VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016

ELEKTRONİK PARA VE ÖDEME KURULUŞLARININ BİLGİ SİSTEMLERİ DENETİMİ

AV.ÖZGÜR ERALP
TURK ELEKTRONİK PARA A.Ş.

ÖDEME VE MENKUL KIYMET MUTABAKAT SİSTEMLERİ, ÖDEME HİZMETLERİ VE ELEKTRONİK PARA KURULUŞLARI HAKKINDA KANUN

Kanun No. 6493 Kabul Tarihi: 20/6/2013

27 Haziran 2013 PERŞEMBE
Resmî Gazete Sayı : 28690

ÖDEME HİZMETLERİ VE ELEKTRONİK PARA İHRACI İLE ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARI HAKKINDA YÖNETMELİK

Resmi Gazete Tarihi: 27.06.2014
Resmi Gazete Sayısı: 29043

ISACA
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

Resmi Gazete Tarihi: 27.06.2014 Resmi Gazete Sayısı: 29043

ISACA Bilgi sistemlerinde güven ve katma değer Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL

BANKACILIK DÜZENLEME VE DENETLEME KURUMU
Sayı : 12509071-010.06.02-2 22/08/2014
Konu : Bağımsız Denetim Rapor Formatı GENELGE 2014/2

ÖDEME HİZMETLERİ VE ELEKTRONİK PARA İHRACI İLE ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARI HAKKINDA YÖNETMELİĞİN 8 İNCİ MADDESİNİN 1 İNCİ FIKRASININ (Ç) BENDİ UYARINCA BAĞIMSIZ DENETİM ŞİRKETLERİNCE DÜZENLENECEK RAPOR

ISACA®
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI
3-4 MART 2016, İSTANBUL

ÖDEME HİZMETLERİ VE ELEKTRONİK PARA İHRACI İLE ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARI HAKKINDA YÖNETMELİĞİN 8 İNCİ MADDESİNİN 1 İNCİ FIKRASININ (Ç) BENDİ UYARINCA BAĞIMSIZ DENETİM ŞİRKETLERİNCE DÜZENLENECEK RAPOR

9. BİLGİLERİN GÜVENLİĞİ İLE GİZLİLİĞİ

Bu bölümde;

-Kullanıcı bilgilerinin güvenliği ile gizliliğine ilişkin;

a)Yönetsel önlemler

b)Teknolojik (bilgi sistemleri) önlemler

c)Personel eğitimi

konularında açıklamalara yer verilir.

10. BİLGİ SİSTEMLERİ

Bu bölümde; Gerçekleştirilecek faaliyetlerin kapsamı da dikkate alınarak, Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğin (Tebliğ) üçüncü bölümünde belirlenen usul ve esaslar çerçevesinde şirketin bilgi sistemlerinin bağımsız denetimi gerçekleştirilir. Şirketin Tebliğ hükümlerine uyum durumunun tespit edilmesi amacıyla Tebliğin 17 nci maddesi çerçevesinde yapılacak değerlendirmede, şirket tarafından yürütülmek üzere başvuruda bulunulan hizmetler ve uygulanacak iş modeli esas alınır ve Tebliğin 20 nci maddesi göz önünde bulundurulur. Denetim sonucunda, "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ"in 4, 5, 6, 7, 8, 9, 10 ve 11 inci maddeleri ile 15 inci maddesinin üçüncü fıkrası çerçevesinde bir rapor hazırlanır. "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ"in dördüncü ekindeki tabloda "Kontrol Hedefi" ve "Detaylı Kontrol Hedefi" bölümleri iptal edilir. Tespit edilen bulgular kodlanırken dört haneli "Süreç" alanı "DiĞR" olarak kodlanır

ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

Resmi Gazete Tarihi: 27.06.2014 Resmi Gazete Sayısı: 29043

Bilgi güvenliği yönetim süreci

MADDE 5 – (1) Kuruluş üst yönetimi, bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutar ve bu amaçla bilgi güvenliği politikasını oluşturur ve onaylar.

(2) Bilgi güvenliği politikası ile bilgi güvenliği yönetim sürecinin oluşturulması, sürdürülmesi ve yönetilmesine ilişkin görev ve sorumluluklar açıkça tanımlanır ve bu kapsamda bilgi güvenliği politikasına uyum durumu yılda en az bir defa yönetim kuruluna raporlanır.

(3) Kuruluş üst yönetimi, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi için yeterli kaynağı tahsis eder ve güvenlik politikasıyla uyumlu olacak şekilde gerekli güvenlik kontrollerinin tesis edilmesini sağlar. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

Bilgi güvenliği yönetim süreci

MADDE 5 –

(4) Üst yönetim, bilgi güvenliği yönetim süreci kapsamında;

a) Bilgi güvenliği politikasının ve tüm sorumlulukların yılda en az bir defa gözden geçirilmesini, güncellenmesini ve onaylanmasını,

b) Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, saklanan ve iletilen verilerin güvenlik hassasiyet derecelerine göre sınıflandırılmasını ve her bir sınıf için uygun düzeyde güvenlik kontrollerinin tesis edilmesini,

c) Güvenlik alanındaki güncel gelişmeler, yeni tehditler ve zafiyetlerin takip edilmesini, gerekli yazılım güncellemelerinin ve yamaların uygulanmasını,

ç) Bilgi güvenliği ihlaline ilişkin olayların izlenmesini ve periyodik olarak değerlendirilmesini,

d) Kuruluşun bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılmasını,

e) Bilgi güvenliği hususunda hem kurum içinde hem de kullanıcılar ve üye işyerleri nezdinde farkındalığı artıracak çalışmaların gerçekleştirilmesini,

sağlar.

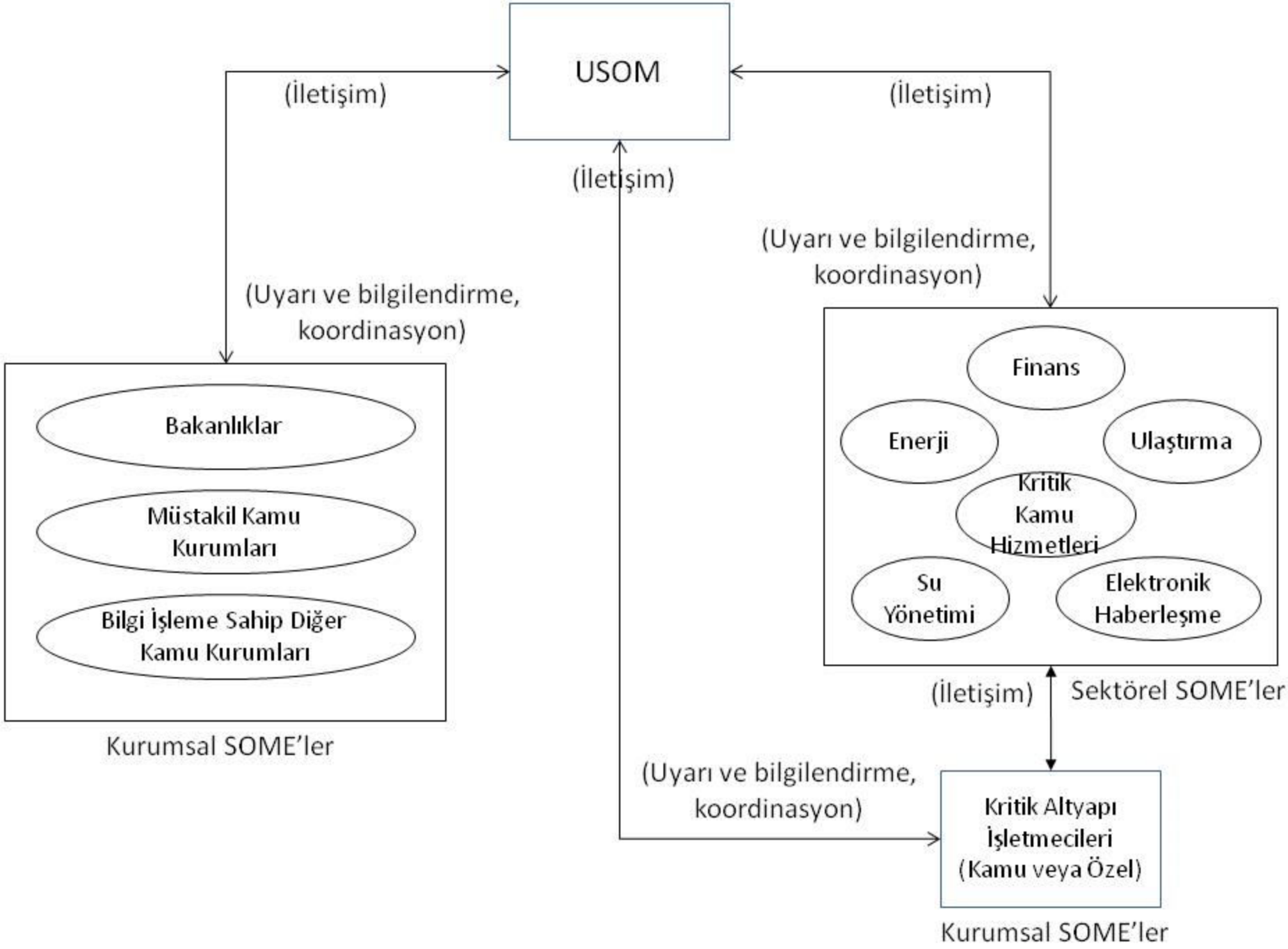
11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında Kurumsal SOME kurma yükümlülüğü olan kurumlar için hazırlanan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde Kurumsal SOME'lerde istihdam edilecek personelin alması tavsiye edilen eğitimler Tablo 6'da verilmiştir.

Organizasyon	İlgili Mevzuat	İlgili Doküman
USOM	22 Mayıs 2013 Tarihli 2013/278 Sayılı Usul ve Esaslar (BTK Kurul Kararı)[1]	–
Sektörel SOME	Tebliğ[2]	Sektörel SOME Kurulum ve Yönetim Rehberi
Kurumsal SOME		Kurumsal SOME Kurulum ve Yönetim Rehberi

Tablo 1 - İlgili Mevzuat ve Dokümanlar

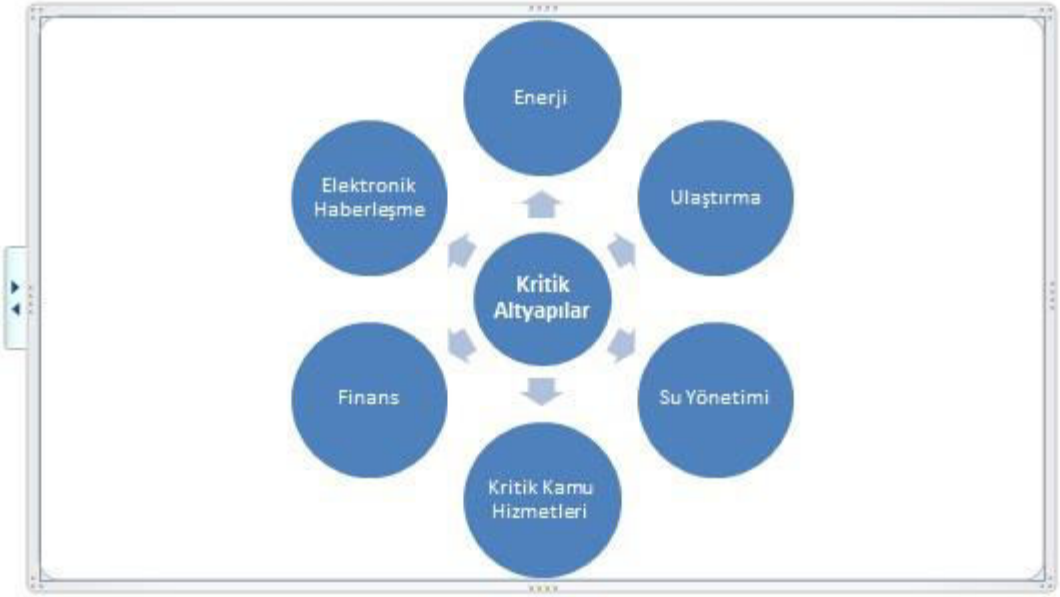
Organizasyon	Kurulduğu Kurum / Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	• Kritik sektörü düzenleyici ve denetleyici kurumlar • Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Tablo 2 - Hizmet Alanları


USOM
(İletişim)
(İletişim)
(İletişim)
(Uyarı ve bilgilendirme, koordinasyon)
(Uyarı ve bilgilendirme, koordinasyon)
Bakanlıklar
Müstakil Kamu Kurumları
Bilgi İşleme Sahip Diğer Kamu Kurumları
Kurumsal SOME'ler
Finans
Enerji
Ulaştırma
Kritik Kamu Hizmetleri
Su Yönetimi
Elektronik Haberleşme
(İletişim)
Sektörel SOME'ler
(Uyarı ve bilgilendirme, koordinasyon)
Kritik Altyapı İşletmecileri (Kamu veya Özel)
Kurumsal SOME'ler

2.1 Kritik Altyapılar ve Sektörel SOME'ler

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5 numaralı eylem maddesi kapsamında, Siber Güvenlik Kurulu'nca ülkemizin kritik altyapı sektörleri "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" olarak belirlenmiştir.



Şekil 2: Türkiye'nin kritik altyapı sektörleri

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum
Enerji	EPDK
Elektronik Haberleşme	BTK
Finans	SPK, BDDK
Su yönetimi	Orman ve Su İşleri Bakanlığı
Kritik Kamu Hizmetleri	Ek 3'te belirtilmiştir
Ulaştırma	Ek 4'te belirtilmiştir

Tablo 3: Sektörel SOME'leri Kurulacağı Kurumlar

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum	Kritik sistemlerin belirlenmesi için kullanılabilecek parametreler
Enerji	EPDK	Sistemlerin ürettiği, depoladığı, ilettiği, dağıttığı veya satışına aracılık ettiği enerji miktarı
Elektronik Haberleşme	BTK	Sistemlerin depoladığı veya taşıdığı veri miktarı, yapılmasına aracılık ettiği konuşma sürelerinin toplam uzunluğu
Finans	SPK, BDDK	Sistemlerin sakladığı mevduat hacmi veya transferine aracılık ettiği mevduat miktarı
Su yönetimi	Orman ve Su İşleri Bakanlığı	Sistemlerin ürettiği, ilettiği, arıttığı veya dağıttığı su miktarı
Kritik Kamu Hizmetleri	Ek 3'te belirtilmiştir	Sistemlerin yapılmasına eşlik ettiği işlem sayısı, iç kullanıcı veya dış kullanıcı sayıları kullanılabilir.
Ulaştırma	Ek 4'te belirtilmiştir	Sistemlerin taşıdığı yük ve/veya yolcu sayısı

Tablo 5: Kritik sistemlerin belirlenmesi için kullanılabilecek parametreler

ISACA®
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

VII.BİLGİ TEKNOLOJİLERİ YÖNETİŞİM VE DENETİM KONFERANSI

3-4 MART 2016, İSTANBUL