ISO 27001 Bilgi Güvenliği Yönetim Sistemi Yazılım Tasarımı

Araştırma Makalesi/Research Article

Ali DURDU[1]*, Ali EREN[2]

[1]Yönetim Bilişim Sistemleri, Ankara Sosyal Bilimler Üniversitesi, Ankara, Türkiye
[2]Denetim ve Risk Yönetimi, Ankara Sosyal Bilimler Üniversitesi, Ankara, Türkiye
ali.durdu@asbu.edu.tr, ali.eren@asbu.edu.tr
(Geliş/Received:09.07.2020; Kabul/Accepted:16.06.2021)
DOI: 10.17671/gazibtd.767198

Özet— Çalışmada, bilgi çağında yaşadığımız bu dönemde en önemli gereklilik haline gelmiş bilgi güvenliğinin bilgi sistemleri ile entegre edilmesi üzerine çalışılmıştır. Sürekliliğe ihtiyaç duyulan bu süreçte maksimum fayda sağlanacak şekilde tasarlanabilmesi için bir yazılım önerilmiştir. Bu uygulamada ISO 27001 bilgi güvenliği yönetimi sistemi standardının maddelerine cevap verebilecek nitelikte modüler bir yapı oluşturulmuş ve kullanıcı dostu bir yazılım uygulaması geliştirilmiştir. Uygulama içerisinde ki varlık yönetimi, risk yönetimi, tedarikçi yönetimi, envanter yönetimi, bakım yönetimi, düzeltici iyileştirici faaliyetler, olay yönetimi, eğitim ve hatırlatma modülleri ile bilgi güvenliği yönetim sistemi kurulum aşamasında ihtiyaç duyulan bütün ana süreçlerin elektronik ortama taşınmasını amaçlamıştır. Geliştirilen uygulama sayesinde bilgi güvenliği yönetimi sürecindeki kâğıt ya da elektronik ortamda yürütülen süreçler ya da yapılan işler uygulama üzerinden takip edilerek her an gözlemlenebilir duruma gelecek ve kurumun kendi durumuyla ilgili sonuca tek bir ara yüzden ulaşabilmesi sağlanacaktır. Ayrıca geliştirilen kullanıcı dostu ara yüzlerle minimum düzeyde bir eforla beklenilen işin gerçekleştirilmesi ve bu süreçte de insan hatasından en az seviyede zarar görülmesi sağlanacaktır.

Anahtar Kelimeler— bilgi güvenliği yönetim sistemi, BGYS, ISO27001, risk yönetimi, varlık yönetimi

ISO 27001 Information Security Management System Software Design

Abstract—In this study, it has been worked on the integration of information security, which has become the most important requirement in this period we live in the information age, with information systems. A software has been proposed so that it can be designed in a way that provides maximum benefit in this process that requires continuity. In this application, a modular structure that can respond to the provisions of the ISO 27001 information security management system standard has been created and a user-friendly software application has been developed. Asset management, risk management, supplier management, inventory management, maintenance management, corrective and remedial activities, incident management, training and reminder modules within the application aim to transfer all the main processes needed during the information security management system setup to the electronic environment. Thanks to the developed application, the processes carried out in the paper or electronic environment in the information security management process or the work done will be monitored through the application, and it will be observable at any time and the institution will be able to reach the result about its own situation from a single interface. In addition, with the user-friendly interfaces developed, it will be ensured that the expected work is carried out with minimum effort and the least damage from human error in the process will be ensured.

Keywords— information security management system, ISMS, ISO27001, risk management, asset management

1. GİRİŞ (INTRODUCTION)

21.yy dünyasında internet çağı yaşanırken insanlık bugüne kadar ki tarihinin toplamından daha fazla bilgiyi üretme, bilgiyi kullanma ve bilgiye erişme ihtiyacı duymaktadır. Günümüze kadar üretilen toplam bilgi günümüzde 2 yılda üretilirken, yakın zaman da 1 yıl ya da belki de 1 ayda üretilecek seviyelere gelecektir. Tabi ki bilgi üretimi faydalarıyla birlikte her şey de olduğu gibi olumsuz yönlerini de gün yüzüne çıkarmaktadır. Her bir bireyin, her

bir kurumun, her bir ülkenin ürettiği bu bilgiler kendileri için sorun oluşturacak şekilde farklı kişilerce ele geçirilmekte ve farklı şekillerde kullanılarak bilgi sahibine çok çeşitli zararlar verebilmektedir.

Bilginin bu kadar yaygınlaştığı, bilgiye olan ihtiyacın bu kadar arttığı bir dönemde oluşturulan bu bilgilerin güvenliği de çağımızın en büyük sorunlarından biri haline gelmiştir. Bilgiyi üreten insanların yanı sıra üretilen o bilgiyi yetkisiz bir şekilde ele geçirmek ve yanlış amaçlar doğrultusunda işleyerek kullanmak isteyen büyük bir insan topluluğunun olduğu da inkâr edilemez. Teknolojik gelişmelerin çok hızlı ve ciddi ilerlemeler kaydettiği günümüzde güvenlik için yapılan çalışmalar çok büyük başarılar kazansa da diğer bir taraftan da farklı tehlikeleri beraberinde doğurmaktadır. Bilgi güvenliği için üretilen her yeni ürün ya da yaklaşım aslında yeni bir açığa, savunulması gereken yeni bir cepheye ortam hazırlamaktadır. Yani kurumsal ve kişisel bilgilerin güvenliğini sadece teknik güvenlik önlemleriyle (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir [1]

İşte bu şartlar içerisinde bilgi güvenliğinin sağlanması tüm paydaşlar için (bilgiyi üreten, bilgiyi işleyen, bilgiye erişen) önem teşkil etmektedir. Bu bilgi güvenliği serüveninde her türlü desteğin alınması olabilecek tüm tehlikeler düşünülerek bir güvenlik mimarisi oluşturulması başarıya ulaşılmasında ki en büyük etkendir. Dünya genelinde bilgi güvenliği için yapılan derinlemesine çalışmalar sonucunda uygulama ve teorik olarak birçok ürün, rehber, standart oluşturulmuş durumdadır. Tüm bunlar bilgi güvenliğinin ne kadar detaylı bir alan olduğunu ve yasal bir zemine oturulması gereken teknik materyallere ihtiyaç duyan ve belli bir kültürün oluşturulmasıyla sağlanabilecek bir sistem olduğunu göstermektedir.

Bilgi güvenliği sağlanırken bilişimsel güvenlik altyapısının oluşturulması, ilgili kişilerin konular hakkında bilinçli ve kabul etmiş bir şekilde tutum sergilemesi ve tüm bunları destekleyici yaptırımları dayatan bir yasal yapı gerekmektedir. Ülkemiz de küresel pazarda yer alan bilişim cihazları büyük ölçüde yer almasına rağmen, kullanıcı bilinci ve yasal mevzuatlarda eksiklikler bulunmaktadır. Bu kampsam da gerek devlet eliyle gerekse özel iştiraklerle birçok farklı alan için birçok standart, prosedür, talimat, çerçeve geliştirilmiş ve halen geliştirilme durumundadır. Bilgi güvenliği özelinde de birçok farklı temel teşkil edebilecek kaynak vardır. Bunların arasında "Finans ve savunma sanayisi gibi özel konular dışında kalan sağlık, haberleşme, üretim, Ar-Ge vb. pek çok sektör için ISO/IEC 27000 ailesi, Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak genel kabul gören süreç yönetimidir" [2]. Ve bu ailenin en temel üyesi olan TS ISO/IEC 27001 BGYS standardı da bilgi güvenliği eksikliğin giderilebilmesi noktasında TSE tarafından oluşturulmuş bu ailenin en yaygın üyesidir [3]. Bu standart kurumsal kimlik barındıran yapıların Bilgi güvenliği için uygulaması gereken asgari şartları barındıran bir yol gösterici olarak eksik olan mevzuatı doldurmuştur. Bu standart ile kendi kendine işleyen, kontrol edilebilen, şeffaflık ilkesine bağlı ve hesap verebilen bir sistem kurulmasına rehberlik etmek istenmektedir. Standart TSE tarafından sürekli güncellenerek çağın getirilerine ayak uyduran bir sistem kurulması için güncelliğini koruması sağlanmaktadır.

Tüm bu çalışmaların paralelinde ise devlet tarafından kamu kurumlarına ISO 27001 BGYS kalite sertifikasının alınması zorunlu kılınmış ve bu kararla birlikte de özellikle kamu kurumlarında bilgi güvenliği ve bilgi güvenliği yönetim sistemi süreçleri hız kazanmıştır [4].

Biraz daha somutlaştırılarak konu ele alındığında bilgi güvenliği yönetim sisteminin varlığının kazançları kabaca aşağıdaki şekilde sıralanabilir [5].

- Yapılan risk çalışmalarıyla etkin bir risk yönetiminin sağlanması.
- Kurumsal prestijin korunması ve artışı.
- İş sürekliliğinin sağlanması.
- Bilgiye erişimin denetlenmesi ve yetkilendirilmesi.
- Tüm paydaşların güvenlik konusunda farkındalık düzeyinin yükseltilmesi.
- Kurulan gerçekçi bir kontrol sistemi ile yönetilen sistemlerde ki duyarlı bilgilerin uygun bir şekilde kullanılmasının sağlanması.
- Bilgi varlıklarının bütünlüğünün ve doğruluğunun korunması.
- Bilgi varlıklarının gizliliğinin korunması
- Bilgi varlıklarının erişilebilirliklerinin artırılması.
- Bilgi sistemleri kaynaklarını en etkili ve güvenilir şekilde kullanılmasının sağlanması.

Gerek bu zorunluluk gerek çağı yakalamak gerekse yukarıda sayılan kazançların cazibesiyle başlanılan ISO 27001 BGYS sürecinde mevcut varlıklar ve süreçler belirlenirken, bu varlık ve süreçlerin doğurduğu risk haritasının çıkartılması ve bu risklerin yürütülebilmesi için riskin ve sürecin yapısına göre farklılık gösterebilen eylemlerin tanımlanması temel teşkil etmektedir. Temeli oluşturan bu risk yönetimi ise hedeflere ulaşabilmek için her seviyede risklerin belirli bir yöntemle sistematik olarak belirlenmesi, değerlendirilmesi, kabul edilebilir seviyelerin kontrol edilmesi, risklerin etkilerini azaltma için önlemlerin alınması ve işlenmesini sağlayacak süreklilik gerektiren bir süreçtir [6].

Riskler yönetilirken risk sahibinin riskin azaltılması, riskten kaçınılması, riskin kabullenilmesi, riskin transfer edilmesi eylemlerinden hangisini seçeceği riskin ve sürecin değerine, zaman ve maliyet verilerine göre değişkenlik göstermektedir. Yapılan detaylı varlık ve risk

çalışmaları sonucunda bilgi güvenliği yönetim sistemi kurmak kurumların bilgi varlıklarının farkına varmasını, hangi varlıklara sahip olduğunu ve bu varlıkların önemini anlayarak, risklerini belirleyip yöneterek iş sürekliliğini sağlayacaktır [6].

Süreç içerisinde gerçekleştirilen tüm bu işlemlerin matbu bir yük getirdiği, oluşturulan yeni süreçlerin iş yükünü artırdığı ve insan hatasına açık noktalar oluşturduğu düşünüldüğünde çağımıza ayak uydurarak süreçlerin elektronik ortama geçmesi dinamiklik, iş sürekliliği, iş yükünde azalış ve matbu yükten kurtuluş anlamına gelecektir.

Ayrıca sistemin denetiminde sürekli denetim uygulaması olarak da kullanılabilecek bu sistem sayesinde denetçilerin, gerçek zamanlı denetim yapabilmesi, denetim kanıtlarını elektronik ortamda inceleyebilmesi ve aylık, haftalık hatta günlük raporlar alabilmesi ve gerekli bilgilendirmeleri yapabilmesi mümkün olacaktır [7].

Literatür de ki çalışmalar incelendiğinde genel olarak bilginin, bilgi güvenliğinin, bilgi güvenliğinin sağlanması gerekliliğinin ve bilgi güvenliğinin nasıl sağlanması gerektiği konusunda çalışmalar bulunmaktadır [6, 8-15]. Bu çalışmaların yanı sıra daha özele inerek süreçteki insan faktörüne dikkat çeken ve sistemlerin en zayıf halkası kadar güçlü olduğunu vurgulayan ve bu haklanın güçlendirilmesi içinde son kullanıcının farkındalıklarının artırılmasını dikkate alan çalışmalarda mevcuttur [16-18].

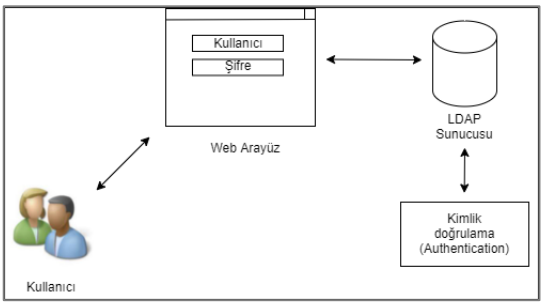
Birçok yayında da sürecin temelini oluşturun risk yönetimi ele alınarak detaylı şekilde incelenmesi ve farklı yönlerden ele alınmaları sağlanmıştır[11,12,19-25]. Literatürdeki bazı çalışmalarda da bilgi güvenliği yönetim sisteminin yazılım altyapısına oturtulması ele alınmış ve uygulama önerileri verilmiştir [7,9,21]. Mevcut literatüre destek vererek var olan önerilerin daha da geliştirilmesi ve ISO 27001 bilgi güvenliği yönetim sisteminin tüm aşamalarının yazılım ortamına aktarılması için gerekli altyapının ve bilgilendirmenin yapılması bu çalışmanın amacını oluşturacaktır.

Çalışmada bilgi güvenliği yönetim sistemi, gerekliliği ve süreçleri ve literatür hakkında verilen bilgilerden sonra çalışmada 2. bölümde uygulama genel hatlarıyla tanıtılmış, 3. bölümde modül modül gereklilikleri ve detayları incelenmiş ve 4. bölümde uygulamanın geliştirilmesi ve eksiksiz hale gelmesi için öneriler sunulmuştur.

2. GELİŞTİRİLEN UYGULAMA (DEVELOPED APPLICATION)

ISO 27001 BGYS kalite sisteminin kurum ve işletmelerde uygulanması gereken birçok süreç bulunmaktadır. Bu süreçlerde kurumun yaptığı işlerin dokümante edilmesi raporlanması, bilgi varlıklarının envanterlerinin tutulması gibi pek çok bilginin tutulması ve bu bilgilerin zaman içinde değişiminin takip edilmesi gerekmektedir. Bu kadar sürecin bilgilerinin manüel olarak tutulması gereksiz iş yükü ve aynı zamanda kontrol dışı durumların oluşmasına neden olmaktadır. Bu amaçla başlanan proje kapsamında Ankara Sosyal Bilimler Üniversitesi (ASBÜ) Bilgi İşlem Daire Başkanlığı bünyesinde ISO 27001 BGYS kontrol ve takibinin yapılabilmesi için web tabanlı bir otomasyon sistemi planlanmıştır. Açık kaynak kodlu bir altyapı da dizayn edilen uygulama da ilişkisel veri tabanı kullanılmıştır. Modüler bir yapı oluşturulmaya çalışılmış ve rol tabanlı yetkilendirme ile kişilere farklı seviyede yetkiler verilebilecek esnek bir çatı oluşturulmaya çalışılmıştır. ISO 27001 BGYS süreçlerinin gerektirdiği gibi kurumda bulunan tüm yazılım sistemlerinde Tek Oturum Açma (Single Sign On - SSO) kimlik doğrulama düzeni kullanılmaktadır. Böylelikle kullanıcılara tek bir oturum bilgileri ile birçok yazılıma erişme imkânı verilmekte ve kullanıcı şifrelerine ASBÜ şifresi adı verilmiştir. Ayrıca kullanıcıların ASBÜ şifrelerini 6 ay süreyle değiştirmeleri zorunlu kılınmıştır. Tek oturum açma kimlik doğrulama düzeni kullanılmadığında her uygulama için farklı kullanıcı bilgileri gerektirmektedir. Bu da kullanıcıların birçok şifreyle boğuşması ve bunun sonucu olarak da güvensiz şifrelerin tercih edilmesi ile sonuçlanmaktadır.

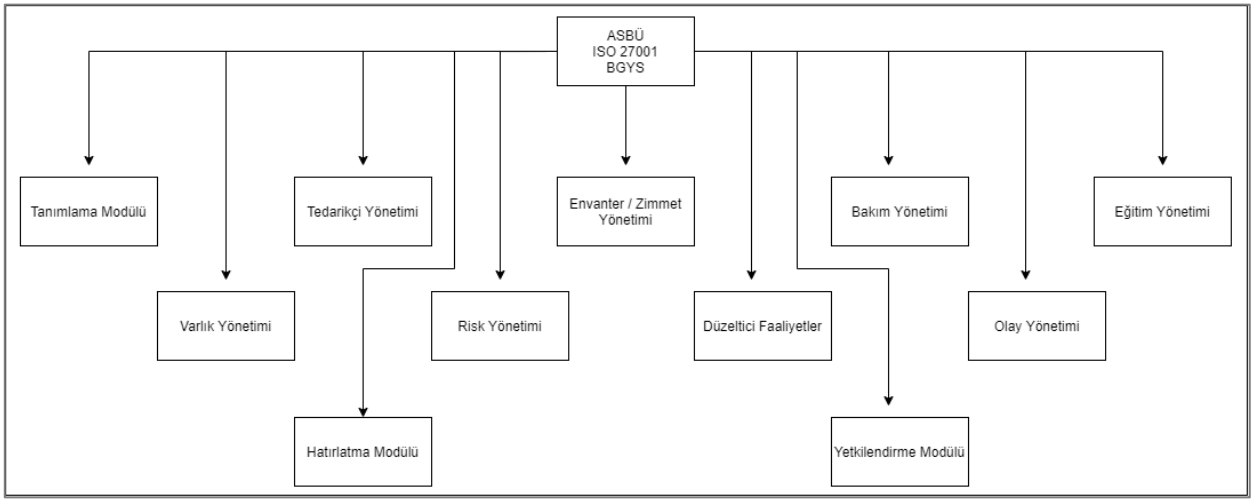
Geliştirilen sistemde SSO kimlik doğrulama sistemi için Basit İndeks Erişim Protokolü (LDAP) katman protokolü kullanılarak kullanıcı doğrulaması yapılmaktadır. LDAP, TCP/IP ile haberleşen dizin servislerini sorgulama yapmak için kullanılan bir uygulama katmanı protokolüdür [22]. Kullanıcı doğrulamasında kullanıcıların ASBÜ kullanıcı adı ve şifresi web ara yüzü ile alınarak LDAP sunucusuna gönderilir. LDAP sunucusunda kullanıcı adı ve şifre doğrulanırsa doğru (True) doğrulanmaz ise yanlış (False) cevabı gelir. Şekil 1'de LDAP katman protokolü çalışma prensibi verilmiştir. Buna göre kullanıcı web ara yüzü üzerinden kullanıcı ve şifresini girerek LDAP sunucusuna kullanıcı doğrulama talebi yapmaktadır. LDAP sunucusu üzerinden kimlik doğrulama işlemi yapılarak işlemin cevabı tekrar kullanıcı istemcisine yönlendirilir ve böylece uygulamada kullanıcı doğrulanarak sisteme alınır.



Şekil 1. LDAP katman protokolü çalışma prensibi
(LDAP layer protocol working principle)

Uygulama içerisinde tanımlama modülü, varlık yönetimi, risk yönetimi, tedarikçi yönetimi, envanter / zimmet yönetimi, bakım yönetimi, düzeltici iyileştirici faaliyetler, olay yönetimi, eğitim yönetimi, hatırlatma modülü ve yetkilendirme modülü geliştirilmiştir. Tüm bu modüller içerisinde kullanılacak olan katsayıların, sabitlerin kullanıcı tarafından tanımlanarak parametrik bir yapı sunulabilmesi için tanımlamalar modülü oluşturulmuştur.

ASBÜ ISO 27001 BGYS uygulamasında geliştirilen modüller Şekil 2'de verilmiştir. Geliştirilen bu yazılım bir bütün olarak düşünüldüğünde süreçleri işleten personeller için iş kolaylaştırıcı ve hatadan kurtarıcı bir ortam sağlarken, yönetim seviyeleri içinde karar almalarına destek sağlayan bir yapı göstermektedir.



Şekil 2. Geliştirilen modüller
(Developed modules)

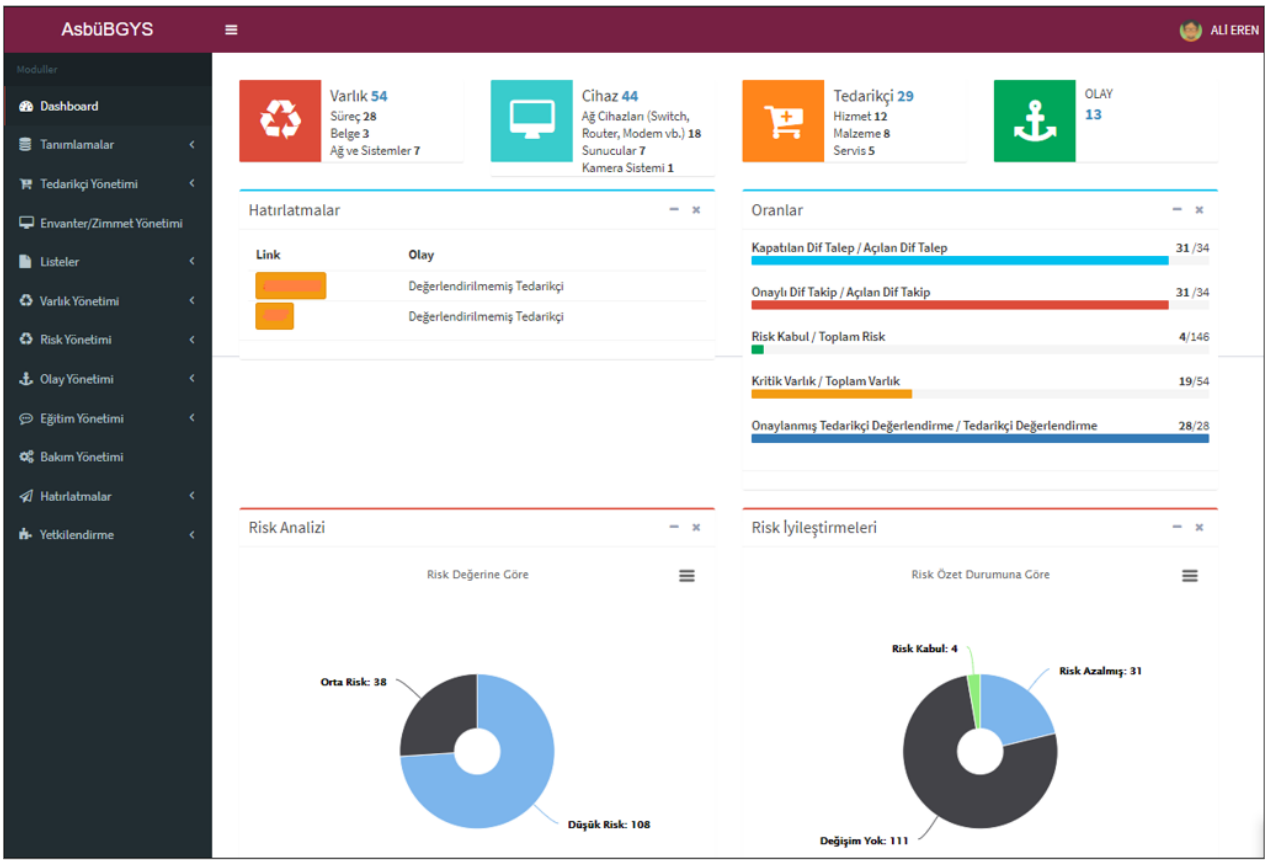
Tüm bu alt modüller, oluşturulan kayıtlar ve girilen veriler sayesinde kurum için yönlendirici olan bir sistem oluşturmaktadır. Uygulama sayesinde dijital dünyanın getirilerinden faydalanarak bir evrağın kaybolması ya da zarar görmesi ihtimalini ortadan kaldırarak oluşturulan kontrollerle veri kaybı yaşanmasının önüne geçilebilecektir. Ayrıca rapor oluşturulması için klasörlerce evrakın incelenmesi yerine bir ekranda bütün istenen sonuçlara ulaşılması sağlanabilecek, sağlanan bu özet ekranlarıyla yöneticiler ve denetçiler tarafından sürekli denetim ve kontrole imkân sağlanabilecektir. Bu noktada yöneticilere birçok enformasyon sağlayan uygulama karar alma sürelerini düşürerek etkin karar almayı sağlar. Yöneticilerin dış ve iç denetimde gerekli evrakları ve dokümantasyonu sunmasında kolaylık sağladığı gibi üst yönetime rapor imkânı sağlayarak sürecin tüm kademelerde kolayca izlenmesine olanak tanır. Yöneticiler için hazırlanan yönetici özeti görünüm sayfası Şekil 3'de verilmiştir. Şekil 3'de görüldüğü gibi yöneticinin sorgulayacağı pek çok değerin uygulama içinde tek ekranda görmesini sağlanmaktadır. Buna göre varlık modülünden gelen toplam varlık sayısı, bu toplamı oluşturan süreç, belge ve ağ ve sistemlerin sayıları görülebilmektedir. Cihaz modülünden gelen toplam cihaz sayısı ve ağ cihazları, router, sunucu gibi cihazların sayıları, kurumda hizmet veren tedarikçi sayısı ve gerçekleşen olay kayıtlarının sayılarına ulaşılabilmektedir. Kurumun ISO 27001 sürecinde elde ettiği kapatılan / onaylı / açılan dif talep, risk kabul / toplam risk, kritik / toplam varlık ve onaylanmış tedarikçi oranları gibi pek çok oran bilgisine ulaşılabilmektedir. Ayrıca süreç için çok önemli olan risk değerlendirmenin bir parçası risk analizini ve risk iyileştirmelerini düşük, orta ve yüksek risk sayıları, risk kabul, risk azalması ve değişim olmayan riskleri grafiksel olarak görebilmektedir. Kısacası sürecin kontrol ve işletilmesinde minimum çaba ve maksimum faydaya erişilmesi için bir ortam sağlanmış olacaktır. Tüm bunların yanı sıra kurum hafızası oluşturulması için önemli bir adım niteliği barındıracak ve sonraki süreç ya da uygulamalar için destekleyici bir kaynak rolü üstlenecektir.

3. GELİŞTİRİLEN MODÜLLER (DEVELOVED MODULS)

Uygulama altında varlık yönetimi, risk yönetimi, tedarikçi yönetimi, envanter / zimmet yönetimi, bakım yönetimi, düzeltici iyileştirici faaliyetler, olay yönetimi, eğitim yönetimi, hatırlatma modülü ve yetkilendirme modülü geliştirilmiştir. Geliştirilen modüller sayesinde uygulama daha esnek bir yapıya kavuşurken aynı zamanda raporlama işlemleri de düzenli ve kolay olmaktadır.

3.1. Varlık Yönetimi (Asset Management)

ISO 27001 sürecinin en temel noktasını oluşturun varlık envanterinin oluşturulması için geliştirilmiştir. Varlık deyince ilk etapta aklımıza gelen fiziki metalar bu süreç içerisinde bu tanım için yeterli gelmemektedir. Varlık kurum bünyesindeki süreçleri, fiziki metaları, dokümanları, yazılımları ya da kurumun sahip olduğu bilgi teknolojileri süreçlerinin tümünü kapsamaktadır. Şekil 4'de uygulamanın varlık tanımlama arayüzü verilmiştir. Uygulama üzerinde varlık tanımlaması yapılırken bilginin temel değerlerini oluşturan gizlilik, bütünlük, erişilebilirlik özellikleri düşünülerek o varlığın kurum için ne derece kritik olduğu çıkartılmaya çalışılmıştır. Bu değerlendirme sonucunda ortaya çıkan varlık değeri risk analizinde kullanılmak üzere varlığın en önemli tanımlayıcısı olmuştur. Uygulamada kaydedilen varlıklar Şekil 5'de verilen varlık envanteri arayüzünden takip edilebilmektedir. Geliştirilen varlık envanteri modülünde varlıkla ilgili birim, konum, bilgi sınıfı, kategori, gizlilik, bütünlük ve erişilebilirlik seviyesi gibi risk değerlendirmesinde önemli bilgiler saklanmaktadır.



Şekil 3. Yönetici özeti görünüm sayfası
(Admin summary view page)

Şekil 4. Varlık tanımlama arayüzü
(Asset definition interface)

3.2. Risk Yönetimi (Risk Management)

Risk yönetimi modülü ISO 27001 BGYS kapsamında kurumun bilgi teknolojileri risk çalışmasını esas almaktadır. Risk çalışmasında varlık modülünde ki varlıkların, süreçlerin içerdiği riskler bulunmaya çalışılmakta ve varlık değeri, bilginin temel değerleri olan gizlilik, bütünlük, erişilebilirlik değerlerinin şiddeti ve riskin olasılık değeriyle çarpılması sonucunda 100'lük skalada bir risk değeri bulunmuştur. Bu değer risk analizinin temel değerlendirme kriteri olarak ele alınmıştır.

Üst yönetim tarafından belirlenen risk değeri eşiğine göre riskler derecelendirilmiş ve risklere bu çerçevede cevap verilmeye çalışılmıştır. Uygulama üzerinde risklerin tanımlanabilmesi için Şekil 6'da verilen risk tanımlama arayüzü tasarlanmıştır. Geliştirilen risk yönetimi modülünde riskle ilgili süreç / varlık, ilgili birim, risk, risk nedeni, risk sorumlusu, önceki ve sonraki risk olasılığı, gizlilik, bütünlük ve erişilebilirlik seviyesi gibi risk analizi için önemli bilgiler saklanmaktadır.

Sistem üzerinde risk cevabı olarak Risk kabuller yapılabildiği gibi, Risklerle ilgili düzeltici iyileştirici faaliyet tanımlanması da sağlanabilmektedir. Riske verilen cevaplar neticesinde risk değerinde bir değişiklik olup olmadığının da sistem üzerinden kontrol edilebilmesi mümkün kılınmıştır.

Riskin olasılığının veya gizlilik, bütünlük, erişilebilirlik özelliklerinden birinin şiddetinin değişmesi risk değerini değiştireceği için risk takibinin yapılması yanlış, yetersiz ya da gereksiz kontrollerden kaçınılmasına yardımcı olacaktır. Kurumdaki risklerin takibi için Şekil 7'de verilen risk analiz arayüzü geliştirilmiştir. Şekil 7'de görülen örnekte sistem odasının uygun konumlandırılmaması kurumların bulundukları bina ve imkânları doğrultusunda sistem odaları yapılandırmalarındaki zorluklar nedeniyle risk kabul edilmiş ve alınan birtakım önlemler sonucu risk olasılığı orta seviyeden küçük seviyeye düşürülmüştür. Risk analiz modülünde kurumun yüksek, orta ve düşük

olasılıklı risklerini izleme, durumlarını takip etme, yapılan müdahaleler sonrası durum kontrolü gibi pek çok özelliğe imkân sağlarken risk önceliklendirmesi ve risk değerlendirmesinde yöneticilere karar alma konusunda gerekli enformasyonu sağlamaktadır.

3.3. Tedarikçi Yönetimi (Supplier Management)

ISO 27001 BGYS sürecinde gereklilik arz eden ve kurumsallaşma, kurum hafızası oluşturma içinde önemli rol oynayacak bir konu olan tedarikçi bilgilerinin barındırılması ve belirli periyodlarla tedarikçilerin değerlendirilmesi için geliştirilmiştir.

Şekil 8'de geliştirilen tedarikçi bilgileri arayüzü sayesinde çalışılan tedarikçilerin bilgilerinin yetkili kişilerin erişimine açılması sağlanmaktadır, bu sayede kurumsal hafıza oluşturulurken, insani hatalardan doğacak olan iletişim kopuklukları gibi risk oluşturabilecek olaylarında önüne geçilmiş olacaktır.

Sürecin bir diğer boyutu olan tedarikçi değerlendirilmesi için ise 10'luk puan sistemi üzerinden 10 soruluk bir anket oluşturulmuş ve bu çerçevede tedarikçinin kurum personeli tarafından değerlendirilmesi sağlanmıştır. Yapılan değerlendirmeler yıllık bazda sınıflandırılmıştır. Yapılan firma değerlendirmeleri yönetici onayına tabi tutulmakta olup bu sayede olası hataların ve duygusal yaklaşımların önüne geçilmesi amaçlanmıştır.

Şekil 9'da uygulamada geliştirilen tedarikçi değerlendirme arayüzü sayesinde 100 lük puan sisteminde bir firma puanı elde edilirken belirlenen seviyelere göre firmanın sınıflandırılması sağlanmaktadır. Bu sayede de firmaya karşı sonraki aşamada alınması gereken tavır için bir yol gösterilmiş olacaktır.

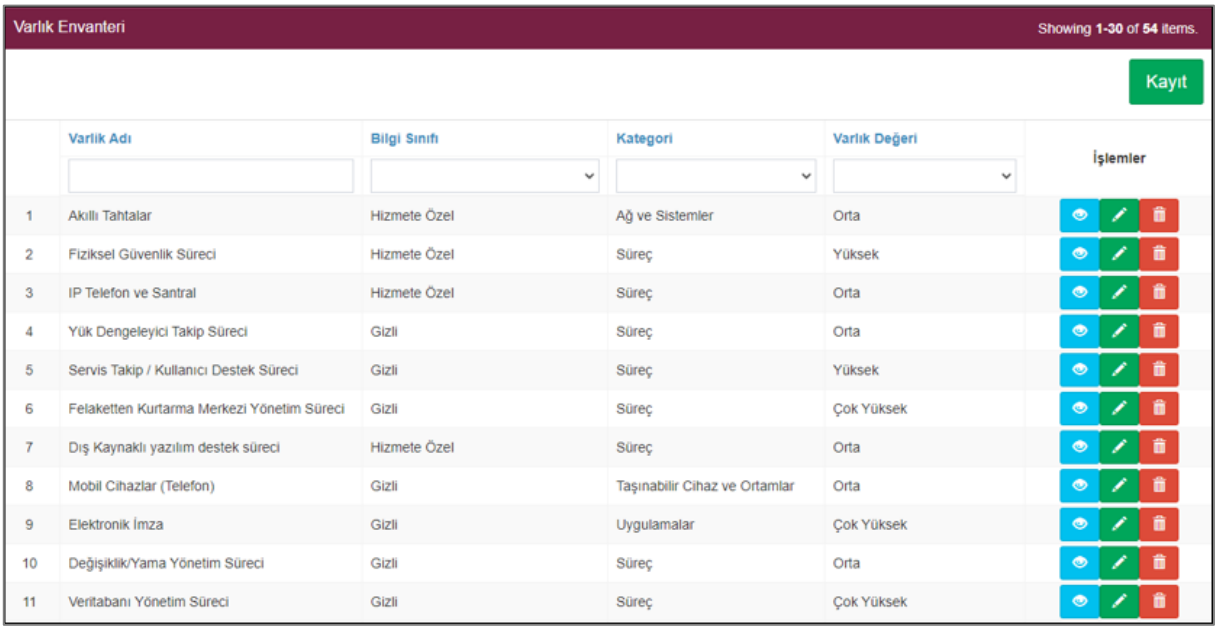
3.4. Envanter Yönetimi (Inventory Management)

Bu modül de kurum bünyesinde kullanılan tüm bilgi teknolojileri envanterinin tutulması bu sayede lisans, adet takibi gibi yoğun süreçler içerisinde gözden kaçabilen ve bu durumda büyük sıkıntılara yol açabilen süreçlerin pratikleştirilmesi amaçlanmıştır.

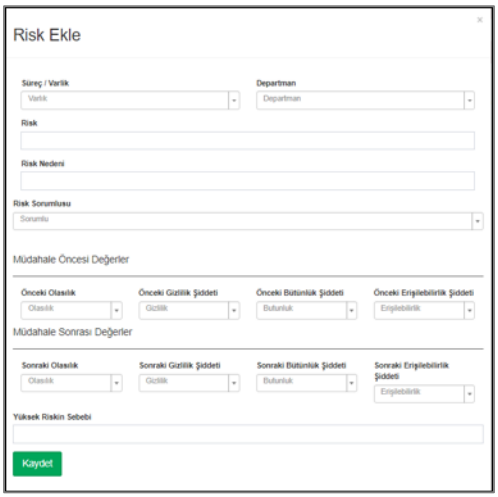
Geliştirilen arayüzler sayesinde cihazların seri numaraları, servis etiketleri, erişim bağlantıları, cihazla ilgili belgeler, alım tarihleri, garanti bitiş tarihleri gibi bilgilerin tutulması mümkün kılınmıştır. Bu bilgilerle birlikte cihazların garanti takibi yapılabilmesi için de 6 aylık, 3 aylık ve 1 aylık sürelerde mail ile garanti bitiş tarihlerinin hatırlatması yapılabilmektedir. Farklı cihaz türleri, farklı marka ve modeller olduğu ve bu çeşitliliğin sürekli değiştiği bilindiğinden her türlü seçeneğin kolayca yetkiler dahilin de kullanıcılar tarafından yapılabilecek şekilde parametrik olarak düzenlenmesi de uygulamaya esneklik kazandırmaktadır. Kurumdaki envanter listesinin tek ekranda görüntülenebilmesi için Şekil 10'daki liste arayüzü tasarlanmıştır.

3.5. Bakım Yönetimi (Maintenance Management)

Cihazların bakım tarihlerinin, bakım formlarının takip edilebileceği modüldür. Gündelik işler içinde cihazların bakımlarının takibinin zorlaştığı ve gözden kaçarak maddi ve manevi kayıplara sebep olduğu gerçeği göz önünde bulundurularak sistemden seçilen periyodlar da bakım hatırlama epostaları da yollanabilmektedir.



Şekil 5. Varlık envanteri arayüzü
(Asset inventory interface)

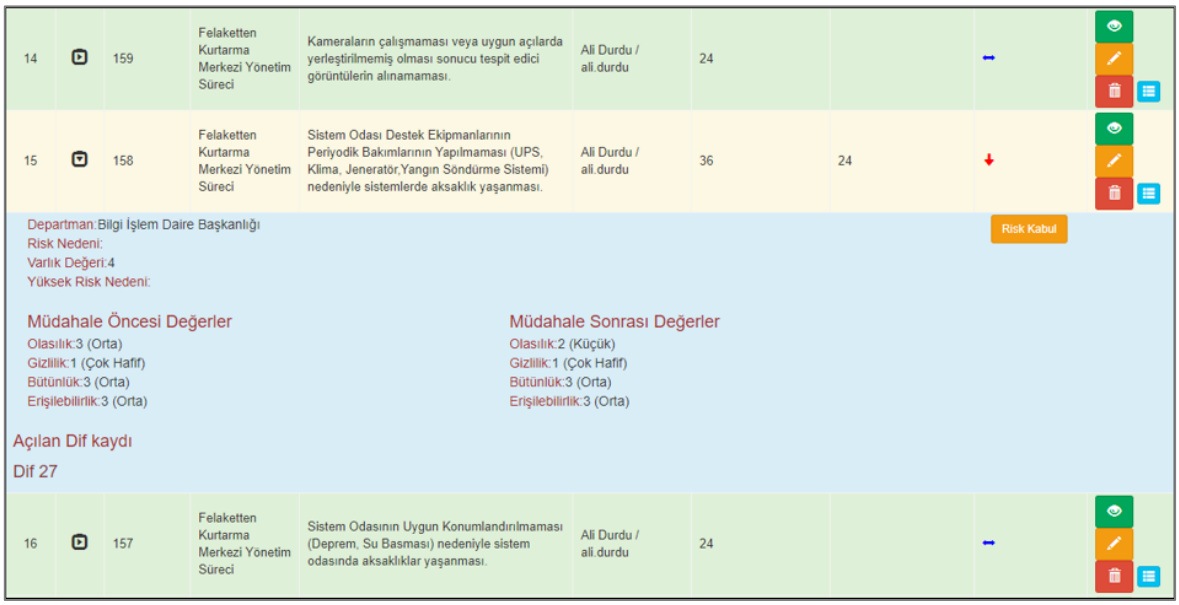


Şekil 6. Risk tanımlama arayüzü
(Risk definition interface)

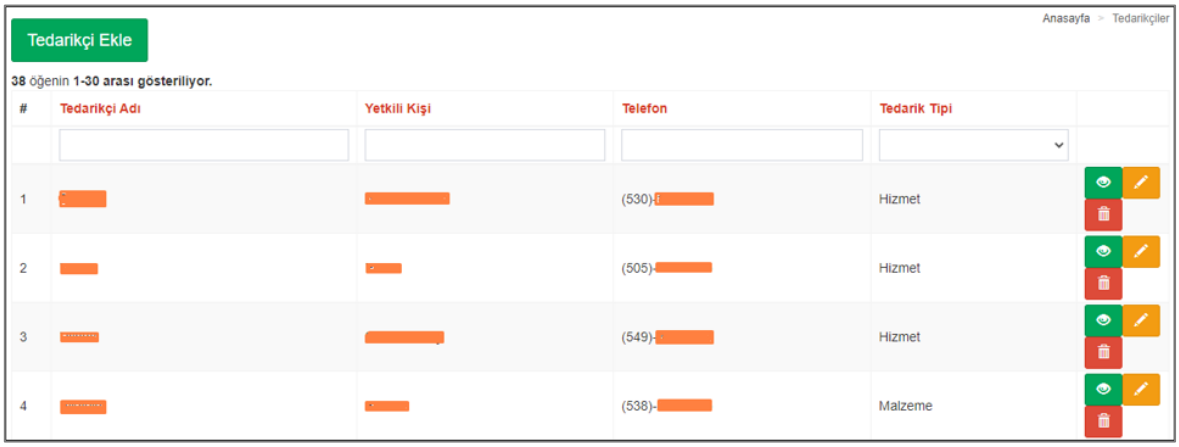
3.6. Düzeltici İyileştirici Faaliyetler (Corrective and Corrective Actions)

Düzeltici iyileştirici faaliyetler (dif) kurumun iş ve süreçlerinin devamlılığını sağlayan, çalışan ve otomatikleşen bir sistem kurulması yolunda destek veren en önemli işlemlerden birisidir. Olası risklerin önüne geçilmesi, var olan risklerin etkisinin ya da olasılığının azaltılması düzeltici iyileştirici faaliyetler sayesinde gerçekleşmektedir. Bir risk için düzeltici iyileştirici bir faaliyet tanımlanabileceği gibi bir düzeltici iyileştirici faaliyetle birden çok riske de cevap verilebilir.

Şekil 11'de ISO 27001 BGYS uygulaması kapsamında geliştirilen dif tanımlama arayüzü verilmiştir.



Şekil 7. Risk analizi arayüzü
(Risk analysis interface)



Şekil 8. Tedarikçi bilgileri arayüzü
(Supplier information interface)

Şekil 9. Tedarikçi değerlendirme arayüzü
(Supplier evaluation interface)

Geliştirilen dif tanımlama arayüzünde difle ilgili talep eden, planlanan tarih, dif durumu, ilgili olduğu riskler, dif konusu, dif sorumlusu bilgileri saklanmaktadır. Açılan dif kaydı kurum genelinde yapılan risk çalışmasına atıfta bulunabileceği gibi son kullanıcılar tarafından tespit edilmiş bir aksaklığa da cevap olabilir. Tanımlanan diflerin listesinin görüntülenebilmesi için Şekil 12'deki dif listesi arayüzü tasarlanmıştır. Şekil 12'deki dif liste arayüzünde tanımlanan diflerle ilgili durum bilgisi üzerinden difin kapatılıp kapatılmadığı ne aşamada olduğu, sorumlusunun ve ilgili olduğu risk bilgileri ile dif formunun yönetici onay bilgisi görülebilmektedir.

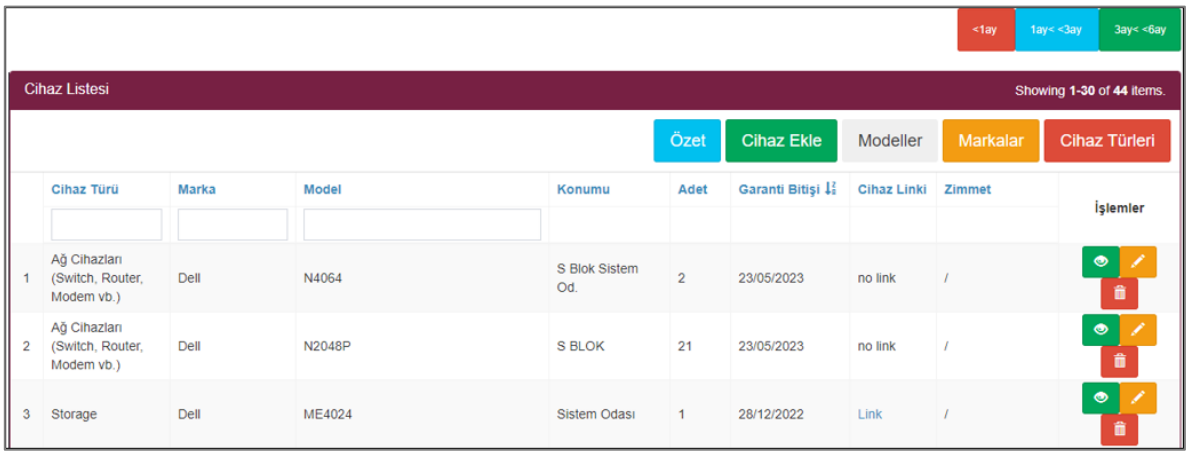
Bir dif kaydı bilgi güvenliği ekibine yapılan bir talep olarak düşünülebileceği için dif talebi olarak adlandırılabilirken, bu taleple ilgili yapılan işlemlerin takibi de dif takip olarak adlandırılabilir. Şekil 13'de uygulamada geliştirilen düzeltici iyileştirici faaliyetler listesi arayüzü verilmiştir. Şekil 13'de girişi yapılan dif talep ve talebe karşılık yapılan müdahaleyi içeren dif kök nedeni, sorumlu kişi, uygulanan faaliyet, sonuç ve tamamlama tarihi gibi dif takip kayıt bilgileri girilmektedir. Tüm bu süreçler yönetici onayına sunulmuş ve bu sayede üst yönetimin de süreçlerle ilgili farkındalığının artması ve süreçlere katılımının artırılması planlanmıştır.

3.7. Olay Yönetimi (Event Management)

Kurum genelinde hissedilen, etkisi genele yayılan bir olayın kayıt altına alınması ve sonraki süreçler için bir kurumsal hafıza oluşturulmasına yardımcı olması gerekmektedir. Bu tarz olaylar kayıt altına alınmazsa sonraki süreçte aynı sorunlarla karşılaşılabilir ve sorun çözümü için aynı süreçlerin tekrar edilmesi ve hem zaman hem de iş gücü kaybı yaşanması olasıdır. Oluşturulan olay kayıtlarıyla sonraki süreçlerde karşılaşılan olaylara müdahale süresi kısaltılabileceği gibi iş gücünde de daha verimli bir kullanım söz konusu olabilecektir. Kurumda gerçekleşen olayların takibi için tasarlanan olay kayıt arayüzü Şekil 14'de verilmiştir. Olay kayıt arayüzünde olayı kayıt eden, olayın konusu, müdahale eden ve olay tarihi gibi bilgiler tutulmakta ve kurum yönetimine sunulmaktadır.

3.8. Eğitim Modülü (Education Module)

ISO 27001 BGYS sürecinde en önemli noktalardan biri de kurum personelin bilgi güvenliği açısından farkında olmasıdır. Pek çok çalışan bilgi güvenliği ile farkındalık sahibi değilken bu durum birçok önemli kurum bilgisinin dışarıya sızmasında temel faktör olarak öne çıkmaktadır.



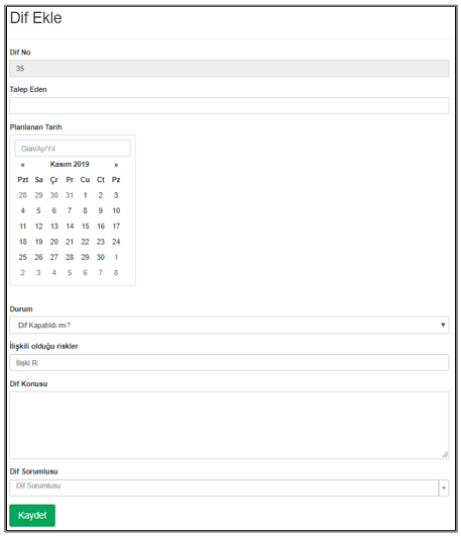
Şekil 10. Envanter listesi arayüzü
(Inventory list interface)

Eğitim modülünde bilgi güvenliğinin en önemli ve aslında en zayıf halkası olan son kullanıcı için gereklilik arz eden farkındalık eğitiminin her an ve her yerde kullanıcıya ulaştırılması amaçlanmıştır. Uygulama içinde geliştirilen eğitim modülü uzaktan eğitim mantığında hazırlanmış ve farkındalık eğitimi videoları ile kullanıcıların eğitilmesi ve eğitim sonunda hazırlanan sınav sistemi ile kullanıcılara sınav yapılabilmektedir. Sınav sonrası kullanıcıların verdiği cevaplar ile personel farkındalığı hakkında bir analiz yapılabilirken üst yönetime enformasyon sağlanabilir.

3.9. Hatırlatma Modülü (Reminder Module)

Kurumdan ayrılan personelin hesaplarının kapatılmasını hatırlatmak amacıyla bilgi güvenliği ekibine hatırlatma e-postası atılması amaçlanmıştır ve bu sayede yetkisiz

erişime yer bırakmayan bir sistem kurulması hedeflenmiştir. Ayrılan kurum personelinin tüm erişim yetkilerinin kapatılması sonradan oluşabilecek güvenlik zafiyetlerinin önüne geçilmesi açısından son derece önemlidir.



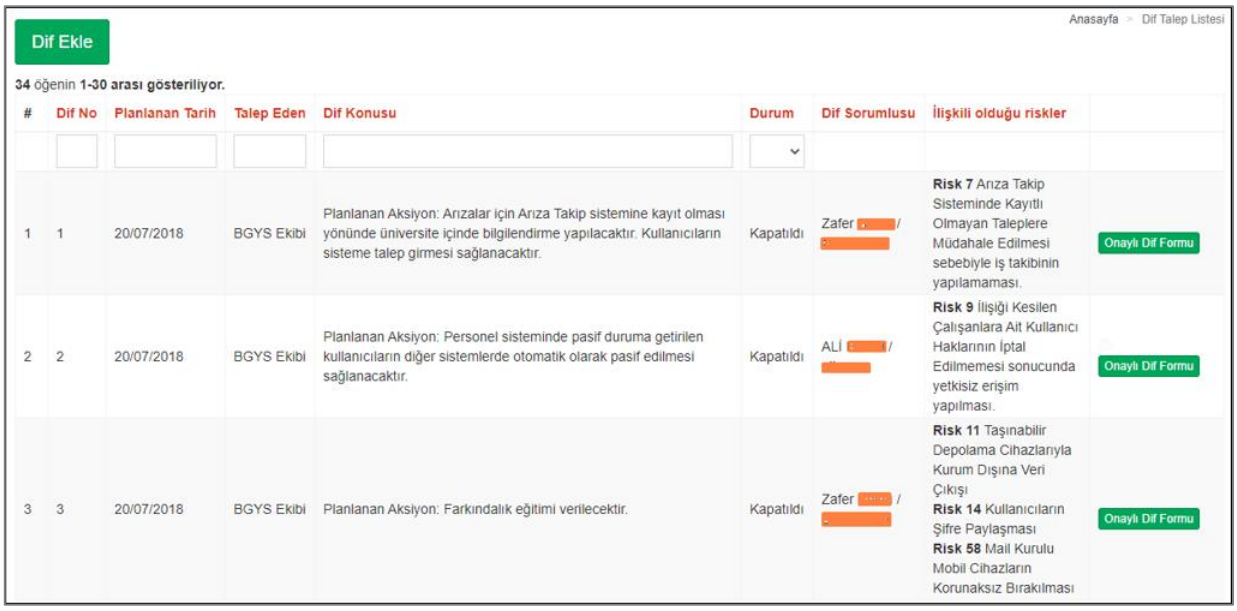
Şekil 11. Düzeltici iyileştirici faaliyet tanımlama arayüzü
(Corrective and corrective action definition interface)

3.10. Yetkilendirme Sistemi (Authorization System)

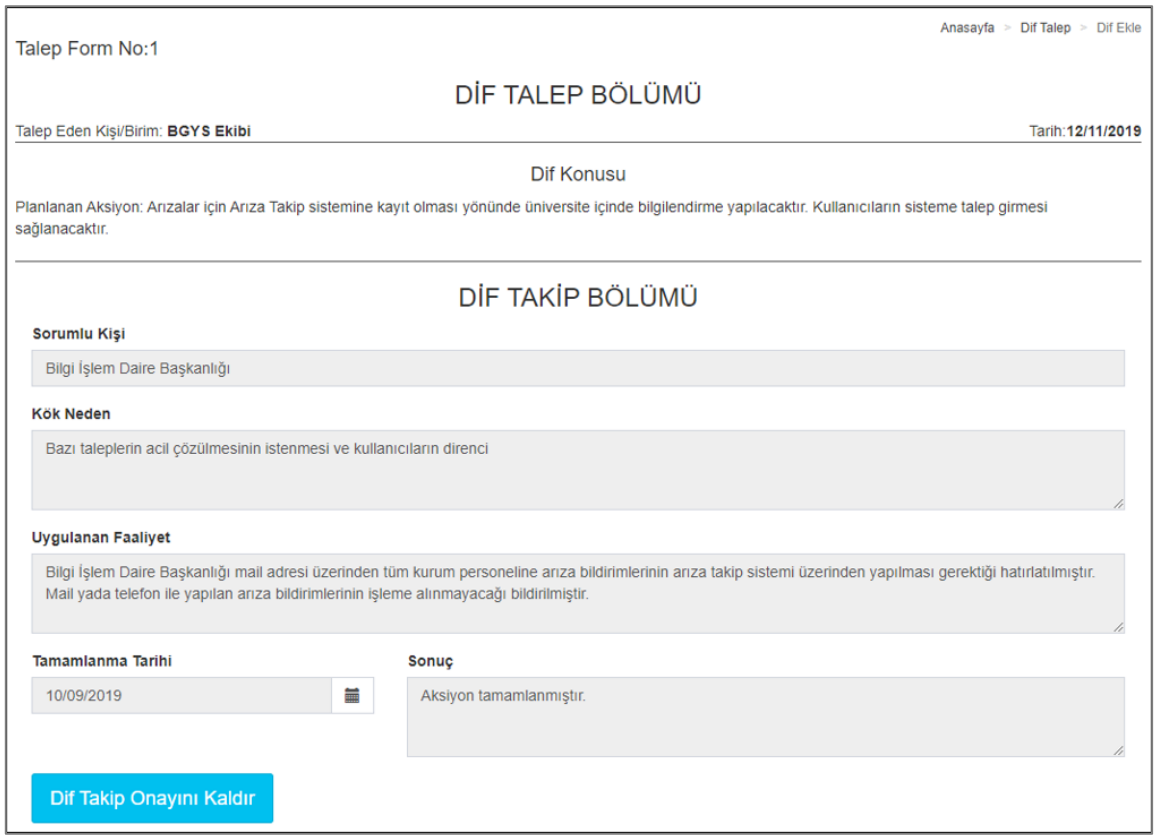
ASBÜ ISO 27001 BGYS yazılımında rol yönetimine göre bir yetkilendirme sistemi geliştirilmiştir. Şekil 15'de uygulamada geliştirilen rol tabanlı yetkilendirme sistemi verilmiştir. Buna göre yetkili kullanıcılar grubu altında süper yetkili (administrator) ve yetkili kullanıcı rolleri bulunmaktadır. Yönetici ve üst yöneticiler için yetkili kullanıcı rolleri geliştirilen modüllere erişim izinleri ayarlanarak verilebilmektedir.

Ankara Sosyal Bilimler Üniversitesi bünyesinde geliştirilen ISO 27001 BGYS süreç yazılımı kuruma bilgi güvenliği sürecini işletmesi konusunda pek çok faydası bulunmaktadır. Ankara Sosyal Bilimler Üniversitesi ISO 27001 belge alım süreci denetimlerinde uygulamanın olmadığı dönem ile uygulama kullanımı sonrası dönemde yapılan kıyaslamalar sayesinde geliştirilen uygulamanın kuruma sağladığı fayda tespit edilebilmektedir.

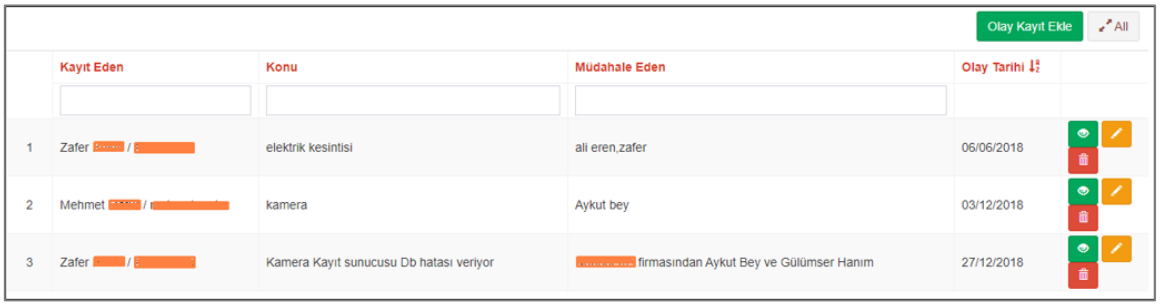
Uygulamanın standarttaki tüm süreçleri kapsayabilmesi için belirli özellikleri kazanması da kurum açısından faydalı olacak ve gerek denetim gerek yönetim aşamalarında çok daha verimli bir ortam sağlayacaktır.



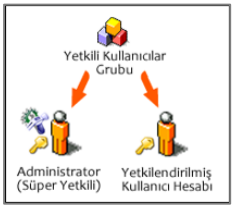
Şekil 12. Düzeltici iyileştirici faaliyetler listesi arayüzü
(Corrective and corrective actions list interface)



Şekil 13. Düzeltici iyileştirici faaliyetler takip arayüzü
(Corrective and corrective actions follow up interface)



Şekil 14. Olay kayıt arayüzü (Event registration interface)



Şekil 15. Yetkilendirme sistemi (Authorization system)

Uygulamada bundan sonraki süreçte aşağıdaki modüllerin geliştirilmesi planlanmıştır.

- Tatbikatlar modülü: Kurum içinde yıllık olarak belirlenen tatbikatların planlanması ve raporlanması.
- Hedefler ve aksiyonlar modülü: Bilgi teknolojileri hedeflerinin belirlenmesi ve takiplerinin yapılması.
- İç tetkik modülü: İç tetkik yapılması ve iç tetkik raporunun oluşturulması.
- Dokuman modülü: Politika, Prosedür, Talimat ve Formların oluşturma, revize işlemleri.
- İzleme, Ölçme ve Değerlendirme modülü: Kurumun takip etmesi gereken iş ve işlemlerin belirlendiği ve ölçülebilir kriterlerle değerlendirilmesi.

Bundan sonraki süreç için mevcut sistemin daha da geliştirilerek tüm matbu süreçleri üzerine alması ve bilgi

güvenliği yönetim sistemi sürecinin tek bir yapı olarak sunulması kurumun menfaatine olacaktır.

Tablo 1'de literatürde bulunan iki çalışmada sunulmuş ISO 27001 BGYS yazılımı ile geliştirilen yazılım kıyaslanmıştır. Buna göre risk tanımlama, risk değerlendirme, risk izleme, hatırlatıcı, envanter modülü, varlık modülü ve yerli ürün özellikleri kıyaslanmıştır. Gönen ve Rasgen'in önerdiği yazılım dış kaynaklı yazılan bir yazılım olmakta ve yerli üretim değildir. Bunun yanında bahsi geçen özellikleri barındırmaktadır. Uğuz yerli üretim yazılım olup önerilen yazılım ile benzer özelliklere sahip olmasına karşın hatırlatıcı modülü bulunmamaktadır. Önerilen yöntem literatürdeki yazılımlar ile benzer özellikleri bulunmasına karşın yerli üretim olması ve ayrıca izleme süreçlerinin aksamaması için hatırlatıcı modülü ile insan hatalarını en aza indirgemektedir.

Tablo 1. ISO 27001 BGYS yazılımlarının karşılaştırılması (Comparison of ISO 27001 ISMS software)

Özellik	Gönen ve Rasgen [7]	Uğuz [9]	Önerilen Yazılım
Envanter Modülü	+	+	+
Varlık Modülü	+	+	+
Risk Tanımlama	+	+	+
Risk Değerlendirme	+	+	+
Risk İzleme Modülü	+	+	+
Hatırlatıcı Modülü	+	-	+
Yerli Ürün	-	+	+

4. SONUÇ (CONCLUSION)

Bilgi güvenliğinin öneminin her geçen gün daha da arttığı günümüz bilgi çağında kurumların bilgi varlıklarının gizliliğini, erişilebilirliği ve bütünlüğünü korumaları büyük önem arz etmektedir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kurumların bilgi varlıklarını korumaları için yapılması gerekli süreçleri barındırmaktadır. ISO 27001 BGYS süreci sürekli yaşayan ve sürdürülmesi gereken süreçler içermektedir.

Bu çalışmada ISO 27001 BGYS süreçlerinin yazılım sistemi üzerinden takip edilmesi ve BGYS standardının maddelerine cevap verebilecek nitelikte modüler bir yapı tasarlanması amaçlanmıştır. Bu kapsamda Ankara Sosyal Bilimler Üniversitesi (ASBÜ) bünyesinde ISO 27001 BGYS yazılımı geliştirilmiştir. Uygulama içerisinde geliştirilen varlık yönetimi, risk yönetimi, tedarikçi yönetimi, envanter yönetimi, bakım yönetimi, düzeltici iyileştirici faaliyetler, olay yönetimi, eğitim ve hatırlatma modülleri ile ISO 27001 BGYS'nin kurulum aşamasında ihtiyaç duyulan bütün ana süreçlerin elektronik ortama taşınmasını sağlanmıştır.

Geliştirilen uygulamanın ISO 27001 standardının beklediği bilgi güvenliği yönetim sistemi kurulması ve yürütülmesi sürecine farklı süreçlerin merkezi yönetim ve takip kolaylığı, görsel uyarılar ve hatırlatma özelliklerinden dolayı olumlu bir etkisinin olduğu görülmüştür.

ASBÜ, ISO 27001 belge alım süreci denetimlerinde uygulamanın olmadığı dönem ile uygulama kullanımı sonrası dönemde yapılan kıyaslamalar sayesinde geliştirilen uygulamanın kuruma sağladığı fayda tespit edilebilmektedir. 2. ve 3. sertifika yenileme denetimleriyle 1. sertifikalandırma denetimi arasında tespit edilen farklar denetçi sorularına verilen cevap sürelerinin kısalması, daha yerinde ve tatmin edici cevap verilmesi, denetçi takdirinin kazanılması, evrak genelinde yapılan denetim süresinin kısalması şeklindedir.

Denetimler arasında tespit edilen bu kazanımların yanı sıra, klasörler ve dosyalar arasında kaybolmak yerine görselleştirilmiş, kolay filtreleme imkânı sunan, özet raporlarla süreç hakkında basit ve etkili bilgi edinilmesini sağlayan yapı sayesinde süreç işletilmesi sırasında da ekip üyelerine kolaylık sağlanmıştır. Oluşturulan tetikler sayesinde insan faktörü nedeniyle unutulan ya da geçekleştirilmeyen işlemlerin hatırlatılması ya da otomatik hale getirilmeleri sayesinde optimum seviyede süreçlerin kayıpsız sürdürülmesi amaçlanmıştır. Matbu evraklarda yaşanacak veri kaybı ve yetkisiz erişim riskleri en aza indirgenmiş ve rol tabanlı yetkilendirme imkânı, yedekleme kolaylığı gibi etkenler sayesinde bilginin temel değerlerinden gizlilik, bütünlük ve erişilebilirliğin maksimum verimle karşılanabildiği bir sistem kurulmuştur.

KAYNAKLAR (REFERENCES)

[1] Y. Rezgui, A. Marks, "Information security awareness in higher education: An exploratory study", *Comput. Secur.*, 27(7-8), 241-253, 2008.

[2] V. Evrin, M. Demirer, "Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği", **IV. Ağ Ve Bilgi Güvenliği Sempozyumu**, Atılım Üniversitesi, Ankara, 25-30, 2011.

[3] Internet: Türk Standartları Enstitüsü, TS EN ISO/IEC 27001:2013, https://www.tse.org.tr/IcerikDetay?ID=2311, 07.07.2020.

[4] Internet: Resmi Gazete, Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ, https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm, 07.07.2020.

[5] F. Çalıkuşu et al., "Risk Management Model Within Information Security Management System", **III. Istanbul Informatics Congress**, İstanbul, 2009.

[6] İ. Durankaya et al., "ISO27001 Bilgi Güvenliği Yönetim Sisteminde Risk Analizi", **5th International Management Information Systems Conference**, Ankara, 29-33, 2018.

[7] S. Gönen, M. Rasgen, "Sürekli Denetim Sisteminin Bir Yazılım Programında Uygulanabilirliğine İlişkin Örnek Olay Çalışması", *International Journal of Alanya Faculty of Business*, 7(1), 181-191, 2015.

[8] E. Dayıoğlu, "Kamu İdarelerinde Bilgi Sistemi Güvenlik Risklerinin Yönetimi", *Denetişim*, 4, 71–81, 2010.

[9] S. Uğuz, "Kurumsal Bilgi Güvenliği Yönetim Sistemi Yazılımları: Örnek Bir Yazılım Geliştirilmesi", *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 2(1), 1-11, 2018.

[10] M. Tuygun, "ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Kamu Kurumlarına Uygulanabilirliğinin İncelenmesi", **5th International Management Information Systems Conference**, Ankara, 25-27, 2018.

[11] L. Nikolić, B., Ružić-Dimitrijević, "Risk Assessment of Information Technology Systems", *Issues Informing Sci. Inf. Technol.*, 6, 595-615, 2009.

[12] S. Alhawari et al., "Knowledge-based risk management framework for information technology project", *Int. J. Inf. Manage.*, 32(1), 50–65, 2012.

[13] Y. Y. İleri, "Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama", *Anadolu Üniversitesi Sos. Bilim. Derg.*, 17(4), 55–72, 2016.

[14] V. Marttin, İ. Pehlivan, "ISO 270012005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme", *Mühendislik Bilimleri ve Tasarım Dergisi*, 1(1),49-56, 2010.

[15] H. Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk", *Denetişim*, 15, 45–59, 2014.

[16] H. Keser, C. Güldüren, "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme", *Kastamonu Eğitim Dergisi*, 20(3), 1167–1184, 2015.

[17] H. Koçak, K. Memiş, "Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu.", *Afyon Kocatepe Univ. J. Soc. Sci.*, 20(3), 1-10, 2018.

[18] E. Çek, **Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi**, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, 2017.

[19] D. Baccarini et al., "Management of risks in information technology projects", *Industrial Management and Data Systems*, 104(3), 286–295, 2004.

[20] A. Vildan, "Bilişim Teknolojileri Risk Yönetimi ve Yöntemleri Üzerine Bir Değerlendirme", **3. Uluslararası Yönetim Bilişim Sistemleri Konferansı**, İzmir**,** 1-14, 2016.

[21] G. Canbek, Ş. Sağıroğlu, "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme", *Politek. Derg. J. Polytech.*, 9(3), 165–174, 2006.

[22] Internet: LDAP, Basit İndeks Erişim Protokolü, https://tr.wikipedia.org/wiki/LDAP, 05.05.2021

[23] E. Kutsch, M. Hall, "The Rational Choice of Not Applying Project Risk Management in Information Technology Projects", *Project Management Journal*, 40(3), 72-81, 2009.

[24] O. Erdem, A. Younis, "Yazılım Projelerinde Risk Yönetimi", *Bilişim Teknolojileri Dergisi*, 5(1), 1-6, Nis. 2012.

[25] E. Kumas, B. Bırgören, "E-Devlet Kapısı Projesi Bilgi Güvenligi ve Risk Yönetimi:Türkiye Uygulaması", *Bilişim Teknolojileri Dergisi*, 3(2), 2010.