T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri

HAZIRLAYAN

TÜBİTAK BİLGEM
BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

Siber Güvenlik Enstitüsü

İÇİNDEKİLER

1 Giriş 3
1.1 Kısaltmalar 5
1.2 Amaç 6
1.3 Kapsam 6
1.4 Güncelleme 6
2 Kamu Kurumlarının Sınıflandırılması 7
3 Uluslararası Standartlar ve Bilgi Güvenliği Kriterleri 8
3.1 Standartlar 8
3.2 Öncelikli Güvenlik Önlemleri 8
4 Bilgi Güvenliği Kriterleri 10
4.1 Kamu Kurumlarının Sağlaması Gereken Kriterler 10
4.2 Bilgi Güvenliği Süreci 14
5 Genel Değerlendirme ve Sonuç 16
Kaynaklar 18

1 Giriş

Dayanak

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanı, "***Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı***"nın 6'ncı ana eylem maddesi olan "Kamu Bilgi Güvenliği Programı" kapsamında hazırlanmıştır. İlgili eylem maddesi Tablo-1'de verilmiştir[1].

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
6	**Kamu Bilgi Güvenliği Programı**	- ***Kamu kurumlarının uyması gereken asgari güvenlik kriterleri dokümanının hazırlanması***	***Ağustos 2013***	- TÜBİTAK (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - USOM (İ)
		- Sistem yöneticilerine ve ilgili diğer teknik personele öncelikli ihtiyaçlar uyarınca periyodik siber güvenlik eğitimlerinin ilkinin verilmesi, eğitim alan personelin yeterliliklerinin tespiti	İlki tamamlanmıştır.	
		- Kurum bazında yapılması zorunlu kılınacak yıllık güvenlik test ve denetimlerinin ilkinin, önceliklendirilecek kamu kurumları için ilgili kurumlarla mutabakat sağlanarak gerçekleştirilmesi	Aralık 2013	
		- Bilişim sistemleri güvenliğine ilişkin sıkılaştırma dokümanları ve standartların yayınlanması ve güncellenmesi	Sürekli	- TÜBİTAK (S)

Tablo-1: Eylem Planı'nın 6. maddesi

Bilişim Sistemleri ve Kamu Kurumları

Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bilgi ve iletişim sistemleri hayatımızın her alanında önemli rol oynamaktadır. Kamu kurumlarına ilave olarak enerji, su, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar da bilgi ve iletişim sistemlerini yoğun olarak kullanmaktadır.

Sözü edilen sistemler, verilen hizmetin kalitesini ve hızını artırmakta, dolayısıyla hem ilgili kurumun daha verimli çalışmasını sağlamakta hem de vatandaşlarımızın yaşam standardının yükseltilmesine katkıda bulunmaktadır.

Kurumlarımızın hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğimizin, hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir. Bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olabilecektir.

Bu tür durumların önüne geçebilmek amacıyla kamu kurumlarının sahip olması gereken asgari güvenlik kuralları belirlenmeli ve belirlenen kurallar ivedilikle hayata geçirilmelidir.

1.1 Kısaltmalar

BGYS:	Bilgi Güvenliği Yönetim Sistemi
IEC:	"International Electrotechnical Commission"
	Uluslararası Elektroteknik Komisyonu
ISO:	"International Organization for Standardization"
	Uluslararası Standardizasyon Kurumu
NIST:	"National Institute of Standards and Technology"
	Amerikan Ulusal Standart ve Teknoloji Enstitüsü
TS:	Türk Standartları
TSE:	Türk Standartları Enstitüsü
TÜBİTAK:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB:	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
USOM:	Ulusal Siber Olaylara Müdahale Merkezi

1.2 Amaç

Bu dokümanın amacı, ülkemiz kamu kurumlarında alınması gereken asgari bilgi güvenliği kriterlerini belirlemektir.

1.3 Kapsam

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanında yer alan kriterler, ülkemizdeki tüm kamu kurumlarını kapsamaktadır.

1.4 Güncelleme

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanı ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak güncellenecektir. Ayrıca Ulusal Siber Güvenlik Politikalarında yapılacak güncellemeler, bu dokümanda güncelleme ihtiyacı doğurabilecektir.

2 Kamu Kurumlarının Sınıflandırılması

Kamu kurumlarına uygulanması gereken asgari bilgi güvenliği kriterlerini belirlemeden önce kamu kurumlarının kategorilere ayrılması ve her bir sınıfa hitap edecek asgari kriterlerin belirlenmesi gerekmektedir.

Ülkemizin kamu kurumları iki kategoriye ayrılabilir.

Her kamu kurumu, öncelikle aşağıdaki tanımları göz önünde bulundurarak hangi kategoride yer aldığına karar vermelidir.

Kritik Bilgi Sistemi:

Bir bilgi sisteminin bozulması veya yetkisiz erişimle karıştırılması halinde;

a. Enerji, su, acil yardım hizmetleri, gıda tedariki ve benzeri hayati hizmetlerin durması sonucunda can kaybı oluşması veya bazı bölgelerin boşaltılması,

b. Para piyasalarının durması, ulaştırma sistemlerinden birinin durması veya diğer nedenlerle ulusal ekonominin ciddi düzeyde zarara uğraması,

c. Ulusal güvenliğin sekteye uğraması

söz konusu oluyorsa o bilgi sistemi kritiktir.

Kritik Kamu Kurumları: Bünyesinde *"**kritik bilgi sistemi**"* bulunduran kamu kurum ve kuruluşları.

Diğer Kamu Kurumları: Bünyesinde *"**kritik bilgi sistemi**"* bulundurmayan kamu kurum ve kuruluşları.

Tüm kamu kurumlarının bulunduğu listeye Başbakanlık Devlet Teşkilatı Veritabanı (http://dtvt.basbakanlik.gov.tr/AnaSayfa.aspx) internet sitesinden ulaşılabilir.

3 Uluslararası Standartlar ve Bilgi Güvenliği Kriterleri

3.1 Standartlar

Kamu kurumları için asgari bilgi güvenliği kriterleri belirlenirken, bu konuda uluslararası platformda akla gelen ilk standartlar olan ISO/IEC 27001 ve ISO/IEC 27002'den faydalanılmıştır[2,3]. ISO/IEC 27001 standardı bilgi güvenliği yönetim sürecini tanımlamakta, standartta yer alan Ek-A'da ise güvenlik önlemleri ve açıklamaları özet halinde yer almaktadır.

ISO/IEC 27002 standardında ise, ISO/IEC 27001 standardı Ek-A'da yer alan güvenlik önlemlerinin detaylı açıklamaları ve iyi uygulamaları yer almaktadır.

Bu standartlara ilave olarak, farklı sektörler için hazırlanmış olmakla birlikte tüm kurum ve kuruluşlara faydalı olacak güvenliği standartları da mevcuttur. NIST'in süreç kontrolü ile uğraşan ya da iletişim sektöründe yer alan kurumlar için hazırladığı bilgi güvenliği dokümanları bu faydalı örnekler arasında gösterilebilir[4,5]. Benzer şekilde ISO/IEC 27032 Siber Güvenlik Standardı, önemi giderek artan siber güvenlik konusunda fikir verme açısından faydalıdır[6]. ISO/IEC 27002 standardının iletişim ve enerji sektörlerinde yer alan kurumlar için özelleştirilmiş güvenlik önlemlerini içeren türevleri de tüm kurumlara bilgi güvenliği konusunda fikir verebilecek dokümanlardır[7,8].

3.2 Öncelikli Güvenlik Önlemleri

ISO/IEC 27002 standardı 11 başlık altında 133 güvenlik önlemine yer vermekle birlikte, bunlardan 10 tanesinin öncelikli olduğunu belirtmektedir. Bu önlemler ISO 27002 referansları ile birlikte aşağıda belirtilmiştir:

1. Bilgi Güvenliği Politikası (5.1.1)
2. Bilgi Güvenliği Sorumluluklarının Atanması (6.1.3)

3. Bilgi Güvenliği Eğitimleri (8.2.2)
4. Yazılım Uygulamalarında Güvenlik (12.2)
5. Teknik Açıklık Yönetimi (12.6)
6. İş Sürekliliğinin Yönetilmesi (14)
7. Bilgi Güvenliği Olaylarının Yönetilmesi (13.2)
8. Veri Koruma ve Kişisel Bilgilerin Mahremiyeti (15.1.4)
9. Kurumsal Kayıtların Korunması (15.1.3)
10. Fikri Mülkiyet Hakları (15.1.2)

4 Bilgi Güvenliği Kriterleri

Bu başlık altında ülkemiz kamu kurumlarının sahip olması gereken asgari bilgi güvenliği kriterleri açıklanmaktadır. Kriterler belirlenirken 2. ve 3. bölümlerde yer alan tanım ve başlıklar esas alınmıştır.

4.1 Kamu Kurumlarının Sağlaması Gereken Kriterler

Bilgi güvenliği kriterleri bu dokümanda iki başlık altında toplanmıştır: Önlemler ve Bilgi güvenliği süreci.

Bilgi güvenliği önlemleri güvenlik duvarı, sistem odasının emniyeti, yedekleme gibi politika ve prosedürler aracılığı ile uygulanacak tedbirlerdir. Bilgi güvenliği süreci ise, önlemlerin kurumdaki risklere uygun şekilde belirlenmesini, ardından önlemlerin izlenmesini, iç tetkik ile tüm önlemlerin gözden geçirilmesini ve yönetim tarafından Düzenleyici ve Önleyici Faaliyetlerin belirlenmesini öngören bir iş sürecidir.

Kamu kurumlarının sağlaması gereken kriterler belirlenirken ISO/IEC 27001 standardına ilave olarak diğer uluslararası standartlar, TÜBİTAK SGE'nin kurumsal deneyimi ve Ulusal Siber Güvenlik Tatbikatlarında elde edilen sonuçlar göz önünde bulundurulmuştur.

Aşağıdaki tabloda kamu kurumlarının sağlaması gereken bilgi güvenliği kriterleri belirtilmekte, dokümanın izleyen bölümlerinde ise bu kriterler açıklanmakta ve somutlaştırılmaktadır.

Aşağıdaki tabloda, "Kritik" kamu kurumlarının tüm kamu kurumları için tanımlanan kriterlere ilave olarak kendi kriterlerini de yerine getirmeleri beklenmektedir.

Bilgi Güvenliği Kriteri	Tüm Kamu Kurumları	Kritik Kamu Kurumları
Yasal Gereksinimlere Uyum	Mevzuattan kaynaklanan insan kaynakları güvenliğinin sağlanması, denetim kayıtları tutulması, lisanslı yazılım kullanılması vb. bilgi güvenliği önlemleri alınmalıdır.	
Bilgi Güvenliği Politikası	Kurum yöneticisi tarafından kurumda uygulanacak bilgi güvenliği önlemlerinin, bilişim teknolojileri bölümü çalışanlarından ve diğer kurum çalışanlarından beklentilerin açıklandığı bir politika dokümanı yayınlanmalıdır. Kurum yönetimi politika dokümanı ile bilgi güvenliğini önemsediğini ve sahiplendiğini açıkça göstermelidir.	
Bilgi Güvenliği Sorumluluklarının Atanması	Bilişim güvenliği konusunda eğitim almış bir uzman "Bilgi Güvenliği Sorumlusu" olarak atanmalı, kurumda bilgi güvenliği politikalarının uygulanmasını, sektörel SOME ve USOM'la koordinasyonu sağlamalıdır.	Kritik sistemlerin her biri için alanında uzmanlaşmış sistem yöneticileri güvenlik sorumlusu olarak atanmalı, ilgili sistemin güvenliğine ilişkin prosedürlerin çalıştırılmasını güvence altına almalıdır.
Bilgi Güvenliği Eğitimleri	Kurum çalışanlarına yılda bir kez düzenli olarak eğitimler verilmeli ve bilgi güvenliğine ilişkin "temiz masa-temiz ekran politikası" vb. sorumlulukları hatırlatılmalıdır. Bilgi Güvenliği	Kritik sistemlerin yöneticilerine sorumlu oldukları sistemlerin güvenliğine ilişkin eğitimler aldırılmalıdır.

Bilgi Güvenliği Kriteri	Tüm Kamu Kurumları	Kritik Kamu Kurumları
	Sorumlusuna ISO 27001 BGYS Uygulama eğitimi aldırılmalıdır.	
Fiziksel ve Çevresel Güvenlik	Manyetik kart vb. kimlik doğrulama yöntemleri ile sistem odalarının güvenliği sağlanmalıdır. Sistem odalarının sıcaklık, nem vb. çevresel şartları sağlanmalı, yangın, sel vb. olaylara karşı önlemler alınmalıdır.	Tüm kritik sistemlerin fiziksel ve çevresel güvenliği sağlanmalı, kritik sistemlere fiziksel erişim kayıt altına alınmalı, sistemlerin çevresel şartları uzaktan izlenmelidir.
Erişim Kontrolünün Yönetilmesi	Tüm kurum kullanıcıları benzersiz kullanıcı isimleri ve parolaları ile donatılmalı, isim ve parolaların kimse ile paylaşılmaması konusunda uyarılmalıdır. Sistemlerin fabrika çıkış parolaları değiştirilmelidir.	Kritik sistemlere erişim bilmesi gereken prensibi uyarınca düzenlenmelidir. Kullanıcılar kuvvetli parola seçmeye ve parolalarını düzenli aralıklarla değiştirmeye zorlanmalıdır.
Yazılım Uygulamalarında Güvenlik	Teknik açıklık yönetimi (bir sonraki başlık) kapsamında değerlendirilir.	Yazılım uygulamalarının çok bilinen (SQL enjeksiyonu vb.) açıklıkları barındırmaması için kurum bünyesinde yazılım geliştiriliyorsa eğitimler alınmalı, üçüncü taraflardan yazılım alınıyorsa güvenlik gereksinimleri geliştirici firmaya iletilmelidir.

Bilgi Güvenliği Kriteri	Tüm Kamu Kurumları	Kritik Kamu Kurumları
Teknik Açıklık Yönetimi	Kurumlar en az iki yılda bir kez bilgi sistemlerine açıklık analizi ve sızma testi yaptırmalı, elde edilen sonuçlar uyarınca düzeltmeleri gerçekleştirmelidir. Bilgi güvenliğinin ağ topolojisi, sınır güvenliği, antivirüs, yama yönetimi gibi alt başlıkları ile ilgili olarak sızma testi yapan firmanın tavsiyeleri göz önünde bulundurulmalıdır.	Kurumlar en az yılda bir kez alanında uzmanlaşmış firmalara açıklık analizi ve sızma testi yaptırmalı, elde edilen sonuçlar uyarınca düzeltici/önleyici faaliyetleri ivedilikle belirlemeli ve gerçekleştirmelidir.
İş Sürekliliğinin Yönetilmesi	Kurumsal bilgi ve kayıtlar düzenli olarak yedeklenmelidir.	İş sürekliliği analizi yapılmalı, kritik sistemler için ılık veya sıcak yedeklerin bulunduğu Felaket Kurtarma Merkezleri (FKM) oluşturulmalıdır. Üçüncü taraflar tarafından sağlanan FKM'ler de kullanılabilir.
Bilgi Güvenliği Olaylarının Yönetilmesi	Bilgi güvenliği olayları Bilgi Güvenliği Sorumlusu'na bildirilmelidir.	Bilgi güvenliği olaylarına müdahale prosedürleri hazırlanmalı, olay anında prosedüre uygun olarak müdahale edilmelidir.
Bilgi Güvenliği Süreci	Bilgi Güvenliği Sorumlusu kurum yöneticisine düzenli aralıklarla bildirimlerde	Kurumsal bilgi güvenliği süreci ISO 27001 standardı gereksinimlerine uygun

Bilgi Güvenliği Kriteri	Tüm Kamu Kurumları	Kritik Kamu Kurumları
	bulunmalı, kurumsal bilgi güvenliği gereksinimleri ile ilgili tavsiyeler üretmelidir.	olarak tüm bileşenleri ile çalıştırılmalıdır. *Detaylı bilgi 4.2 bölümünde yer almaktadır.*

Tablo-2: Kamu kurumlarının sağlaması gereken bilgi güvenliği kriterleri

4.2 Bilgi Güvenliği Süreci

Bilgi güvenliği yönetiminde kurumların odaklanması gereken esas nokta, olabildiğince çok güvenlik önleminin kurumda uygulanması değil, uygulanan güvenlik önlemlerine sahip çıkılmasıdır. ***Sahip çıkma kurum üst yönetiminin bilgi güvenliğini kurumsal bir süreç olarak benimsemesi***, süreci oluşturan adımları gerçekleştirmek için gereken insan kaynağını ve maddi kaynağı sağlaması ile mümkün olabilmektedir.

Bilgi güvenliğine sahip çıkma, aynı zamanda ISO/IEC 27001 standardında tarif edilen "Risk Analizi ve Tedavisi", "İç Tetkik ve Gözden Geçirme", ve "Düzeltici/Önleyici Faaliyetler" adımlarının gerçekleştirilmesi ile mümkün olabilmektedir.

Risk Analizi ve Tedavisi

Kurum, çalıştırdığı bilgi kritik sistemleri başta olmak üzere bilgi varlıklarını belirler, bu bilgi varlıklarında bulunan açıklıkları ve bu açıklıklara yönelebilecek tehditleri değerlendirir. Gerçekleştirilen değerlendirme sonucunda risk tedavisini gerçekleştirir. Risk analizi ve tedavisi işlemi yılda bir kez tekrarlanır.

İç Tetkik ve Gözden Geçirme

Bilgi güvenliği süreci uyarınca yapılan çalışmalar yılda bir kez kurum yönetimi tarafından atanan ve bilgi güvenliği çalışmalarına katılmayan tetkikçiler tarafından denetlenir. İç tetkik

sonucu bir rapor halinde kurum yönetimine arz edilir ve kurum yönetimi tarafından değerlendirilir.

Kurum yönetimi iç tetkik sonucunu ve diğer verileri değerlendirerek bilgi güvenliği sürecini kapsam, etkinlik, yasal yükümlülüklere uyum ve benzeri açılardan değerlendirir, gerçekleştirilmesi gereken düzeltici ve önleyici faaliyetleri belirler.

Düzeltici/Önleyici Faaliyetler

Yönetim gözden geçirmesi ve benzeri mekanizmalar tarafından belirlenen sorunların tekrar etmemesi için "kök sebep"ler belirlenir ve bu kök sebeplerin ortadan kaldırılması için düzeltici faaliyet gerçekleştirilir. Diğer kurumların yaşadığı sorunlar veya değişen riskler göz önünde bulundurularak önleyici faaliyetler belirlenir ve gerçekleştirilir. Düzeltici/önleyici faaliyetler kayıt altına alınır ve koyulan güvenlik hedeflerini sağlama açısından takip edilir.

5 Genel Değerlendirme ve Sonuç

20.10.2012 tarihli Resmi Gazete'de yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile 5809 sayılı Elektronik Haberleşme Kanunun eklenen EK MADDE 1 – (Ek: 6/2/2014-6518/106 md.) çerçevesinde Siber Güvenlik Kurulu'nun kurulmuş olması, ülkemiz için büyük bir kazanç olarak değerlendirilmektedir[10,11]. Bu Karar ve Kanun, ülkemiz siber güvenliği olgunluk seviyesinin gelişmiş ülkelerin seviyesine çıkmasına vesile olacaktır. Bu adımın atılmasına müteakip hazırlanan eylem planı ise[1] bu kapsamda itici güç arz etmektedir. Eylem planındaki maddelerin gerçekleştirilmesiyle, ülkemizin siber güvenlik konusunda dünyada başı çeken ülkelerden birisi olması kaçınılmazdır.

Eylem Planı uyarınca hazırlanan bu dokümanda, ülkemiz kamu kurumlarının uyması gereken asgari bilgi güvenliği kriterleri belirlenmiştir. Bu kapsamda öncelikle kamu kurumları kendi içlerinde sınıflandırılmış, kritik bilgi sistemi bulunan ve bulunmayan kamu kurumlarının sağlaması gereken kriterler belirlenmiştir. Bilgi güvenliği kriterleri belirlenirken uluslararası alanda en çok kullanılan bilgi güvenliği standartlarından ve TÜBİTAK SGE'nin kurumsal birikiminden faydalanılmıştır. Bu arada, bilgi güvenliği standartlarının yaşayan dokümanlar olduğu da unutulmamalıdır. Örneğin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri standardının güncellenmesi beklenmektedir[9].

Bu dokümanda belirlenen bilgi güvenliği önlemlerinin ve yapılandırmalarının, kamu kurumlarının sınıflandırılmasının ardından, ivedilikle hayata geçirilmesinin, ülkemiz siber güvenliğine katkı yapması beklenmektedir.

Son olarak, asgari güvenlik önlemlerinin kurumdaki belli başlı açıklıkları kapatma konusunda etkili olacağı, ancak bütün açıkların kapatılmasını *sağlamayacağı* unutulmamalı, kurumsal

bilgi güvenliğinin en üst düzeyde gerçekleştirilmesi gereken noktalarda detaylı risk analizini ve tedavisini içeren bilgi güvenliği süreçleri oluşturulmalı ve çalıştırılmalıdır.

Kaynaklar

[1] "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", T.C. Resmi Gazete, 20 Haziran 2013. http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

[2] TS ISO/IEC 27001: Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, TSE, Mart 2006

[3] ISO/IEC 27002: Information Technology — Security Techniques — Code of Practice for Information Security Management, Haziran 2005

[4] "Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security", http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800.82.pdf , NIST, Haziran 2011

[5] "Telecommunications Security Guidelines for Telecommunications Management Network", http://csrc.nist.gov/publications/nistpubs/800-13/sp800-13.pdf, NIST, Ekim 1995

[6] ISO/IEC 27032: Bilgi Teknolojisi – Güvenlik Teknikleri – Siber Güvenlik Kılavuzu, Temmuz 2012

[7] ISO/IEC TR 27019: Information Technology — Security Techniques — Information Security Management Guidelines Based On ISO/IEC 27002 for Process Control Systems Specific to the Energy Industry, Mayıs 2013

[8] ISO/IEC 27011: Information technology — Security Techniques — Information Security Management Guidelines for Telecommunications Organizations Based On ISO/IEC 27002, Aralık 2008

[9] "Have Your Say on the ISO/IEC 27001Revision", http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision, Birleşik Krallık Standartlar Enstitüsü, Erişim Tarihi: 16 Mayıs 2013

[10] "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Resmi Gazete, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf, Ekim 2012

[11] "Elektronik Haberleşme Kanunu", Mevzuat, http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5809&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5809