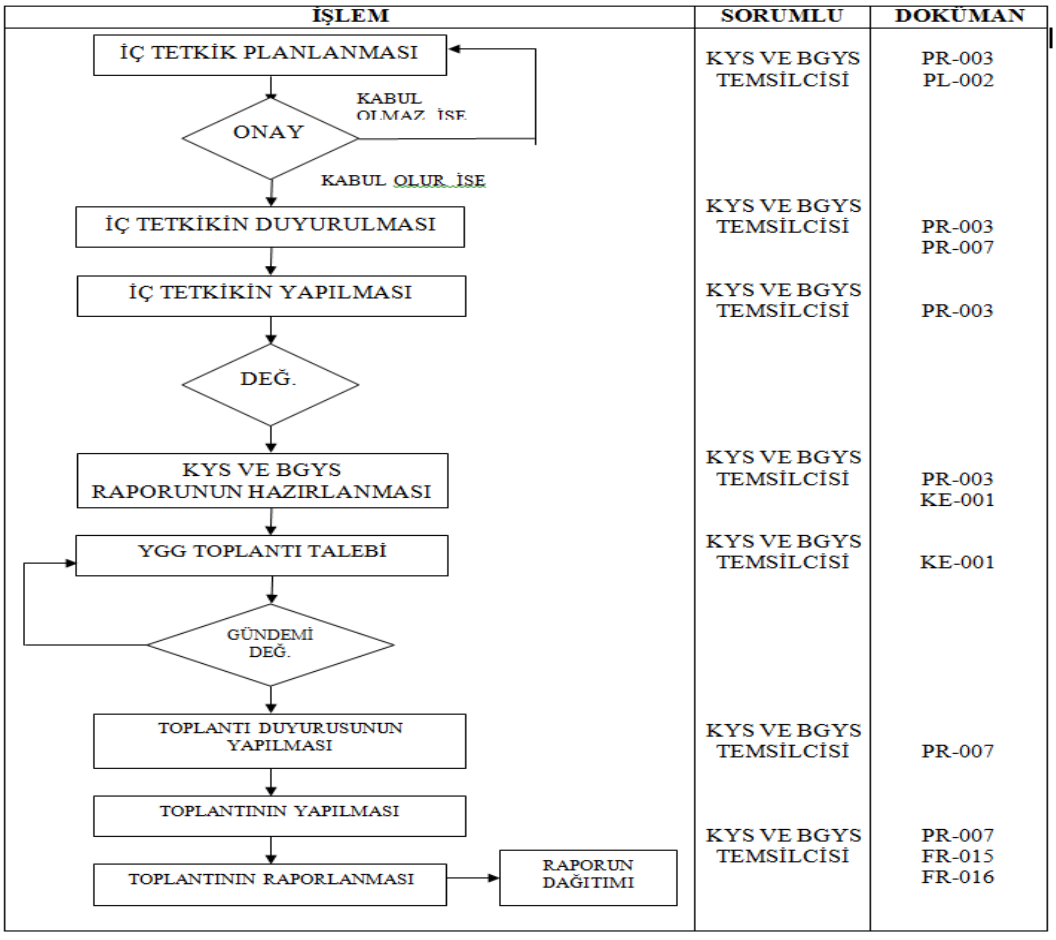
Ölçme analiz ve iyileştirme prosesi tablosu aşağıdaki gibi oluşturulmuştur.

Tablo 3.1 Ölçme Analiz ve İyileştirme Prosesi Tablosu

Proses Sorumlusu	Kalite ve Bilgi Güvenliği Yönetim Temsilcisi
Proses Girdileri	Kalite ve Bilgi Güvenliği Tetkikleri, Düzeltici ve Önleyici Faaliyet, Eğitim Değerlendirme Sonuçları, Veri Analizi, Uygun Olmayan Ürün Raporları, Bilgi Güvenliği İhlal Olayları, Müşteri Geri Beslemesi, Proses/Ürün Uygunluğu, Kalite ve Bilgi Güvenliği Politikaları/Hedefleri, Yön. Tem. Performans Raporu, Önceki YGG Kararları

Proses Çıktıları	Kalite ve Bilgi Güvenliği Politikası, Kalite ve Bilgi Güvenliği Hedefleri, Önleyici Faaliyet, Tanımlanmış Kaynaklar
Proses Faaliyetleri	Akış Şeması
Proses Kaynakları	Toplantı Salonu, Sunu araç gereçleri
Proses Dokümantasyonu	YGG Toplantı tutanağı
İzleme Ölçme	Yazışma ve rapordaki hatasızlık oranları
Performans Kriteri	Zamanında yapılmış olması, Beklenen katılımın gerçekleşmesi, KYS ve BGYS' ye ait verilerin mevcudiyeti ve anlaşılabilirliği, Önleyici faaliyet sayısı, Proses hedeflerinin gerçekleşme oranı ve bir önceki döneme göre KYS ve BGYS'nin iyileşme yüzdesi
Proses Etkileşimi	Kalite ve Bilgi Güvenliği Yönetim Sistemi kapsamındaki tüm proseslerle etkileşimdedir.

Sürekli İyileştirme Prosesi Akış Şeması (Şekil 3.7) oluşturulmuştur.



Şekil 3.7 Sürekli İyileştirme Prosesi Akış Şeması

3.2.7.1. Düzeltici Faaliyet

Kuruluşta meydana gelen bir uygunsuzluğu gidermek ve sebep sonuç analizleri kullanarak uygunsuzluğun kök sebebini araştırmak için KYS ve BGYS kapsamında Düzeltici Faaliyet Prosedürü (Şekil 3.8) oluşturulmuştur. Böylece Yönetim Temsilcisi tarafından her iki sistemin zorunlu şartı olan düzeltici faaliyet prosesini entegre olarak uygulamaktadır. Öncelikle düzeltici faaliyet gerektiren uygunsuzluklar belirlenir ve gerekli işlemlere ilgili prosedüre göre başlanır.

Uygunsuzlukların sebebinin araştırılması ve gerekli düzeltici faaliyetlerin başlatılması, iş ve hizmet performansının ölçülmesinde ve değerlendirilmesinde istatistik teknikler kullanılmaktadır.

Burada amaç, uygunsuzlukların analiz edilmesi, değerlendirilmesi, sebeplerinin ortaya çıkartılması, dönemler halinde raporlar oluşturulması ve ilgililerin dikkatine sunularak tekrar olmasının önlenmesidir. Düzeltici faaliyetlerle ilgili yapılan çalışmaların kayıtları tutulması için düzeltici faaliyet kayıt formları oluşturulmuş ve muhafaza edilmekte ve yönetime sunulmaktadır. Düzeltici faaliyetlerin planlanması ve uygulanması için Düzeltici Faaliyet Prosedürü aşağıdaki gibi oluşturulmuştur.

	Doküman Adı	Doküman no	PR-005
netsolutions	DÜZELTİCİ FAALİYET PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	00
		Revizyon tarihi	-
		Sayfa no	1 / 2

1.AMAÇ:

Uygunsuzlukların gözden geçirilerek nedenlerinin belirlenmesi ve tekrarını önlemek için yapılacak düzeltici faaliyetlerin belirlenmesi, uygulanması, kaydedilmesi sonuçlarının değerlendirilmesi.

2.KAPSAM

KYS VE BGYS Sistemindeki tüm faaliyetleri kapsar

3.SORUMLULUKLAR:

1- Şirket Müdürü
2- Kalite ve Bilgi Güvenliği Yönetim Temsilcisi
3- Birim Sorumluları

4.TANIMLAR

Düzeltici Faaliyet: Saptanan bir uygunsuzluğun sebebini veya diğer bir istenmeyen durumu yok etmek için yapılan faaliyet.

Düzeltme: Saptanan uygunsuzluğu gidermek için yapılan faaliyet.

5.PROSEDÜR:

1. Uygunsuzlukların tekrarlarını engellemek için aşağıdaki faaliyet ve veri kaynakları gözden geçirilerek, gerçekleştirilecek düzeltici faaliyetler belirlenir.

   - Müşteri şikayetleri pazarlama-Satış sorumlusunun koordinasyonunda şikayet konusu proses sorumlusuyla beraber,
   - Ürün ve üretim prosesleriyle ilgili uygunsuzluklar birim sorumluları koordinasyonunda,
   - Yönetim sistemiyle ilgili uygunsuzluklar Kalite ve Bilgi Güvenliği yönetim temsilcisinin koordinasyonunda,
   - Satın alma ile ilgili uygunsuzluklar satın alma sorumlusunun koordinasyonunda ilgili birim sorumlularıyla beraber değerlendirilmeye alınır.

2. Uygunsuzlukların nedenleri işçilik, dokümantasyon, proses akışları, eğitim yetersizliği, geçmiş deneyimler, proses hedefleri, ürün şartları baz alınarak değerlendirilir. Bu değerlendirmelerde gerektiğinde geçmiş kayıtların kontrolü, mevcut dokümanların kontrolü, birebir görüşmeler, toplantılar ve yine gerektiğinde temel istatistiksel teknikler kullanılarak araştırılır.

3. Uygunsuzluğun tekrarlanmaması için proses değişikliği, personel eğitimi, kaynak ihtiyacı (yetersiz yardımcı malzeme), dokümantasyon iyileştirme şeklinde faaliyetlerden biri veya birkaçı belirlenir ve uygulamaya konur.

4. Uygunsuzluk konusu ile ilgili birim sorumlusu ‘’**Düzeltici/Önleyici Faaliyet İstek Formu’’ (FR-005)** doldurur. Kalite ve Bilgi Güvenliği Yönetim temsilcisini bilgilendirir ve Düzeltici faaliyet no’ sunu alır. Uygunsuzluk kendi birim sorumluluğu kapsamında giderilebiliyorsa birim sorumlusu tarafından uygunsuzluğun tanımı, yapılan ve yapılacak faaliyetlerin sonuçları düzeltici önleyici faaliyet formuna yazılır ve kapanan formun bir nüshası Kalite ve Bilgi Güvenliği Yön. Tem. verilir.

5. Uygunsuzluk başka bir proses sorumluluğunda ise Düzeltici ve Önleyici Faaliyet İstek Formu doldurularak Kalite ve Bilgi Güvenliği Yön. Tem. gönderilir. Kalite ve Bilgi Güvenliği Yön. Tem. Uygunsuzluğun giderilmesi için düzeltici faaliyeti tamamlamak üzere ilgili birime gönderir.

	Doküman Adı	Doküman no	PR-005
netsolutions	DÜZELTİCİ FAALİYET PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	00
		Revizyon tarihi	-
		Sayfa no	2 / 2

6. Düzeltici faaliyet ihtiyacı tespit edilen birim sorumluları gecikmelere sebep vermeden düzeltici faaliyeti sonuçlandırmak ve uygulamaya konulan kararların etkinliğini takip etmekten sorumludur.

7. Düzeltici faaliyetlerle ilgili kayıtların bir sureti ilgili birimde diğer sureti Kalite ve Bilgi Güvenliği Yön. Tem. de kayıtların kontrolü prosedürüne göre saklanır.

8. Kalite ve Bilgi Güvenliği Yön. Tem. tüm düzeltici faaliyetleri **"Düzeltici/Önleyici Faaliyet İzleme Listesi" (LS-005)** aracılığıyla takip eder.

9. Düzeltici faaliyetlere ait değerlendirme Yönetim Temsilcisi tarafından yapılır ve hazırlanan rapor "Yönetimin Gözden Geçirme" Toplantısında görüşülür.

6. REFERANSLAR:
TS –ISO 9001–2008 KYS
TS-ISO/IEC 27001 BGYS

7. KAYITLAR:
- Düzeltici/Önleyici Faaliyet İstek Formu **(FR-005)**
- Düzeltici Faaliyet İzleme Listesi **(LS-006)**

Rev. No	Sayfa No	Değişiklik Sebebi	Onay	Tarih
Rev 0	Tümü	İlk Yayın	G.M	16.09.2010

Şekil 3.8 Düzeltici Faaliyet Prosedürü

3.2.7.1. Önleyici Faaliyet

Kuruluş; Potansiyel bir uygunsuzluğun sebebinin veya diğer istenmeyen durumların bertaraf edilmesi için yapılan faaliyetlerde önlemeye yönelik olarak Önleyici Faaliyet Prosedürü (Şekil 3.9) hazırlanmış ve uygulanmaktadır.

Önleyici faaliyetlerle ilgili yapılması gerekli faaliyetler ilgili prosedürde belirlenmiştir. Değişen ve gelişen koşullarda sürekli iyileşmeyi prensip edinen kuruluş önleyici faaliyetler konusunda bilgili personelden yararlanır ve tüm faaliyetler Önleyici Faaliyet Prosedürü (Şekil 3.9) kapsamında gerçekleştirilir.

.

	Doküman Adı	Doküman no	PR-006
netsolutions	ÖNLEYİCİ FAALİYET PROSEDÜRÜ	İlk yayın tarihi	06.06.2011
		Revizyon no	0
		Revizyon tarihi	–
		Sayfa no	1 /1

1. AMAÇ:

Potansiyel uygunsuzluk risklerini değerlendirerek sebeplerini ortadan kaldıracak uygulamaları belirlemek, uygulamaya koymak, sonuçlarını doğrulamak ve kayıtlarını tutmak.

2. KAPSAM:

KYS VE BGYS Sistemindeki tüm faaliyetleri kapsar

3. SORUMLULAR:

1- Şirket Müdürü
2- Kalite ve Bilgi Güvenliği Yönetim Temsilcisi
3- Birim Sorumluları

4. TANIMLAR:

5. PROSEDÜR:

Potansiyel riskler kalite ve bilgi güvenliği yönetim sistemi kalite ve bilgi güvenliği politikası, kalite ve bilgi güvenliği hedefleri, üretim (ürün ve proses) performans raporları, müşteri şikayetleri, iç ve dış tetkikler, yönetimin gözden geçirme toplantıları çıktıları, teknolojik gelişmeler, pazardaki değişiklikler vb. kaynaklardan elde edilen veri analizi ile tespit edilir.

Tespit edilen risklerin boyutu üst yönetimin katıldığı değerlendirme toplantılarında, kıyaslama çalışmalarıyla ve istatistiksel teknikler kullanılarak değerlendirilir.

Değerlendirme sonucunda potansiyel uygunsuzluğu ortadan kaldırmaya yönelik yapılacak faaliyetler; alt yapı ve çalışma ortamı iyileştirme, personel yeterliliğinin artırılması, proses değişikliklerinden bir veya birkaçı şeklinde olur.

Önleyici faaliyet talepleri birim sorumluları, birim müdürleri tarafından teklif edilir. Teklif sahibi potansiyel uygunsuzluğun risk değerlendirmesini ve alınacak önlemler ile ilgili görüşlerini belirterek KYS ve BGYS Yönetim Temsilcisi. aracılığıyla Şirket Müdürü'ne sunulur.

Söz konusu önleyici faaliyet en az teklif sahibi, KYS ve BGYS Yönetim Temsilcisi. ve Şirket Müdürünün yer aldığı toplantıda değerlendirilir. İhtiyaç halinde diğer birim sorumluları da toplantıya katılabilir.

Değerlendirmede yapılacak önleyici faaliyet tespit edilir ve tespit konusu en az şu maddeleri içerir; yapılacak işin adı, kaynak ihtiyacı, yetkilisi ve bitiş süresi.

Faaliyetlerin kayıtları ve takibi KYS ve BGYS Yönetim Temsilcisi. tarafından yapılır. Karar verilen önleyici faaliyet metodu uygulamaya konur. Uygulamanın özelliğine göre 1-3-6 ay gibi sürede etkinliği değerlendirmeye alınır.

6. REFERANSLAR:

- TS ISO 9001:2008
- TS ISO/IEC 27001:2005 Standartları

7. KAYITLAR:

- Düzeltici/Önleyici Faaliyet İstek Formu **(FR-005)**
- Önleyici Faaliyet İzleme Listesi **(LS-008)**

Rev.No	Sayf No	Değişiklik Sebebi	Onay	Tarih
Rev 0	Tümü	İlk Yayın	G.M	16.09.2010

Şekil 3.9 Önleyici Faaliyet Prosedürü

4. SONUÇ VE TARTIŞMA

Günümüzde bilgi güvenliğinin önemi sürekli olarak artmakta ve bilgi güvenliği daha karmaşık bir hal almaktadır. Sürekli gelişen ve değişen yeni teknolojilerle birlikte daha da girift olmaktadır. Teknoloji ile birlikte kullanıcıların bilinç ve eğitim seviyelerindeki yetersizlikler sebebiyle bilginin ve bilgi kaynaklarının korunmasının önemi konusunda hassas davranılması gerekmektedir [28].

Bilgi teknolojileri ve bilgi güvenliği standartları kuruluşun risk analizi yapmasını, belirlenen riskler çerçevesinde gerekli kontrolleri devreye sokarak mevcut riskleri gidermesi veya kabul edilebilir risk seviyesine indirmesini şart koşmaktadır. Bilgi güvenliği sağlamak isteyen kuruluşun teknolojik olarak bilgi teknolojilerinin uygulaması donanımsal olarak gerekli tedbirleri almaları kurumsal bilgi güvenliğinin sağlandığı anlamına gelmemektedir [18].

Kurumsal bilgi güvenliğini, sadece saldırganlar, siber saldırılar veya oluşan yazılımsal güvenlik açıkları tehdit etmemektedir. Kurumsallaşamayan kuruluşlardaki dokümantasyon, yönetilemeyen prosesler, metot eksikliklerden kaynaklanan hatalar veya çalışanların sebebiyet verdiği güvenlik ihlali olayları ve kazalar da bilgi güvenliğini en az saldırganlar kadar tehdit etmektedir [26].

Bütün bunlar göz önüne alındığında Bilgi Güvenliği Yönetim Sistemi'nin yönetilmesi güçleşmektedir.

Bilgi güvenliği konusunda son yıllarda yapay zeka temelli BGYS'yi ele alan çalışmalar yapılmaktadır. Böyle bir çalışmada, yapay zekâya dayalı olarak önerilen çözüm sayesinde kuruluş yöneticileri veya çalışanı, kuruluşu için ISO/IEC 27001'e göre BGYS'nin planlanmasını, kurulmasını, oluşturulmasını uzman sistem yardımıyla gerçekleştirebileceği bildirilmiştir [32].

ISO 9001 Kalite Yönetim Sistemi, genel olarak tüm yönetim modellerine alt yapı oluşturmakta olup, etkin bir kalite sisteminin nasıl kurulacağını, ne şekilde dokümante edileceğini ve uygulama yollarını gösterir. Bununla birlikte kuruluşa etkinlik, verimlilik ve kalite gibi, unsurları içeren bir yönetim anlayışı kazandırır. Mevcut veya potansiyel problemler verilere dayalı analiz edilir. Tespit edilen sorunlar düzeltici ve önleyici faaliyet bilinci ile giderildiğinden problemlere geçici çözüm getirilmesinden ziyade sebep sonuç analizleri ile kök nedenine inilir ve kalıcı çözümler elde edilir. Kalite Yönetim Sistemi'nin bilgi yönetim modellerini oluşturan bilginin elde edilmesi, bilginin depolanması ve

korunması, bilginin paylaşımı-kaynaklara tahsisi, bilgi teknolojileri ve bilginin uygulanması süreçlerine katkı sağladığı sonucuna varılmıştır [31]. Bilgi yönetimi uygulamak isteyen firmaların öncelikli olarak Kalite Yönetim Sistemi'ni uygulamaları ve entegre olarak kurulum yapmaları bilgi yönetimi sürecini daha etkin kılacaktır.

Kalite Yönetim Sistemi ile entegre kurulan Bilgi Güvenliği Yönetim Sistemi hem kendi sisteminin gerekleri, hem de kalite sisteminin gereklerinin birlikte yönetilmesini daha da kolaylaştıracaktır. Diğer türlü sadece bilgi teknolojileri yani teknik ve donanımsal çözümlerden ileri gitmeyecektir.

Bu çalışma ile KYS ve BGYS'nin entegre olarak planlanması, kurulması ve uygulanması kuruluşta sağladığı faydalardan bazıları aşağıda verilmiştir;

- Entegre olarak oluşturulan dokümantasyon yapısı ile yönetim sistemlerinin en büyük sorunlarından olan dokümantasyon yükü azaltılmıştır.

- Dokümanların ve kayıtları yönetilmesi tek elden yapılmıştır. Böylece dokümanların kontrolü, yayınlanması, değiştirilmesi, yürürlükten kaldırılması güncelliği güvence altına alınmıştır. Hazırlanan her bir doküman çok amaçlı olarak hazırlanmakta olup kağıt tasarrufu sağlanmıştır.

- KYS ve BGYS sistemleri birbirini tamamlamıştır.

Kuruluşta kalite ve bilgi güvenliğinin birlikte uygulanabileceği anlayışı yerleştirilerek çalışanlar motive edilmiştir.

- Yönetimin gözden geçirme süreci üst yönetim tarafından yapılan planlamalarda birlikte uygulanmıştır. Buda üst yönetimin, sistemleri birlikte yürütme gereği hissettirmiş, zaman ve kaynakların kullanımında tasarruf sağlanmıştır.

- Sürekli iyileştirme kapsamında uygunsuzlukların giderilmesi, iç tetkiklerin planlanması, uygulanması, takip tetkiklerinin yapılması, düzeltici ve önleyici faaliyetlerin tanımlanması ve gerçekleştirilmesi kuruluşun insan, finans ve zaman gibi en değerli kaynaklarda tasarruf sağlanmıştır.

- Yönetim sistemlerin belgelendirilmesi açısından bakıldığında entegre kurulmuş ve belgelendirmemiş yönetim sistemleri kuruluşun finansal yüklerini azalmaktadır. Akredite belgelendirme kuruluşları tarafından KYS sistemi ile diğer yönetim sistemleri BGYS, Çevre Yönetim Sistemi, İş Sağlığı ve Güvenliği gibi sistemler entegre olarak belgelendirilirse, ikinci ve üçüncü yönetim sistemlerinin belgelendirme ücretlerinde %20 ile %50 arasında indirim yapıldığı görülmüştür [33, 34].

Ayrıca sağlık işletmelerinde yapılan bir çalışmada, sağlık yönetiminde bilgi güvenliği ilkelerinin uygulanması, sağlık güvenliği, kalitesi ve geleceği için büyük bir önem taşıdığı, bu nedenle sağlık kurumlarında bilgi güvenliği eğitimlerinin kurumsal bir yapı kazanması bakımından önemli olduğu vurgulanmıştır[35]. Sağlık işletmelerindeki çalışanlarda bilgi bilişim güvenliği kültürünün gelişimi, oluşturulacak kalite ve standartların şartlarının sağlanması, artan oranda bir güven, katılım ve geleceğe doğru sürekli gelişen, yüksek güvenilir, etkin ve kaliteli bir model ile oluşturulabileceğini bildirmişlerdir [35].

Sonuç olarak, BGYS'nin KYS ile entegre kurulması, sistemin etkinlik ve verimlilik ile beraber zamandan ve kaynaklardan önemli ölçüde tasarruf sağladığı, ayrıca mevcut sistemi geliştirmenin yanında uygulama oluşabilecek birçok probleme de çözüm getirecektir.

Bu çalışmada Kalite Yönetim Sistemi ile Bilgi Güvenliği Yönetim Sistemi'nin birlikte entegre olarak planlanması, kurulması ve daha da önemlisi uygulaması ele alınmıştır. BGYS'nin teknik tarafına girilmemiştir. ISO 9001 ve ISO/IEC 27001 Entegre sistemi ISO 20000 Bilgi Teknolojileri Yönetimi ve Bilgi Teknolojisi Altyapı Kütüphanesi (ITIL) standartları ile daha geniş ve kapsamlı olarak düşünülmesi ve bu yönde çalışmaların yapılması bilgi güvenliğini daha güvenli kılacaktır.

KAYNAKLAR

[1] **TS EN ISO 9000,** 2007. Kalite Yönetim Sistemleri – Temel Esaslar, Terimler ve Tarifler, *Türk Standartları Enstitüsü*, Ankara.

[2] **Kostak, F.,** 2007. Kalite ve Bilgi Güvenliği Sistemi ve Türkiye'de Uygulamaları, *Yüksek Lisans Tezi*, K.H.Ü., Sosyal Bilimler Enstitüsü, İstanbul.

[3] **Sadioğlu, S.,** 2000.Kalitenin Boyutları, GİM Ofset, Ankara.

[4] **Durakbaşa, M. N., Çavuşoğlu, İ. ,** 2005. Sektörel Kalite Standartları ve Entegre Kalite Yönetim Sistemleri, *V. Ulusal Üretim Araştırmaları Sempozyumu, İstanbul Ticaret Üniversitesi*, **,** 185-190.

[5] **TS EN ISO 9001,** 2009. Kalite Yönetim Sistemleri – Şartlar, *Türk Standartları Enstitüsü*, Ankara.

[6] **Baş, T.,** 2002.ISO 9000:2000 Kalite Yönetim Sistemi, Sistem Yayıncılık, İstanbul.

[7] **Önel, D., Dinçkan, A.**, Bilgi Güvenliği Yönetim Sistemi Kurulumu, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html, 10.12.2011.

[8] **Zobi, A.,** 2008. TS ISO /IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi ve KOSGEB'de Uygulaması, *KOSGEB Uzmanlık Tezi*, Ankara.

[9] **ISO/IEC 27000:2009,** 2009. Information Technology - Security Techniques- Information Security Management Systems- Overview and Vocabulary,*ISO Copyright Office*, Switzerland.

[10] **ISO/IEC 13335-1: 2004,** 2004. Information Technology - Security Techniques - Management of Information and Communications Technology Security,*ISO Copyright Office*, Switzerland.

[11] **Koç, F.,** 2008.BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu, Ulusal Elektronik ve Kriptoloji Araştırma Merkezi, Ankara.

[12] **Doğantimur, F.,** 2009. ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, *Mesleki Yeterlilik Tezi*, Maliye Bakanlığı, Ankara.

[13] **TS ISO/IEC 27001,** 2006. Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, *Türk Standartları Enstitüsü*, Ankara.

[14] **ISO/IEC 17799:2005,** 2005. Information Technology - Code of Practice Security Mnagemant,*ISO Copyright Office*, Switzerland.

[15] **Calder, A.,** 2009.mplementing Information Security Based on ISO 27001/ISO 27002: A Management Guide, 2nd Edition, Van Haren, Amersfoort.

[16] **Buluç, S.,** 2009. TS EN ISO 9000:2008 Kalite Yönetim Sistemi'nin Bir Mobilya Fabrikasında Uygulama Aşamaları ve Dokümantasyon Yapısının Oluşturulması, *Yüksek Lisans Tezi*, Bartın Üniversitesi, Fen Bilimleri Enstitüsü, Bartın.

[17] **Kılıç, K.,** 2010. ISO 9001 Kalite Yönetim Sistemi Uygulamalarının Başarısında Kurum Kültürünün Rolü; Orman Genel Müdürlüğü Örneği, *Doktora Tezi*, T.C. Sakarya Üniversitesi, Sosyal Bililer Enstitüsü, Sakarya.

[18] **Çalıkuşu, F., Karamehmet, B., Denizci, Ö.M.**, Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli, http://www.farukcalikusu.com/BGYS.pdf, 19.09.2011.

[19] B.S.I, ISO 27001 Baş Tetkikçi Kursu Katılımcı El Kitabı ve Kurs Notları, ISM04101TRTR/Yayın 24.3, İstanbul, 2010.

[20] **Kumaş, E.,** 2007. Kurumlar Üstü Bilgi Güvenliği Stratejisi, *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Elkitabı*, 330-335.

[21] **Martin, V., Pehlivanlı, İ.,** 2010. TS ISO /IEC 27001 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'de Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme, *Mühendislik Bilimleri ve Tasarım Dergisi* , **1,** 49-56.

[22] **Tekerek, M.,** 2008. Bilgi Güvenliği Yönetimi, *Kahraman Maraş Sütçü İmam Üniversitesi, Fen ve Mühendislik Dergisi*, **11,** 132-136.

[23] **Topoyan, M.,** 2003. Gıda Sektöründe Kritik Kontrol Noktaları ve Tehlike Analizleri (HACCP) ve ISO 9001:2000 Kalite Yönetim Sistemi İlişkinin İncelenmesi, *Yüksek Lisans Tezi*, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

[24] **Türkmen, Ç.,** 2006. Kalite Yönetim Sistemi'nin Kuruluşlara Sağladığı Yararlar ve Uygulamada Karşılaşılan Sorunlar - Tekstil Sektöründe Faaliyet Gösteren Bir Kuruluşta Uygulama, *Yüksek Lisans Tezi*, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

[25] **Tank, Ö.,** 2005. ISO 9001 Kalite Yönetim Sistemi Açısından Bir Aile Şirketinin Kurumsallaşma Modeli, *Yüksek Lisans Tezi*, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[26] **Vural, Y.,** 2007. Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, *Yüksek Lisans Tezi*, Gazi Üniversitesi , Fen Bilimleri Enstitüsü, Ankara.

[27] **Calder, A. , Watkins, S.,** 2008.IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002, Kogan Page, Philadelphia.

[28] **Emiral, F.**, Bilgi Güvenliği Bilincinin Genele Yayılması, http://www.btrisk.com/documents/BilgiGuvenligiBilinciningeneleYayilmasi.pdf, 10.12.2011.

[29] **Çorlu, B.,** 2006. Kalite Çevre İş Sağlığı ve Güvenliği Entegre Yönetim Sistemleri ve Bir Uygulama*, Yüksek Lisans Tezi*, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

[30] **TS EN ISO 19011,** 2004. Kalite ve Çevre Yönetim Sistemleri Tetkik Kılavuzu, *Türk Standartları Enstitüsü*, Ankara.

[31] **Güleryüz, D.,** 2008. Bilgi Yönetim Modellerinin yapılandırılmasında Etkin bir araç: ISO 9000:2000 Kalite Yönetim Sistemi*, Yüksek Lisans Tezi*, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

[32] **Gemci, C., Bay, Ö.F.**, Yapay Zeka Temelli Bilgi Güvenliği Yönetim Sistemi Yaklaşımı, http://www.emo.org.tr/ekler/4847ee98ac2a5d6_ek.pdf, 10.02.2012.

[33] **B.E.C**, Sistem Belgelendirme Hizmetlerinde Uygulanan Ücretlendirme Tarifesine İlişkin Kılavuz, http://www.bec.com.tr/docs/bec-web-k-30-05.pdf, 12.01.2012.

[34] **BVA**, Belgelendirme Hizmetleri Ücretleri Listesi, http://www.bva-bel.com.tr/Ucret.pdf, 12.01.2012.

[35] **Marsap, A., Akalp, G., Yeniman, E.,** 2008. Sağlık işletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi, *Bilişim Teknolojileri Dergisi*, **3,** 31-40.

ÖZGEÇMİŞ

Necati ALASULU

1978 yılında Samsun'da dünyaya geldi.

Eğitim- Öğretim:

2009 Fırat Üniversitesi, Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı Yüksek Lisans (devam ediyor).

2000 Ondokuz Mayıs Üniversitesi, Fen Edebiyat Fakültesi İstatistik Bölümü

1999 Ondokuz Mayıs Üniversitesi, Eğitim Fakültesi Eğitim Bilimleri Anabilim Dalı Pedagojik Formasyon Eğitimi

1994 Atakum Teknik EML Lisesi, Bilgisayar Yazılım Bölümü

İş Tecrübesi:

2009- KOSGEB (Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı) Bilgi İşlem Dairesi Başkanlığı, Bilgi İşlem Müdürlüğünde sözleşmeli Uzman

2005- TÜV CERT ve BBS CERT TS EN ISO 9001 Kalite Yönetim Sistemi Tetkikçi/Baştetkikçi

2002–2008 KADEM LTD ŞTİ. Yönetim Danışmanı/ Bilgi İşlem Müdürlüğü/ Eğitimci / Marka Vekili olarak, Küçük-Orta ölçekli şirket organizasyonu, görev, yetki ve sorumluluk tayini, kurum kültürü, mali ve satışların analizler raporlanması, veri analizleri ve iyileştirmeler yapıldı. Danışmanlığını yaptığımız şirketlere;

TS EN ISO 9001 Kalite Yönetim Sistemleri,

ISO 14001 Çevre Yönetim Sistemleri,

ISO 16949 Otomotivde Kalite Yönetim Sistemleri,

ISO 17025 Kalibrasyon ve Deney Laboratuvar Yönetim Sistemi,

TS 18001 OHSAS İş Sağılığı ve Güvenliği Yönetim Sistemleri kuruldu ve

ISO 22000 Gıda Güvenliği Sistemleri,

TS ISO /IEC 27001 Bilgi Güvenliği Yönetim Sistemleri, uygulamaları yapılarak belgelendirilmeleri sağlandı.

Aldığı Eğitimler:

TS ISO/IEC 27001 BGYS Tetkikçi /Baş Tetkikçi Eğitimi BSI (IRCA) 2010

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri Temel Eğitimi TÜV 2010

KYS Tetkikçi /Baş Tetkikçi Eğitimi, CMC(IRCA) 2005

OHSAS Tetkikçi /Baş Tetkikçi Eğitimi, CMC 2005

Ölçüm Belirsizliği Eğitimi

ISO 17025 Kalibrasyon ve Den Laboratuvarları KYS, Genel Metroloji ve Kalibrasyon

KYS Temel Eğitimi, İç Tetkik Eğitimi

ISO TS 16949 Temel Eğitim, Üretim Parçaları 0nay Prosesi, İleri Ürün Kalite Planı

ISO 22000 GGYS (HACCP) Eğitimi

TS 18001 İş Sağlığı ve Güvenliği

ISO 14001 Çevre Yönetim Sistemi

Problem Çözme ve Karar Verme Teknikleri

Toplantı Yönetimi ve Problem Çözme Teknikleri

AB Mevzuatı ve CE Direktifleri

Kamu Kuruluşlarında ISO 9000 ve TKY ve Hizmet Sektöründe Kalite

Eğiticilerin Eğitimi

Sunum Yapılan Kongreler:

XII. Biyoistatistik Kongresi – 2010

VI. İstatistik Kongresi -2008

X. Biyoistatistik Kongresi - 2007

Uygunluk Değerlendirme ve Akreditasyon Kongresi-2007

Verdiği Eğitimler:

TS EN ISO 9001 KYS Temel, Dokümantasyon ve İç Tetkik Eğitimi

ISO 17025 Laboratuvar Akreditasyonu Eğitimi

ISO 22000 GGYS (HACCP) Temel, Dokümantasyon ve İç Tetkik Eğitimi

ISO/IEC 27001 BGYS Temel, Dokümantasyon ve İç Tetkik Eğitimi

TS 18001 İSG(OHSAS) Temel, Dokümantasyon ve İç Tetkik Eğitimi

ISO 14001 ÇYS Temel, Dokümantasyon ve İç Tetkik Eğitimi

Problem Çözme ve Karar Verme Teknikleri Eğitimi

Toplantı Yönetimi Teknikleri Eğitimi

İstatistiksel Proses Kontrol Teknikleri Eğitimi

Makaleler:

1. Sağıroğlu, S., C. Çolak, M.C. Çolak, İ. Onay ve **N. Alasulu**, "Radial Basis Function Neural Network and Logistic Regression Analysis for Prognostic Classification of Coronary Artery Disease", *Ankara Üniversitesi Tıp Fakültesi Mecmuası*, **60(3)**, 97-102 (2007).
2. **Alasulu, N.,** C. Çolak, A. Duyan Çamurdan, İ. Onay ve Ö. Hastürk, "0-2 Yaş Türk Çocukların Baş Çevresi Tahmininde Farklı Modellerin İncelenmesi", *Ankara Üniversitesi Tıp Fakültesi Mecmuası*, **60(2),** 61-65 (2007).
3. **Alasulu, N.,** C. Çolak, M.N. Orman, F. Şahin ve A. Çamurdan Duyan, "0-2 Yaş Sağlıklı Çocukların Baş Çevresine ilişkin Gelişimin İzlenmesi için Büyüme Eğrileri", *Ankara Üniversitesi Tıp Fakültesi Mecmuası*, **59**, 89-92 (2006).

Bildiriler:

1. Çolak, C., **N. Alasulu** ve İ. Ercan, "Tıp Bilişiminde Bilgi Güvenliği Yönetim Sistemi'nin Diğer Yönetim Sistemleri ile İlişkisi", *XII. Biyoistatistik Kongresi*, Van, 2010.
2. **Alasulu, N.,** C. Çolak, N. Halisdemir ve S. Çalık, "Altı Sigma Yaklaşımının Proses Kontrolü ve Yönetimi ile İlişkisinin İncelenmesi", *3. İstatistik Günleri Sempozyumu*, Samsun, 2008.
3. Çolak, C., **N. Alasulu** ve M.N. Orman, "Yönetim Sistemi Yaklaşımı İle Bilgi/Bilişim Güvenliği", *X. Ulusal Biyoistatistik Kongresi*, Sivas, 2007.
4. **Alasulu, N.,** C. Çolak, A. Duyan Çamurdan ve İ. Onay, "0-2 Yaş Çocukların Baş Çevresi Tahmininde Farklı Modellerin İncelenmesi", *X. Ulusal Biyoistatistik Kongresi*, Sivas, 2007.