KPMG
cutting through complexity™

KPMG TÜRKİYE
Araştırma Raporu

Uluslararası Destek Hizmetleri Uygulamaları

Finansal Hizmetler **Mart 2013**

kpmg.com.tr

Araştırma Hakkında

Araştırmanın amacı, kapsama alınan ülkelerde mevcut olan destek hizmetleri uygulamalarına ilişkin düzenlemelerin ve tedarikçi firmaların güvence ve denetimleri için kullanılan uluslararası standartların incelenmesidir.

Araştırmamız; destek hizmetleri kullanım oranları, finans ve bankacılık sektörünün büyüklüğü ve olgunluk seviyesi, denetim ve güvence uygulamaları, bilgi sistemlerinin kullanım oranları, destek hizmeti kullanımına ilişkin yasal düzenlemeler ve uyum çalışmaları göz önünde bulundurularak hazırlanmıştır. Araştırma raporu kapsamına alınan ülkeler; finansal sektördeki ana aktörler arasından seçilmiş olmakla birlikte, Avrupa Birliği üyesi olmaları, müşteri ve veri gizliliği ilkeleri hakkında köklü ve kapsamlı yasal düzenlemelere sahip olmaları seçim için dikkate alınan faktörlerden bazılarıdır. Raporda ek olarak, uluslarası standartların kapsam dahilindeki ülkelerdeki kullanım alanları ve Türkiye'de mevcut olan destek hizmetleri kapsamındaki düzenlemeler ile ilişkisi mercek altına alınmıştır.

Araştırma raporu kapsamına alınan ülkelerin seçilme kriterleri açısından öne çıkan başlıklara aşağıda yer verilmiştir:

Almanya: Avrupa Birliği üyelerinden olan Almanya, gelişmiş ve küresel bir bankacılık sektörüne sahiptir. Avrupa Birliği standartlarına uyum adına, Türkiye için bir örnek teşkil edebileceği göz önüne alınarak, araştırma raporu kapsamına alınmıştır. Aynı zamanda destek hizmetleri denetim ve güvence uygulamaları çerçevesinde, ISAE 3402 tabanlı ulusal bir standardının bulunması, araştırma raporuna konu edilmesinde önemli bir rol oynamıştır.

Amerika Birleşik Devletleri: Finansal sektörün öncülerinden olan Amerika Birleşik Devletleri, gerek Avrupa Birliği ülkeleri, gerekse diğer dünya ülkeleri üzerinde önemli bir rol modelidir. Enron skandalı sonrası, özellikle yönetim beyanı uygulamalarını ve SOX uygulamalarını yasal bir zorunluluk haline getirmiş ve diğer ülkelere denetim ve standartlar konusunda örnek teşkil etmiştir. Aynı zamanda destek hizmeti kullanımı konusunda yüksek bir orana sahip olması da, araştırma raporuna konu edilmesinde önemli rol oynamıştır.

Birleşik Krallık: Küresel çapta önem teşkil eden bir finansal sektöre sahip olan Birleşik Krallık, özellikle bankacılık sektöründe köklü ve kapsamlı yasal düzenlemelere sahip bir Avrupa Birliği üyesidir. Dünya finansal sektörünün lokomotiflerinden olması da göz önüne alındığında, araştırma raporu kapsamına alınmıştır. Aynı zamanda destek hizmetleri denetim ve güvence uygulamaları çerçevesinde, ISAE 3402 tabanlı ulusal bir standardı bulunması ve ülkedeki verilerin korunma yasasına uyum çalışmaları araştırma raporuna konu edilmesinde önemli bir rol oynamıştır.

İsviçre: Dünyanın mali konjonktüründe önemli bir rol oynayan İsviçre, dünyadaki bankacılık merkezlerinden biridir. 1934'de yasalaşan müşteri bilgi gizliliğini öne çıkaran "bankacılık sırrı" geleneği, araştırma raporuna konu edilmesinde dikkate alınan bir faktör olmuştur.

Avustralya: Destek hizmetleri denetim ve güvence uygulamaları çerçevesinde, ISAE 3402 tabanlı ulusal bir standardı bulunması, ülkenin araştırma raporuna konu edilmesinde önemli bir rol oynamıştır. Aynı zamanda risk yönetimi, yönetişim, destek hizmeti denetim ve güvence uygulamaları konusunda en iyi uygulamalara ("best practices") sahip olması ve bunları etkin olarak kullanması dikkate alınmıştır.

İçindekiler

Yönetici Özeti

Gelişmiş pazarlarda özellikle büyük bankalar destek hizmetlerinin en büyük kullanıcılarından biri olmuş ve öncelikle ülke içerisinde başlayan kullanımlarını daha ucuz kaynakların bulunduğu ülke dışına yönlendirerek kullanım düzeyini önemli ölçüde artırmışladır. İş süreçlerini kısmen veya tamamen dış kaynaklardan temin etmenin bu derece arttığı ve küresel pazarda günümüzde tek bir firma ile bankalar arasında yapılmış milyonlarca dolar değerinde destek hizmeti alım sözleşmelerinin bulunduğu göz önüne alındığında; büyük veya orta ölçekteki küresel bankalar arasında tüm iş ve bilgi sistemleri süreçlerini kendi bünyesinde işleten banka sayısının yok denecek kadar az olduğu görülmektedir.

Süreçlerin işletiminin bankaların bünyesinden çıkartılarak üçüncü taraflardan temin edilmesi ve dolayısıyla destek hizmetleri pazarının büyümesi yalnızca tedarikçilerin iştahını kabartmakla kalmamış; aynı zamanda, özellikle bankalar ve finansal kuruluşları düzenleyen otoritelerin de dikkatini çekmiştir. Ülkedeki bankacılık mevzuatı ve bankacılık anlayışının, ülke risklerinin, genel risk toleransının ve büyük ölçekli bankaların destek hizmetleri kullanımına yöneliminin, hakim otoritelerin bu çerçevedeki yaklaşımını etkilediği ve şekillendirdiği düşünülmektedir. Otoritelerin bu çerçevedeki tutumları, kimi zaman uyum gerektiren mevzuat, standart veya düzenleme olarak şekil bulurken; kimi zaman ise rehber, tavsiye veya herhangi bir şekilde aksiyon almama halinde kendini göstermiştir.

Tedarikçilerden temin edilecek hizmete karar verilmesi, değerlendirilmesi, firma seçimi ve ilgili hizmetin düzenleyici kuruluşlara bildirilmesi konusundaki önceliğin, tamamen bankalara verildiği veya sürecin düzenleyici kuruluş tarafından adım adım tasarlandığı durumlar mevcuttur. Temel olarak yapılan çalışmalarda ortak bir risk algısı mevcut olsa da; yukarıdaki bahsi geçen uygulama farklılığı, destek hizmetlerinden kaynaklanan risklerin yönetimi konusunda da gündeme gelmektedir. Ancak, görülen farklı yaklaşımlara rağmen, tüm düzenleyici kuruluşların hemfikir olduğu tek konunun, destek hizmetleri sunan firmalarda iç kontrol ortamının yeterli, uyumlu ve etkin bir biçimde kurulması ve takip edilmesi olduğu görülmektedir.

Destek hizmeti sunan firmaların iç kontrol ortamlarının ve faaliyetlerinin takip edilmesi kapsamında düzenleyici otoriteler tarafından cevaplandırılmakta zorlanılan, fakat bankalar tarafından da cevabı en çok merak edilen sorular arasında ise "Nasıl?" ve "Kim?" gelmektedir. Bu sorulara verilecek olan her cevap ise bu alanda etkin olan tüm aktörlerin operasyonel ve finansal faaliyetlerini etkilemekte; birisi için kaçınılması gereken yük olarak görülebilirken, bir diğeri için ise bir fırsat olarak kabul edilmektedir.

Birden çok banka ve finansal kuruma hizmet sunan destek hizmet kuruluşları, gerek mevzuat gerekse ilgili kurumların iç düzenlemeleri doğrultusunda, iç kontrol ortamlarının hizmet sundukları bankalar tarafından denetlenmesi kapsamında çeşitli maliyetlerle karşı karşıya kalabilmektedirler. Bankalar tarafından yapılan ilgili denetim çalışmaları destek hizmet kuruluşları nezdinde verimsiz çalışmalara ve operasyonel maliyetlerin artmasına sebebiyet vermektedir.

Diğer taraftan, bankaların yürütmekte oldukları ana bankacılık faaliyetleri dışındaki konularda destek hizmetleri sunan kuruluşlar nezdinde denetimler gerçekleştirmeleri, yapılan denetim çalışmalarının destek hizmetleri ile ilgili risklerin tamamının ortaya çıkarılamamasına yol açmaktadır.

Destek hizmeti sunan kuruluşların iç kontrol ortamlarının denetimine ilişkin yukarıdaki mevzu bahis durumun araştırmaya konu olan ülkelerin düzenleyici otoriteleri tarafından da göz önünde bulundurulduğu ve bu çerçevede tüm taraflara uygun olabilecek makul çözümlerin sunulmaya çalışıldığı görülmüştür. Söz konusu ülkelerde, destek hizmetleri kullanımına direkt olarak atıfta bulunan yasa, genelge, tebliğ, standart veya kılavuz olarak yayımlanmış düzenlemeler bulunmaktadır.

Ülke mevzuatlarında destek hizmeti sunan kuruluşların iç kontrol ortamlarının, hizmet verdikleri kuruluşlar dışında, bağımsız denetim firmaları tarafından da denetlenebileceği ve raporlama yapılabileceği belirtilmektedir.

Genel itibarıyla, destek hizmetleri konusunda güvence, denetim ve raporlama standartlarına, ülke mevzuatlarında açıkça yer verilmemekte ve bu alana ilişkin herhangi bir sınırlama bulunmamaktadır.

Ek olarak, hangi destek hizmetlerinin denetim kapsamına alınması gerektiği ve kimler tarafından denetlenmesi ile ilgili konulara da ülke mevzuatlarında açıkça yer verilmemektedir.

İsviçre ve Avustralya özelinde, dış kaynak hizmeti sunan firmaların iç kontrol ortamlarına ilişkin bağımsız dış denetim faaliyetlerinin ve raporlarının destek hizmeti alan kuruluşlar/bankalar tarafından kabul edilebileceği ve bankaların iç kontrol ve risk yönetimi çalışmalarında referans olarak kullanılabileceği belirtilmiştir. Bu tarz yaklaşımlar, uluslararası kabul görmüş güvence denetim ve raporlama standartlarının yaygınlaşmasına sebebiyet vermiştir.

IFAC ("International Federation of Accountants") tarafından yayımlanmış olan hizmet sağlayıcılara ilişkin güvence standardı ISAE 3402, araştırmaya konu olan ülkeler tarafından kabul görmüş ve Avustralya, ABD, Almanya ve Birleşik Krallık kendi ulusal standartlarının oluşturulmasında ISAE ("International Standard on Assurance Engagements") 3402'yi temel almışlardır.

ISAE 3402 ve benzeri güvence, denetim ve raporlama standartlarının yaygınlaşması ve kabul görmesiyle birlikte, pazardaki yerini koruma altına almak isteyen destek hizmeti sunan kuruluşlar da kendilerini bu değişime adapte etmeye çalışmaktadırlar. Bu adaptasyon sürecinde, sektöre hakim firmalar uyum sorunu yaşamadan faaliyetlerine devam edebiliyorken, küçük ölçekli firmalar, mevzuatların giderek katılaştığı bankacılık sektöründen ayrılmak zorunda kalmaktadırlar.

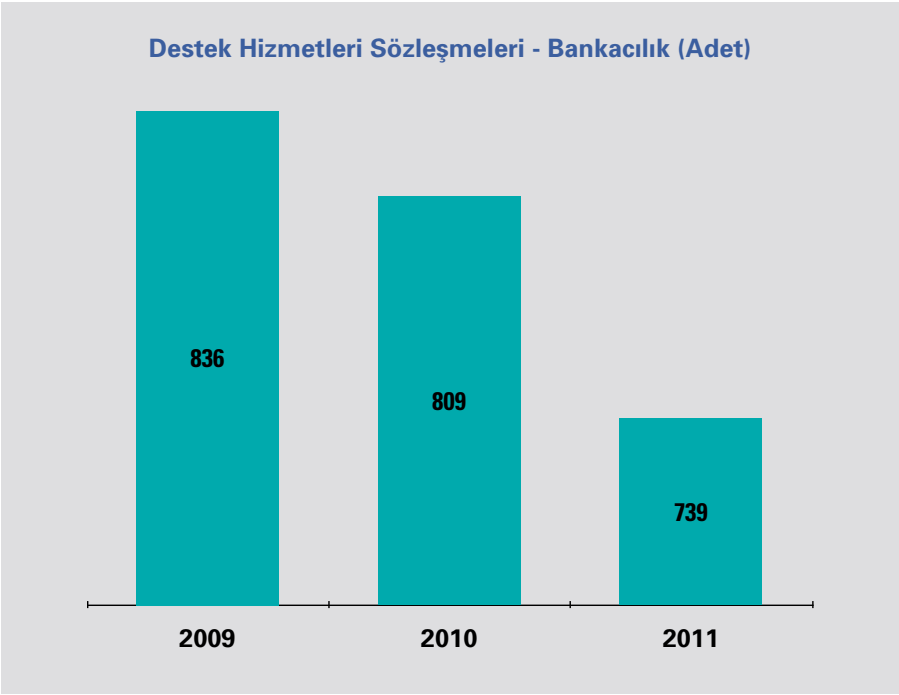
ISAE 3402, bir finansal denetim raporu olmayıp, destek hizmet kuruluşunun finansal durumunu göstermekten ziyade, iç kontrol ortamına ilişkin bağımsız denetim sonucu güvence sunmayı amaçlamaktadır. İlgili rapor, destek hizmetini temin eden kuruluşun talebi ve belirlediği kapsam doğrultusunda, tedarikçi tarafından seçilen bağımsız denetçi tarafından hazırlanır ve tedarikçinin iç kontrol ortamına güvence sunacak şekilde raporlanır.

Bankacılık ve finans sektöründe faaliyet gösteren destek hizmet kuruluşlarını etkileyen düzenlemelerin, kısa ve orta vadede bankaların destek hizmeti kullanımına yöneldikleri bu dönemde artması, sektörde yapılan toplam anlaşmaların ve destek hizmetleri sunan firma çeşitliğinin azalmasına; büyük ölçekli destek hizmet firmalarına ise bağımlılığın artmasına sebebiyet vermektedir.

Birden fazla firmaya hizmet veren destek hizmet kuruluşları için, hizmet alan firmalar ve denetçileri tarafından gerçekleştirilen denetimlerde, hem destek hizmet kuruluşları, hem de ilgili firmalar açısından verimlilik ve maliyet avantajı sağladığı için ISAE 3402 standardının yaygın bir kullanım alanı bulduğu görülmektedir. ISAE 3402 raporu, denetim konusu ("subject matter") kapsamında esnek olup; destek hizmet kuruluşunun kendi finansal verilerinin denetlenmesinden ziyade, destek hizmeti sunulan firmanın finansal raporlama sürecine ve iç kontrol ortamına etkisi olabilecek destek hizmet kuruluşu bünyesindeki insan kaynağı, süreç, sistem ve altyapının denetimini ve raporlanmasını içermektedir.

Ülkemizde yürürlükte olan destek hizmetleri mevzuatı göz önüne alındığında, ISAE 3402 standardının yukarıda bahsedilen özellikleri ve esnek yapısı nedeniyle, destek hizmeti sunan kuruluşların iç kontrol ortamlarının denetlenmesi çerçevesinde kolaylıkla kullanılabileceği düşünülmektedir.

1 Uluslararası Destek Hizmetleri Uygulamaları



Kaynak: FSO Knowledge Exchange. Financial Services Outsourcing Deals – 2011. (2012). Dünya Geneli.

Artan maliyetlerin, yasal uyum gereksinimlerinin ve müşteri odaklı yaklaşımın finansal kuruluşları özellikle de zorlu ekonomik koşullarda, yeni teknolojilere ve çalışma şekillerine karşı daha esnek ve hızlı olmaya zorlaması sonucu hizmet alımlarında bir azalmanın gerçekleştiği düşünülmektedir.

1.1 Finansal Kuruluşlarda Destek Hizmeti Yönelimleri

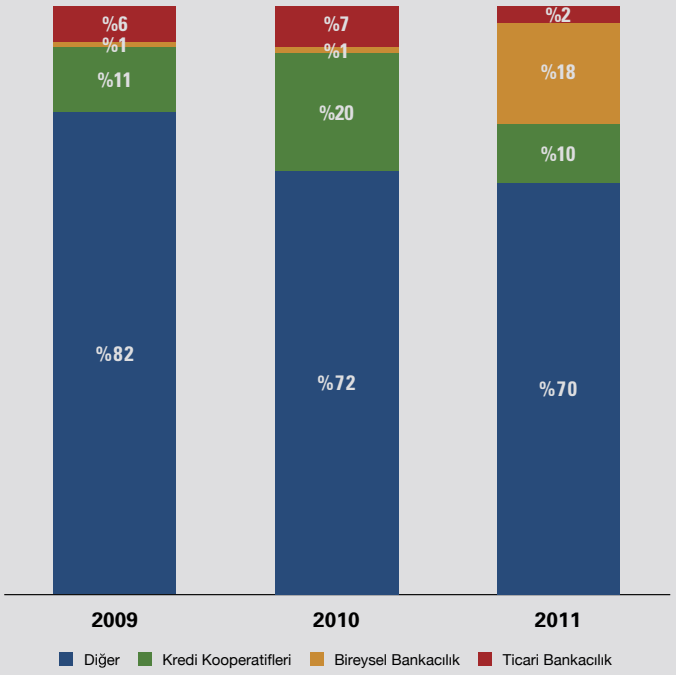
Küresel pazarın en rekabetçi ve en dinamik sektörlerinden biri olan finansal hizmetler sektörü de tıpkı diğerleri gibi, değişen ve gittikçe artan yasal düzenlemelere uyum, pazara adaptasyon, müşteri ihtiyaçlarını karşılama ve maliyetleri azaltma gibi amaçlar doğrultusunda var olan iş, operasyonel ve bilgi sistemleri süreçlerini ve dış kaynak kullanım stratejilerini belirlemektedir.

Bankacılık sektörü de bu değişimin bir parçası olmuş ve 2011 yılında dış kaynaklardan temin edilen hizmetlere istinaden yapılan sözleşmelerin sayısı 2010 ve 2009 yıllarına kıyasla düşüş yaşamıştır. Bununla birlikte, bankacılık sektöründe yapılan sözleşmelerin ortalama tutarlarında artış olduğu gözlemlenmektedir.

Banka türleri özelinde dış kaynaklardan alınan hizmet dağılımlarına bakıldığında, ticari ve bireysel bankacılık tarafında yapılan dış kaynak sözleşmelerinde azalan bir eğilim gözlemlenmekle birlikte 2011 yılına girildiğinde bireysel bankacılık tarafında artış olduğu gözlemlenmektedir.

Son dönemlerde artan maliyetlerin, yasal uyum gereksinimlerinin ve müşteri odaklı yaklaşımın finansal kuruluşları özellikle de zorlu ekonomik koşullarda, yeni teknolojilere ve çalışma şekillerine karşı daha esnek ve hızlı olmaya zorlaması sonucu hizmet alımlarında bir azalmanın gerçekleştiği düşünülmektedir.

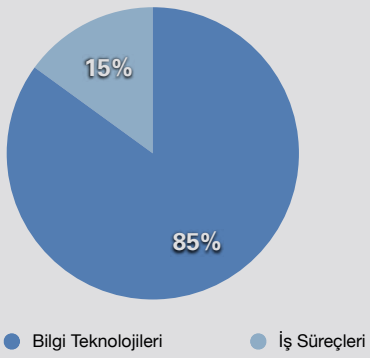
Destek Hizmetleri Sözleşmeleri - Bankacılık Sektörü



Kaynak: FSO Knowledge Exchange. Financial Services Outsourcing Deals – 2011. (2012). Dünya Geneli.

Bankaların bilgi teknolojileri alanındaki dış kaynak kullanımı, iş süreçleri alanındaki kullanımın önemli derecede üstünde kalmaktadır.

Destek Hizmetleri Kullanım Alanı

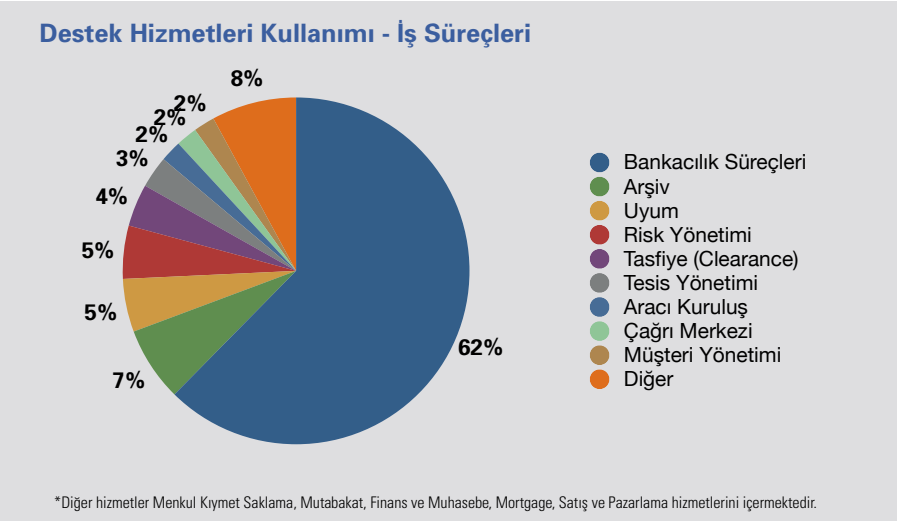


2011 yılında bankaların bilgi teknolojileri alanındaki dış kaynak kullanımı, iş süreçleri alanındaki kullanımın önemli derecede üstünde kalmaktadır.

Bilgi teknolojilerine ilişkin süreçlerin dışarıdan temin edilmesinin temel nedenlerinin; maliyetlerin azaltılması ve iç kaynak kullanımının verimliliğinin artırılması olduğu düşünülmektedir.

Kaynak: FSO Knowledge Exchange. Financial Services Outsourcing Deals – 2011. (2012). Dünya Geneli.

2011 yılında iş süreçleri dikkate alındığında, dış kaynak kullanımının özellikle bankacılık süreçleri kırılımında yoğunlaştığı gözlemlenmektedir. Bankaların son dönemlerde özellikle üzerinde durduğu uyum ve risk yönetimi konularının da öne çıkan başlıklar arasında olduğu ancak toplam dış kaynak kullanım pastasında %5 ile sınırlı kalma nedeninin bu alandaki bağlayıcı yasal mevzuatların olduğu düşünülmektedir.

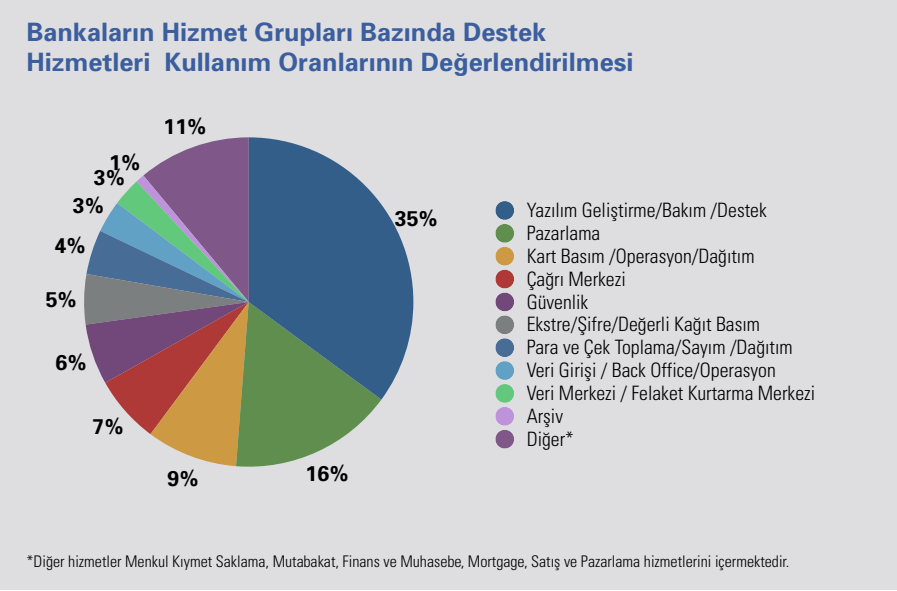


Kaynak: FSO Knowledge Exchange. Financial Services Outsourcing Deals – 2011. (2012). Dünya Geneli.

1.2 Türkiye'deki Destek Hizmeti Yönelimleri

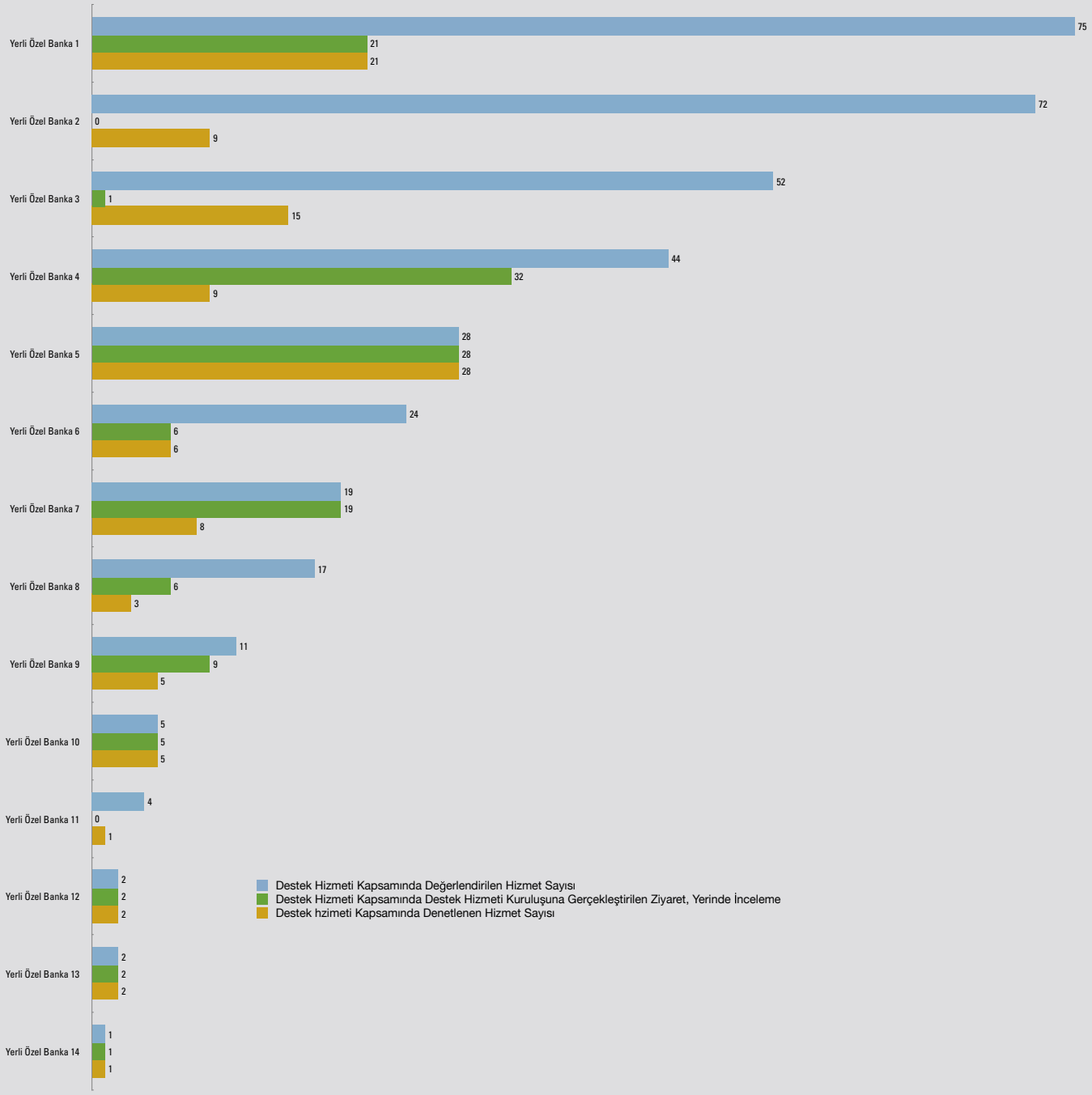
Türkiye Bankalar Birliği tarafından birliğin üyesi olan bankalara gönderilen ve 24 bankanın katılım sağladığı, bankalardaki destek hizmetleri yönelimini ölçme amacı taşıyan çalışmanın sonuçları aşağıda yer almaktadır:

Bankaların almakta olduğu destek hizmetlerinin dahil olduğu hizmet grupları incelendiğinde, alınan hizmetler arasında %35 ile en yoğun hizmet kullanımının yazılım geliştirme, bakım ve destek hizmetlerinde olduğu görülmektedir. Bu hizmetin ardından %16 ile pazarlama hizmetleri, %11 ile sunulan kategorilere girmeyen diğer hizmetler, %9 ile kart basım, operasyon, dağıtım ve %7 ile çağrı merkezi hizmetleri gelmektedir.



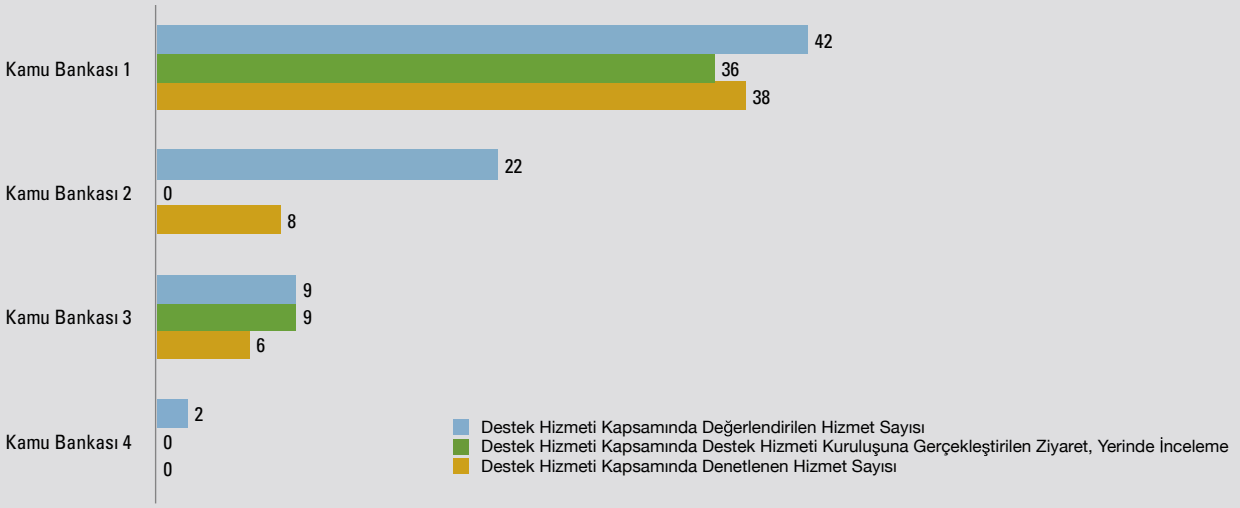
Yerli özel bankaların genel olarak destek hizmetleri kapsamına aldığı hizmetlerin tümünü denetlemediği, yerli özel bankalar tarafından hizmet firmalarında gerçekleştirilen denetim sayısının, destek hizmeti kapsamına aldığı toplam hizmet sayısına oranının %32.3 olduğu gözlemlenmiştir. Denetim hizmeti kapsamında denetlenen kuruluşlara ziyaret, yerinde değerlendirme ve incelemenin, bankalar tarafından kapsama alınan hizmetlere oranının %37.7 olduğu belirlenmiştir.

Yerli Özel Bankalar
Destek Hizmetleri Anket Sonuçları



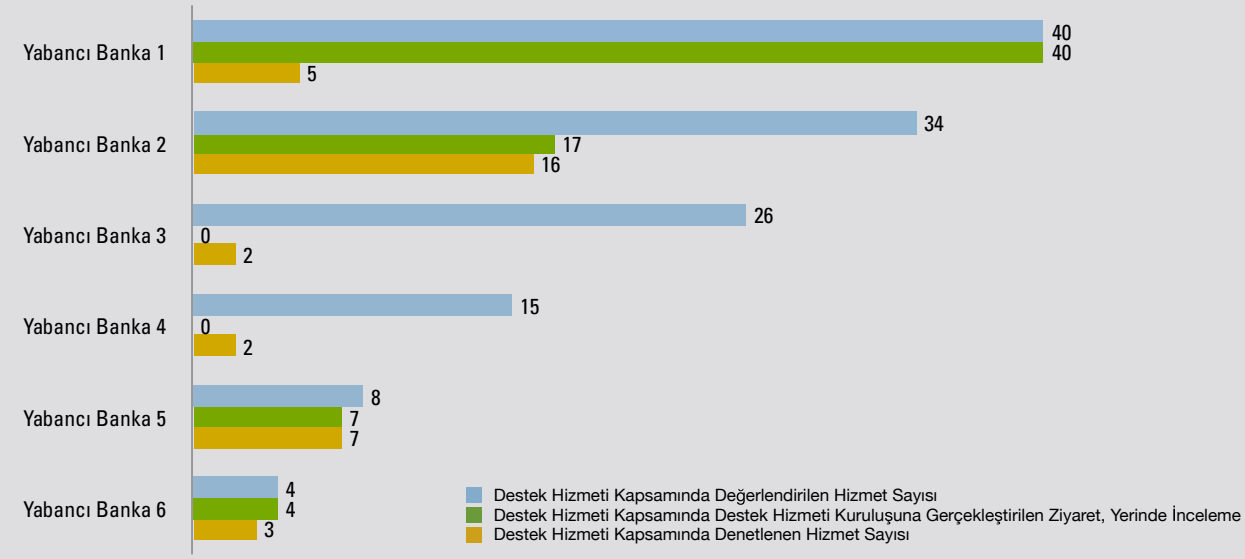
Kamu bankaları tarafından hizmet sunan firmalarda gerçekleştirilen denetim sayısının, destek hizmeti kapsamına alınan toplam hizmet sayısına oranının %65 olduğu gözlemlenmiştir. Denetim hizmeti kapsamında denetlenen kuruluşlara ziyaret, yerinde değerlendirme ve incelemenin, bankalar tarafından kapsama alınan hizmetlere oranının %57.5 olduğu belirlenmiştir.

Kamu Bankaları
Destek Hizmetleri Anket Sonuçları



Yabancı bankalar tarafından hizmet sunan firmalarda gerçekleştirilen denetim sayısının, destek hizmeti kapsamına alınan toplam hizmet sayısına oranının %27,5 olduğu gözlemlenmiştir. Denetim hizmeti kapsamında denetlenen kuruluşlara ziyaret, yerinde değerlendirme ve incelemenin, bankalar tarafından kapsama alınan hizmetlere oranının %53,5 olduğu belirlenmiştir.

Yabancı Bankalar
Destek Hizmetleri Anket Sonuçları



1.3 Destek Hizmetleri Yönetimi ile ilgili Düzenlemeler

Bu başlık altında, destek hizmetleri yönetimi ve düzenlemeleri çerçevesinde, araştırma raporunda yer alan ülkelere genel bir bakış ve karşılaştırma yapılmaktadır. Destek hizmetleri mevzuatı ve uygulamalar ile ilgili detay bilgilere ülkeler bazında raporun 1.4 başlığı altında yer verilmiştir.

Araştırma raporu kapsamında seçilmiş ülkeler, söz konusu ülkelerde banka ve finansal kuruluşlar üzerinde düzenleyici otoriteler ve bu düzenleyici otoriteler tarafından yayımlanmış ve destek hizmetleri kullanımı ile ilgili yasal düzenlemelere ilişkin özet bilgiye Tablo 1'de yer verilmiştir.

Ülkelerde destek hizmeti firmalarının denetimi konusunda hükümler barındıran yasal düzenlemeler hakkında özet bilgiye Tablo 2'de yer verilmiştir.

Sözleşme Maddeleri: Destek hizmeti firması ile banka arasında yapılacak olan sözleşmeye, bilgiye ve belgeye erişim hakkı (Erişebilirlik) ve firmayı yerinde veya uzaktan inceleme/ denetleme hakkı (Denetlenebilirlik) maddelerinin sözleşmeye eklenmesine ilişkin hükümler.

Denetim Hakkı: Destek hizmeti firmasında yapılacak olan denetim haklarının düzenleyici otoriteye, bankaya veya bankanın bağımsız denetçisine verilmesine ilişkin hükümler.

Destek Hizmeti Firmasının Bağımsız Denetçisi: Bankanın, destek hizmeti firmasının bağımsız denetçisi tarafından gerçekleştirilen denetim faaliyetlerini kullanabilmesine ilişkin hükümler. Almanya, ABD ve Birleşik Krallık'ta, ülke mevzuatlarında açık olarak bağımsız denetçi raporlarının kullanılabilmesiyle ilgili bir hüküm bulunmamasına karşın uygulamada bu durumu engelleyen bir hüküm de bulunmamaktadır ve bu ülkelerde fiili olarak bağımsız denetim raporları kullanılabilmektedir.

Ülke	Düzenleyici Otorite	Düzenleme
Almanya	BAFIN (German Federal Supervisory Authority)	Circular 11/2010 (BA) BDSG (German Federal Data Protection Act)
Amerika Birleşik Devletleri	FFIEC (The Federal Financial Institutions Examination Council) FDIC (The Federal Deposit Insurance Corporation) FED (The Federal Reserve Bank of New York)	Supervision of Technology Service Providers (TSP) Booklet Guidance for Managing Third-Party Risk (2008), Third Party Pocedures (2011) FED Cirrucular (Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks)
Avustralya	APRA (The Australian Prudential Regulatory Auhtority)	Outsourcing: Prudential Standards CPS231, Prudential Frameworks (Banking Act 1959)
Birleşik Krallık	FSA (Financial Services Authority)	SYSC 8 (Senior Management Arrangements, Systems and Controls)
İsviçre	FINMA (Swiss Financial Market Supervisory Authority)	Circular 08/7
Türkiye	BDDK (Bankacılık Düzenleme ve Denetleme Kurumu)	Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik

Tablo 1. Düzenleyici Otoriteler ve Yasal Düzenlemeler

Ülke	Sözleşme Maddeleri		Denetim Hakkı			Destek Hizmeti Firmasının Bağımsız Denetçisi
	Erişebilirlik	Denetlenebilirlik	Regülatör	Banka	Bağımsız Denetçi	
Almanya	√	√	√	√	√	x
Amerika Birleşik Devletleri	√	x	√	√	√	x
Avustralya	√	√	x	√	√	√
Birleşik Krallık	√	x	√	√	√	x
İsviçre	√	√	√	√	√	√
Türkiye	√	√	√	√	√	x

Tablo 2. Denetim Hükümleri

Bankacılık, sigortacılık ve sermaye piyasalarının düzenleyici otorite temsilcilerinden oluşan "The Joint Forum" tarafından, 2005 yılında hazırlanan "Outsourcing in Financial Services" çalışmasında finansal hizmet kuruluşlarının, destek hizmeti kullanımından fayda sağlaması için Tablo 3'te bahsedilen risklerin etkin olarak yönetilmesi gerektiği belirtilmiştir.

Risk	Başlıca Sorunlar
Stratejik risk	• Destek hizmeti kuruluşunun, hizmeti alan kuruluşun genel stratejik hedefleri ile tutarsız faaliyetleri yürütmesi • Destek hizmeti aktivitelerine ilişkin etkin bir denetim mekanizması kurulamaması • Gözetim faaliyetlerini gerçekleştirilecek yeterli uzmanlığın bulunmaması
İtibar Riski	• Destek hizmeti firmasının düşük kalitede hizmet sağlaması • Müşteri etkileşiminin, hizmet alan kuruluşun genel standartları ile tutarlı olmaması • Destek hizmeti kuruluşunun, hizmet verdiği kuruluşun anlayışıyla (etik veya diğer) uyumlu olmaması
Uyum Riski	• Gizlilik kanunlarına uyulmaması • Tüketici ve sanayi kanunlarına yeteri kadar uyum sağlanmaması • Hizmet sağlayıcı, sistem ve kontrol uyumluluğunun sağlanmaması
Operasyonel Risk	• Teknolojik hataların meydana gelmesi • Yükümlülükleri yerine getirmekte ve çözüm sağlamada finansal kapasitenin yetersiz kalması • Dolandırıcılık veya hata yapılması
Çıkış Stratejisi Riski	• Uygun çıkış stratejilerinin uygulamada olmaması • Personel veya entellektüel birikimin kaybolması nedeniyle hizmetlerin ülkeye geri getirilmemesi
Karşı Taraf Riski	• Uygun olmayan sigortalama veya kredi değerlendirmeleri • Alacakların kalitesinin azalması
Ülke Riski	• Politik, sosyal ve hukuksal iklimin riski artırması • Karmaşık iş sürekliliği planları
Sözleşme Riski	• Ülke dışı hizmet alımlarında uygulanacak yasal mevzuatın seçilmesi
Erişim Riski	• Destek hizmeti firmasının düzenleyicilere veri ve diğer bilgileri zamanında gönderememesi • Destek hizmeti firması tarafından gerçekleştirilen aktivitelerin anlaşılmasının düzenleyici otorite tarafında güçleşmesi
Yoğunlaşma ve Sistemik Riski	• Destek hizmeti firmalarının kendi alanında çok fazla kuruluşa hizmet vermeleri • Destek hizmeti firması üzerinde kontrol sağlanamaması

Tablo 3. The Joint Forum - Destek Hizmeti Riskleri

Almanya'daki yasal mevzuatta destek hizmeti firmalarında gerçekleştirilecek denetime ilişkin haklara yer verilmekle birlikte; denetim faaliyetlerinin nasıl gerçekleştirileceğine ilişkin bir hüküm veya tavsiye bulunmamaktadır.

1.4 Destek Hizmetleri Risk ve Güvence Düzenlemeleri

1.4.1 Almanya

Almanya ulusal kanunları içerisinde destek hizmetleriyle ilgili bir düzenleme bulunmamakla birlikte, destek hizmetleri ile gerçekleştirilen tüm sözleşmelerin Alman Medeni Kanunu ("Bürgerliches Gesetzbuch") dahilinde belirtilen hükümlerle uyumlu olması gerekmektedir.

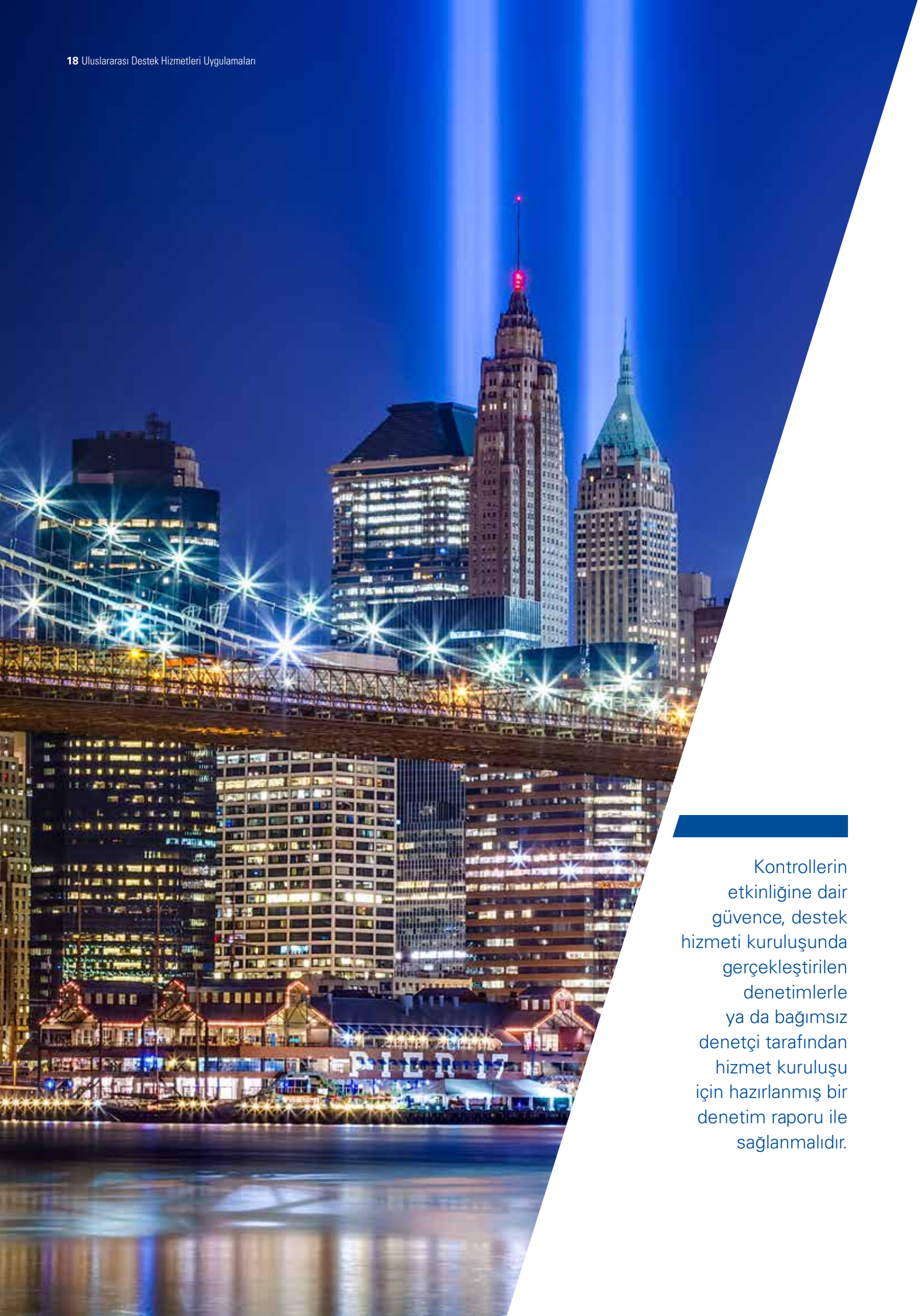
Finansal hizmetler sektörü özelinde, Aralık 2001'de, BaFin tarafından, tüm kredi kuruluşlarını ve finansal hizmet kurumlarını kapsayan Circular 11/2010 (BA) sayılı genelge kapsamında destek hizmetleri yönetimine ilişkin kılavuz ilkeler yayımlanmıştır. Bu kılavuz ile destek hizmetleri firmalarından temin edilen hizmetlerle ilgili gereksinimler tanımlanarak, operasyonel faaliyetlerin dışarıdan temininin; iş veya hizmetlerin düzenliliğini, yöneticilerin bu faaliyetleri yönetme ve izleme kabiliyetini ve BaFin'in kendi yetkisi altındaki kredi kurumlarını denetleme ve izleme yeteneğini zaafa uğratmamasının garanti altına alınması hedeflenmektedir.

Söz konusu genelge kapsamında destek hizmeti alan bankalar ve finans kuruluşları tarafından uyulması gereken asgari yükümlülükler belirtilmektedir:

- Banka ve diğer finansal kuruluşların, kendi risk yönetimi süreçlerine tüm destek hizmeti aktivitelerini dahil etmesi ve uygun denetim ortamını sağlaması gerekmektedir.
- Banka ve diğer finansal kuruluşlar, iç denetim alanında destek hizmeti alınıyorsa, banka ve diğer finansal kuruluşların bu faaliyete ilişkin bir denetim sorumlusu tayin etmeleri beklenmektedir.
- Banka ve finansal kuruluşların, iş sürekliliğini ve kalitesini sağlamak amacıyla destek hizmeti sözleşmesinin feshi halinde izlenecek yolu belirlemeleri gerekmektedir.

Destek hizmeti sunan firma ile yapılacak olan sözleşmeye dahil edilecek asgari hükümlere bu genelgede yer verilmektedir. Destek hizmeti alan kuruluşun ve bu kuruluşun bağımsız denetçisinin ve BaFin'in denetim haklarının korunması denetim anlamında öne çıkan sözleşme maddeleri arasındadır. Bunlara ek olarak, veri gizliliği ve güvenliği, yasal mevzuata uyum ve fesih hakları gibi hususların da sözleşmede asgari hükümler başlığı altında incelenmektedir.

Almanya'daki yasal mevzuatta yukarıda belirtildiği üzere destek hizmeti firmalarında gerçekleştirilecek denetime ilişkin haklara yer verilmekle birlikte; denetim faaliyetlerinin nasıl gerçekleştirileceğine ilişkin bir hüküm veya tavsiye bulunmamaktadır. Destek hizmetleri kuruluşlarının iç kontrol ortamlarına güvence verme amacıyla Alman Denetçiler Enstitüsü ("Institut der Wirtschaftsprüfer") tarafından ISAE 3402 tabanlı bir ulusal denetim ve güvence standardı olan IDW PS 951 yayımlanmıştır. Söz konusu standart, ülkede kabul görmekte ve finansal kuruluşlar tarafından itibar edilmektedir.



Kontrollerin etkinliğine dair güvence, destek hizmeti kuruluşunda gerçekleştirilen denetimlerle ya da bağımsız denetçi tarafından hizmet kuruluşu için hazırlanmış bir denetim raporu ile sağlanmalıdır.

1.4.2 Amerika Birleşik Devletleri

The Financial Industry Regulatory Authority ("FINRA"), Amerika finansal endüstrisinde yatırımcıları korumayı hedefleyen sistemsel düzenlemeler yapan bir kurumdur. 2011 yılında FINRA tarafından üye kurumları için tedarikçi yönetimine yönelik oluşturulan 3190 isimli yönetmelik hazırlık aşamasında olup tedarikçi firma ve kurum sorumluluklarının yönetimine ilişkin düzenlemeleri içermektedir.

Office of the Controller of the Currency ("OCC"), ulusal bankaları düzenleme ve denetleme yetkisine sahip olan kurumlardan bir diğeri olarak tanımlanmaktadır. OCC tarafından 2000 yılında bütün ulusal bankalara hitaben yayınlanan "Risk Management of Outsourcing Technology Services" konulu tavsiye mektubunda destek hizmeti firmalarından alınan teknoloji hizmetleri ile ilgili risk yönetim unsurları belirlenmiştir.

The Federal Deposit Insurance Corporation ("FDIC"), Amerika'da faaliyet gösteren finansal kurumlara yönelik düzenlemeler gerçekleştiren başka bir kurumdur. Bu kurumun, 2011 yılında yayımlamış olduğu "Third Party Procedures" dokümanında, destek hizmeti yönetimi için yapılması gerekenler dört ana başlık altında incelenmektedir:

1. Risk Değerlendirmesi: Hizmetin türüne göre oluşabilecek risklerin değerlendirilmesi

2. Tedarikçi Firma Durum Tespiti: Teknik yeterlilik, operasyon, kontrol ve finansal durum gibi alanların değerlendirilmesi

3. Sözleşme Düzenlenmesi ve Gözden Geçirilmesi: Sözleşmede tarafların sorumluluk ve haklarının açıkça belirtilmesi

4. Gözetim Programı: Dış kaynak hizmeti sağlayan kuruluşun finansal durumunun, sözleşmeye uyumun ve yenileme gerekliliklerinin ve süreklilik planlarının değerlendirilmesi

Bu doküman içerisinde, FDIC tarafından finansal kurumlara ve bankalara uygulanan bir kontrol tablosu bulunmaktadır ve söz konusu tabloda yer alan kontrol sorularına verilen cevaplara göre FDIC tarafından kuruluşlara para cezası uygulanabileceği hükmü yer almaktadır.

FDIC tarafından yayınlanan ilgili dokümanda, tedarikçi firma olarak belirtilen firmaların yurt içi ve yurt dışı farkı gözetmeksizin ilgili risk yönetim düzenlemelerine tabi tutulması gerekliliği bildirilmekte ve hizmet alımında göz önünde bulundurulması gereken riskler; stratejik, itibar, faaliyet, işlem ve kredi riskleri olarak sınıflandırılmaktadır. Buna ek olarak, teknik yeterlilik yönetiminin yapılması ile ilgili gerekliliklerin tedarikçi firma durum tespiti sırasında oluşturulması gerektiği belirtilmiştir. Teknik yeterlilik ve risklerin hizmet alım süresi boyunca belirli periyotlarla izlenmesi gerekliliği "Oversight" alt başlığında incelenmiş ve hizmet alan kurum tarafından destek hizmeti firmasının teknik yeterliliğinin izlenmesi şart koşulmuştur.

The Federal Financial Institutions Examination Council ("FFIEC"), tarafından yayınlanan "Supervision of Technology Service Providers ("TSP") Booklet" dokümanında teknoloji hizmeti sunan firmaların risk yönetimi kapsamında denetim sorumlulukları belirtilmiş ve denetim periyotlarının kılavuzda belirtildiği şekilde kritiklik değerlendirmesinin sonucunda belirlenmesi gerektiği vurgulanmıştır.

The Federal Reserve Bank of New York tarafından 1999 yılında yayımlanan "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks" dokümanında risk yönetiminde öne çıkan başlıklar incelenmektedir.

Ülkede, destek hizmeti firması denetimi ve güvence uygulamalarına ilişkin hükümlerin bulunduğu yasal bir mevzuat bulunmamakla birlikte; American Institute of CPAs ("AICPA") tarafından hazırlanmış ve ISAE 3402 tabanlı ulusal bir denetim ve güvence standardı olan SSAE 16 yaygın olarak kullanılmaktadır.

Public Company Accounting Oversight Board ("PCAOB"), tarafından yayımlanmış olan AS5 numaralı denetim standardına göre denetçilerin, destek hizmeti kuruluşunun ve hizmet alan kuruluşun kontrol ortamını anlaması ve denetçinin görüşüne temel teşkil eden kontrollerin etkinliğine dair kanıtlar elde etmesi gerekmektedir. Bu standarda göre kontrollerin etkinliğine dair güvence, destek hizmeti kuruluşunda gerçekleştirilen denetimlerle ya da bağımsız denetçi tarafından hizmet kuruluşu için hazırlanmış bir denetim raporu ile sağlanmalıdır.

Mevduat kuruluşu bünyesinde yapılan denetim çalışmalarına ilişkin raporların APRA tarafından kullanılabilir şekilde hazırlanması ve çalışma bedelinin mevduat kuruluşu tarafından ödenmesi beklenmektedir.

1.4.3 Avustralya

Avustralya'da destek hizmeti alımlarını düzenlemek amacıyla, bankacılık kanunu ("Banking Act 1959") dahilinde; The Australian Prudential Regulatory Authority ("APRA") tarafından; mevduat kuruluşları, genel sigorta şirketleri ve hayat sigortası şirketlerini kapsayan "Prudential Standards CPS231" isimli bir çerçeve düzenleme oluşturulmuştur. Söz konusu çerçeve 2013 yılında yayımlanmış olup; Bankacılık Kanunu 11AF maddesi ile yasal zorunluluk haline getirilmiştir.

CPS231 çerçevesi kapsamında; destek hizmeti kullanım politikası, firma seçimi, sözleşme, ülke dışından alınan hizmetlere ilişkin düzenlemeler, APRA'ya bildirim şartları, destek hizmeti sunan firmalarının takibi ve denetimi gibi konulara yer verilmiştir.

Buna ek olarak, APRA tarafından destek hizmeti kullanımı alanındaki çerçeveye uyum sağlama ve destek hizmeti kullanımının yönetilmesi amacıyla kullanılacak olan yasal uyum gerektirmeyen kılavuz niteliğinde, "Prudential Practice Guide" isimli bir doküman yayımlanmıştır. Söz konusu kılavuz dahilinde, anlaşmalarda göz önünde bulundurulması gereken maddeler, ülke dışından destek hizmeti kullanımı ve firma ilişkilerinin kontrolü ve yönetimi gibi başlıklara yer verilmiştir.

Destek hizmeti kullanımına ilişkin risk unsurlarına "Prudential Standards CPS231" standardı ve "Prudential Practice Guide" kılavuzları kapsamında yer verilmiştir. Söz konusu riskler firma seçimi ve yönetimi bazında incelenmiştir.

Risk yönetimi kapsamında yer alan talimatlara aşağıda yer verilmiştir:

- Destek hizmeti alımına ilişkin yönetim tarafından onaylanmış bir politika oluşturulmalı ve söz konusu politika destek hizmeti firmalarından temin edilecek hizmetlere ilişkin bütün riskleri içermelidir.

- Mevduat kuruluşu, destek hizmeti alımına ilişkin risklerin değerlendirilebilmesi kapsamında, sözleşme taraflarının ve ilgili donanıma sahip diğer kişilerin bulunduğu bir çalışma grubu kurması tavsiye edilmektedir. Söz konusu çalışma grubunun, yönetim onaylı destek hizmetleri politikasının destek hizmetleri süreçlerinde (teklif, değerlendirme, geliştirme, üst yönetime önerilerin sunulması vb.) izlenmesini sağlaması önerilmektedir.

- Mevduat kuruluşu, APRA'ya sözleşmede yer alan anahtar risklerin ve söz konusu risklere ilişkin risk azaltma stratejilerinin yer aldığı bir özet sağlamalıdır. APRA, anlaşmanın etkilerini anlayabilmek ve değerlendirebilmek adına gerekli gördüğü durumda ek kaynak talep etme hakkına sahiptir.

Ülke dışından destek hizmeti kullanımına gidilmesi durumunda ortaya çıkan riskler; ülke riski, uyum riski, sözleşme riski ve karşı taraf riski olarak belirtilmiş olmakla birlikte, bu riskleri bertaraf etme amaçlı sözleşmeye eklenmesi gereken ek şartlar; geçerli olan yasal hükümlerin seçimi, bilgi gizliliği ve güvenliği ve bilgiye erişim olarak belirlenmiştir.

CPS231 standardında, destek hizmeti sunan firmalardan hizmet alınmadan önce hizmete ilişkin bir sözleşmenin hazırlanması ve imzalanması gerektiği belirtilmiş ve sözleşmede yer alması gereken asgari unsurlara yer verilmiştir. Denetleme ve izleme prosedürü, sözleşme kapsamı, hizmet seviyesi ve performans hükümleri, başlangıç ve bitiş tarihleri, iş sürekliliği yönetimi, bilgi gizliliği ve güvenliği ile sorumluluk ve tazminat hususları standart tarafından beklenen sözleşme maddeleridir.

CPS231 kapsamında destek hizmeti firmalarının ve sağladıkları hizmetlerin denetimine ilişkin bilgilere de yer verilmektedir:

APRA, mevduat kuruluşu dış denetçisinden veya bağımsız bir uzmandan önemli iş faaliyetlerine ilişkin destek hizmetleri düzenlemeleri ile ilgili risk yönetim süreçlerinin değerlendirilmesi için talepte bulunma hakkına sahiptir. Söz konusu değerlendirme; bilgi sistemleri, bilgi gizliliği, iç kontrol çerçeveleri ve iş sürekliliği planları alanlarını kapsayabilir. Bu tür çalışmaların bedelinin mevduat kuruluşu tarafından ödenmesi ve söz konusu raporların APRA tarafından kullanılabilir şekilde hazırlanması beklenmektedir.

İç denetim fonksiyonunun, önemli destek hizmetlerine ilişkin faaliyetleri kapsaması ve mevduat kuruluşunun standartta altı çizilmiş olan destek hizmetlerine ilişkin politikaya uyumunu değerlendirmesi ve Yönetim Kurulu'na raporlaması beklenmektedir.

Avustralya'da denetim standartları düzenleyen kuruluş "Auditing and Assurance Standards Board ("AUASB")'dir. AUASB tarafından destek hizmetleri denetimi kapsamında yer alan standartlar "Auditing Standard ASA 402 Audit Considerations Relating to an Entity Using a Service Organisation" ve ASAE 3402 (Assurance Reports on Controls at a Service Organisation)'dir. ASAE 3402 standardı, ISAE 3402 tabanlı ulusal bir standart olup ISAE 3402'ye ek maddeler içermektedir. AUASB tarafından ASAE 3402 ile uyum sağlamış firmalar ISAE 3402 ile uyum sağlamış olarak kabul edilmekte olup; tersi geçerli olmamaktadır.


LEFT ONLY

Alınan hizmetin zayıf kalması, kesintiye uğraması veya başarısız olması durumunda bankanın faaliyetlerinin asgari düzeyde devamının sağlanıp sağlanamayacağı hususunda ciddi şüpheler doğuyorsa, bu hizmet önemli bir destek hizmetidir.

1.4.4 Birleşik Krallık

Financial Services Authority ("FSA"), finansal piyasalarda hizmet veren şirketler ve borsa için standartları belirlemek ve denetlemek amacıyla kurulmuş bağımsız bir kuruluştur. Destek hizmetleri ile ilgili FSA tarafından yayımlanan ilkeler, Senior Management Arrangements, Systems and Controls ("SYSC8") adlı kılavuzda yer almaktadır.

FSA, destek hizmeti firmalarının değerlendirmesi aşamasında önemlilik ve kritiklik kıstasını "Alınan hizmetin zayıf kalması, kesintiye uğraması veya başarısız olması durumunda bankanın faaliyetlerinin asgari düzeyde devamının sağlanıp sağlanamayacağı hususunda ciddi şüpheler doğuyorsa önemli bir destek hizmetidir." şeklinde tanımlamaktadır. Bu tanımlamaya ek olarak, standartlaşmış hizmetler, telekomünikasyon ve danışmanlık hizmetleri gibi konular da kılavuz kapsamı dışında bırakılmıştır.

Kritik ve önemli operasyonel fonksiyonların ya da ilgili hizmet ve aktivitelerin destek hizmeti kuruluşlarından temin edilmesi durumunda sağlanması gereken koşullar belirlenmiş olup; tarafımızca önemli bulunan hususlara aşağıda yer verilmiştir:

• Destek hizmeti firmasının, tedarik edilen fonksiyonlarının, hizmetlerinin ya da aktivitelerinin güvenilebilir ve profesyonel olması için yeterli kapasiteye sahip olması ve ilgili yasalarla uyumlu olması gerekmektedir.

• Destek hizmeti firmasının, felaket kurtarma planının ve yedeklerinin periyodik olarak gözden geçirilmesi için bir süreklilik planı kurması, uygulaması ve devam ettirmesi gerekmektedir.

• Destek hizmeti firmasının, müşterilerine ait gizli bilgileri koruması beklenmektedir.

• Destek hizmeti firmasının mevzuata uyumsuz olması durumunda finansal kuruluş tarafından gereken aksiyonların alınması gerekmektedir.

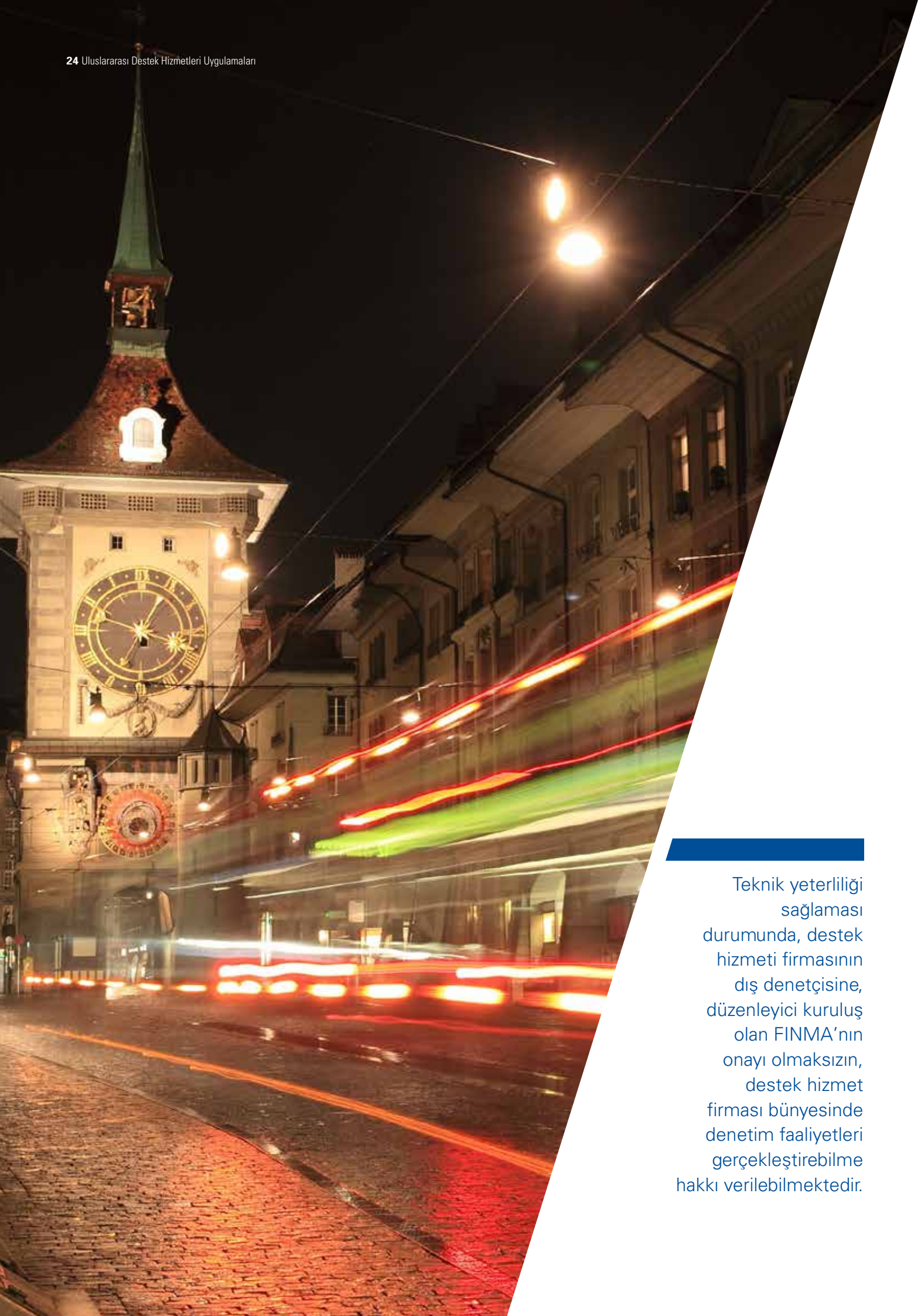
• Destek hizmeti firmasının, sağladığı hizmet üzerinde etkisi olabilecek önemli değişiklik ve geliştirmeleri hizmet sunduğu finansal kuruluşa bildirmesi gerekmektedir.

• Hizmet alan kuruluşun, destek hizmeti firmasının faaliyetlerini ve bunlara ilişkin riskleri gözetebilecek uzmanlığı edinmesi gerekmektedir.

• Hizmet alan kuruluşun, gerekli durumlarda destek hizmeti firmasından aldığı hizmeti, kendi müşterilerine sunduğu hizmetin kalitesini ve sürekliliğini sekteye uğratmayacak şekilde sonlandırabiliyor olması gerekmektedir.

Destek hizmetleri firması ile imzalanan sözleşmelerde, firmadan talep edilebilecek raporlama ve bilgilendirme gereksinimlerine ve firmaların iç ve dış denetçilerinin erişimlerine açık olmasına ilişkin hükümlerin yer alması gerektiği FSA tarafından bildirilmektedir.

Ülkede destek hizmetleri firmalarından alınan hizmetlerin denetlenmesine ve raporlanmasına ilişkin yönetmelik bazında bir düzenleme bulunmamasına karşın, Institute of Chartered Accountants in England and Wales ("ICAEW") tarafından ISAE 3402 temel alınarak hazırlanmış olan raporlama standardı yaygın olarak kullanılmakta ve bu raporlara finansal kuruluşlar tarafından itibar edilmektedir.



Teknik yeterliliği sağlaması durumunda, destek hizmeti firmasının dış denetçisine, düzenleyici kuruluş olan FINMA'nın onayı olmaksızın, destek hizmet firması bünyesinde denetim faaliyetleri gerçekleştirebilme hakkı verilebilmektedir.

Ülke mevzuatı gereğince, hizmet alım süresi boyunca teknik yeterlilik ve riskler anlamında alınan önlemlerin periyodik olarak gözden geçirilmesi gerekmektedir.

1.4.5 İsviçre

Destek hizmetleri kapsamında, bankalar üzerinde geçerli olan mevzuat, FINMA Circular 08/7, the Swiss Financial Market Supervisory Authority ("FINMA") tarafından 2009 yılında yayımlanmıştır.

Kural olarak, her bir iş alanı için destek hizmeti alımı yapılması, FINMA'nın onayı olmadan da mümkündür. Ancak bu prensiple birlikte, 1992'de yayımlanmış olan Veri Gizliliği Hakkındaki Kanun'un 30. ve devam eden maddelerinde belirtilmiş olan güvenli hizmet alımı kurallarına uyulduğu ve yurtdışından hizmet alındığı durumlarda destekleyici dokümanların sağlanması gerektiği kabul edilmektedir.

Tüm destek hizmeti alımlarının, daha önceden belirlenmiş genel şartları asgari olarak sağladığını belirten yazılı sözleşmelere dayandırılması gerekmekte ve iç onay sürecine ek olarak sözleşmenin sonlandırılmasına ilişkin koşul ve gereksinimlerin destek hizmeti alan kuruluş tarafından belirlenmesi beklenmektedir.

Ülke mevzuatı gereğince, hizmet alım süresi boyunca teknik yeterlilik ve riskler anlamında alınan önlemlerin periyodik olarak gözden geçirilmesi gerekmektedir. Buna ek olarak; müşteri verisinin otomatik süreçlerle işlendiği durumlarda, destek hizmeti kuruluşlarının fiziksel ve mantıksal erişim noktaları ile veri taşıma, depolama, kullanma süreçlerini kontrol etmek amacıyla gerekli teknik ve kurumsal önlemlerin banka tarafından alınması beklenmektedir.

İsviçre'de bankacılık sektöründe destek hizmeti denetimi ile ilgili düzenlemelere de yukarıda bahsi geçen mevzuat kapsamında yer verilmiştir. Söz konusu mevzuat gereğince; FINMA'nın gözetimine tabi olmayan bir destek hizmeti kuruluşunun, banka ile yapılan sözleşme çerçevesinde; gözetim aktivitesi için gerekli olan ve hizmeti alınan iş sahası ile alakalı tüm bilgi ve belgeleri FINMA'ya sunmayı kabul etmesi gerekmektedir. Buna ek olarak, destek hizmeti firmasının, denetim faaliyetinin destek hizmetleri kuruluşunun denetçisi tarafından yürütülmesi durumunda, talep edildiği durumlarda denetim raporunu, FINMA ve hizmeti alan kuruluşun iç ve dış denetim şirketine sunması gerekmektedir.

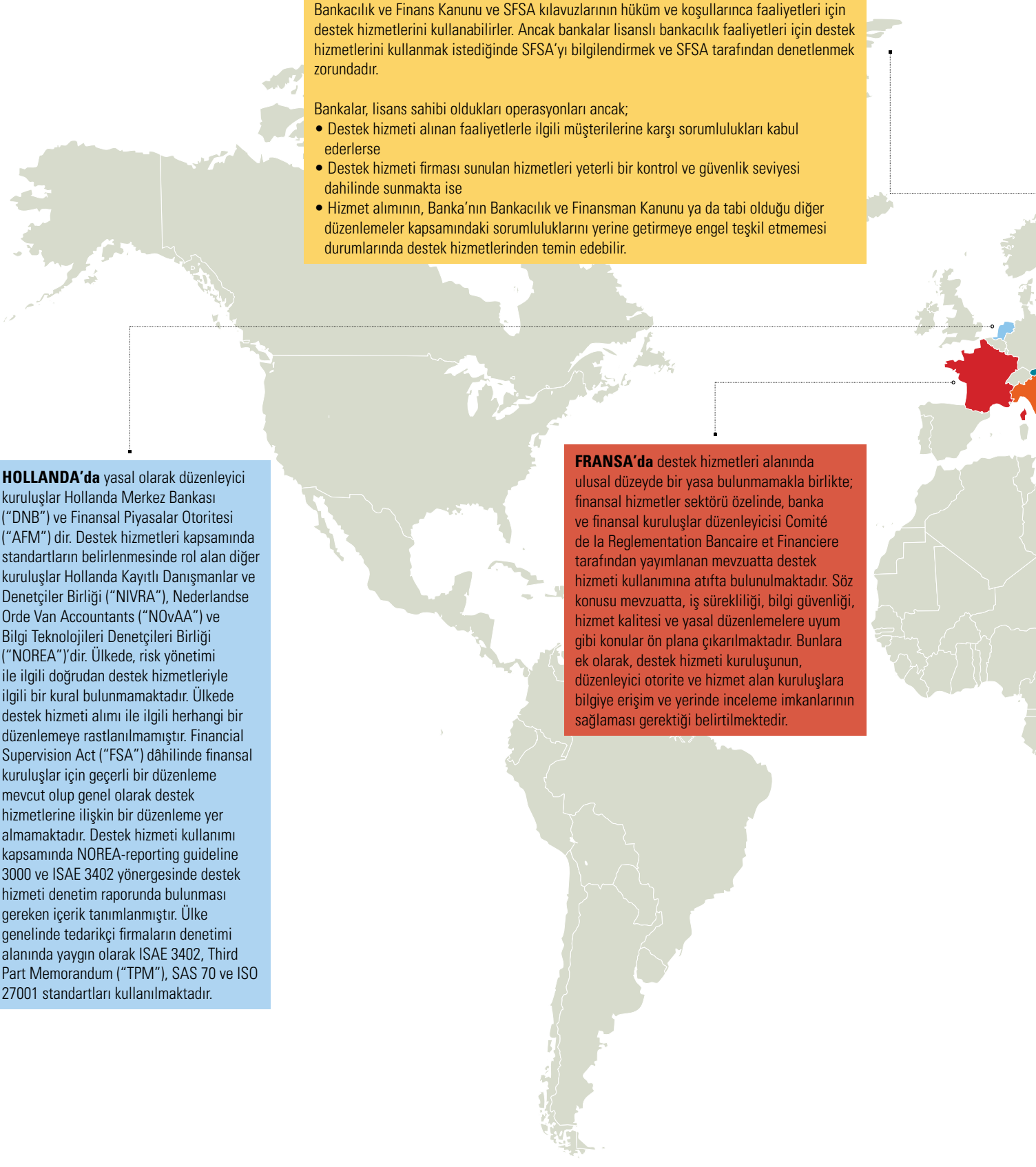
Destek hizmeti alan bankanın iç denetim birimleri, banka ile anlaşmalı dış denetim şirketi ve FINMA, destek hizmeti alınan firmada her zaman sınırsız inceleme ve tetkik hakkını korumalıdır. FINMA, destek hizmeti firmasının bankacılık ve menkul kıymet borsası yasalarına uyumluluğunu denetleme hakkını bankanın iç ve dış denetçilerine vermektedir. Buna ek olarak; teknik yeterliliği sağlaması durumunda destek hizmeti firmasının dış denetçilerine de söz konusu denetim faaliyetlerini gerçekleştirme hakkı verilmektedir. Bu faaliyetlerin destek hizmeti firmasının dış denetçileri tarafından yürütülmesi FINMA'nın onayına tabi tutulmamaktadır. Destek hizmetleri kuruluşunun denetçileri tarafından gerçekleştirilen denetim faaliyetleri İsviçre yasalarına uygun ve FINMA Circular 08/7 mevzuatı Madde 10 ve Madde 11'i yerine getirir nitelikte organize edilmiş ise; bankaların iç ve dış denetçileri bu denetim çalışmalarını kullanma hakkına sahiptirler.

1.4.6 Diğer Ülkeler

İSVEÇ'te finansal hizmetler sektöründe destek hizmetleri kapsamında yürürlükte olan temel yasalar: Banking and Financing Business Act (SFS 2004:297), Investment Funds Act (SFS 2004:46), Securities Market Act (SFS 2007:528) olarak dikkate alınmaktadır. Ülkede düzenleyici otoritelerden biri olan kurum The Swedish Financial Supervisory Authority'nin ("SFSA") destek hizmetlerine ilişkin kural ve kılavuzları bulunmaktadır. Bankacılık ve Finans Kanunu ve SFSA kılavuzları İsveç ve dış ülke kuruluşlarını kapsamaktadır. Bankalar, Bankacılık ve Finans Kanunu ve SFSA kılavuzlarının hüküm ve koşullarınca faaliyetleri için destek hizmetlerini kullanabilirler. Ancak bankalar lisanslı bankacılık faaliyetleri için destek hizmetlerini kullanmak istediğinde SFSA'yı bilgilendirmek ve SFSA tarafından denetlenmek zorundadır.

Bankalar, lisans sahibi oldukları operasyonları ancak;

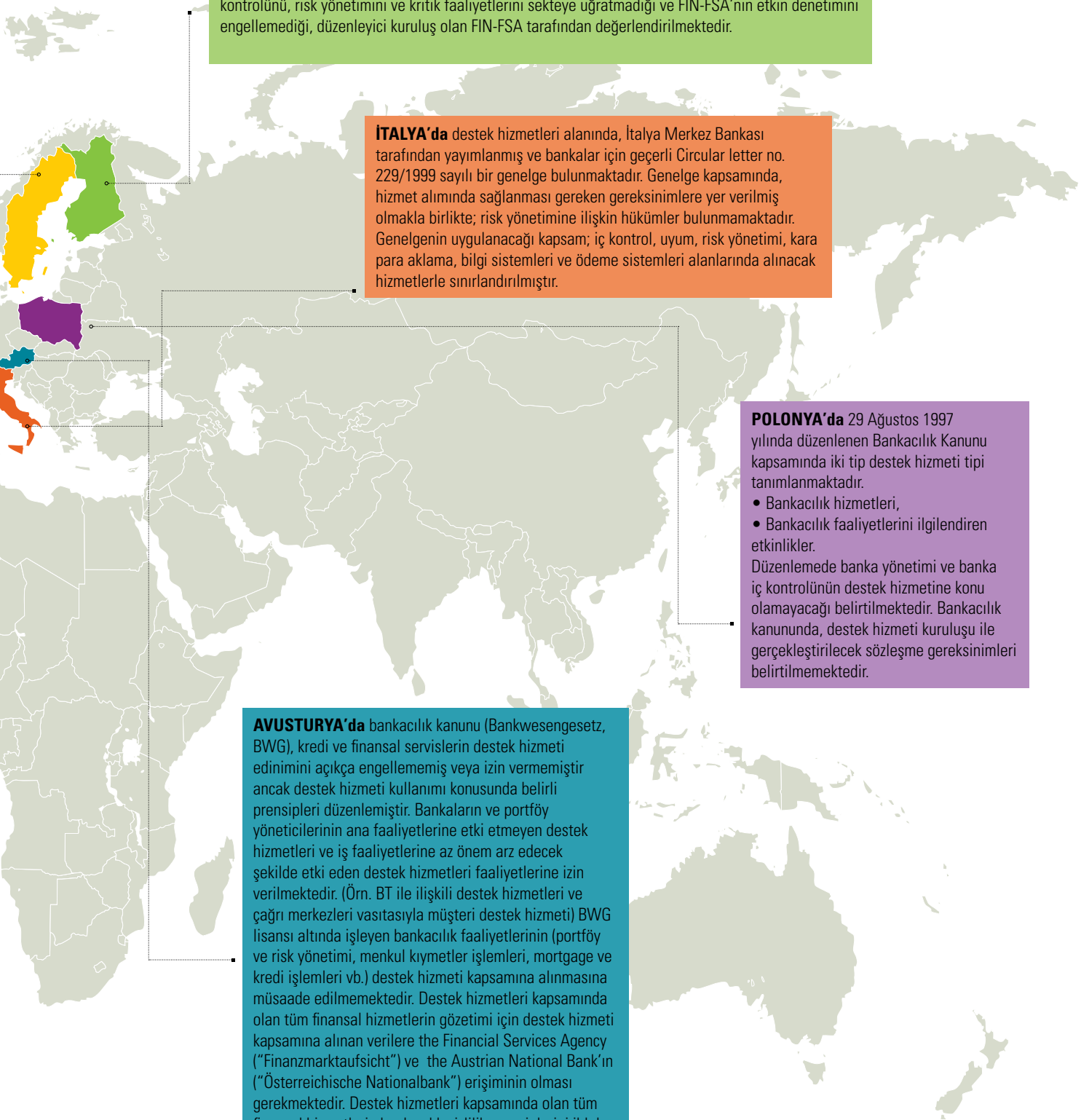
- Destek hizmeti alınan faaliyetlerle ilgili müşterilerine karşı sorumlulukları kabul ederlerse
- Destek hizmeti firması sunulan hizmetleri yeterli bir kontrol ve güvenlik seviyesi dahilinde sunmakta ise
- Hizmet alımının, Banka'nın Bankacılık ve Finansman Kanunu ya da tabi olduğu diğer düzenlemeler kapsamındaki sorumluluklarını yerine getirmeye engel teşkil etmemesi durumlarında destek hizmetlerinden temin edebilir.



HOLLANDA'da yasal olarak düzenleyici kuruluşlar Hollanda Merkez Bankası ("DNB") ve Finansal Piyasalar Otoritesi ("AFM") dir. Destek hizmetleri kapsamında standartların belirlenmesinde rol alan diğer kuruluşlar Hollanda Kayıtlı Danışmanlar ve Denetçiler Birliği ("NIVRA"), Nederlandse Orde Van Accountants ("NOvAA") ve Bilgi Teknolojileri Denetçileri Birliği ("NOREA")'dir. Ülkede, risk yönetimi ile ilgili doğrudan destek hizmetleriyle ilgili bir kural bulunmamaktadır. Ülkede destek hizmeti alımı ile ilgili herhangi bir düzenlemeye rastlanılmamıştır. Financial Supervision Act ("FSA") dâhilinde finansal kuruluşlar için geçerli bir düzenleme mevcut olup genel olarak destek hizmetlerine ilişkin bir düzenleme yer almamaktadır. Destek hizmeti kullanımı kapsamında NOREA-reporting guideline 3000 ve ISAE 3402 yönergesinde destek hizmeti denetim raporunda bulunması gereken içerik tanımlanmıştır. Ülke genelinde tedarikçi firmaların denetimi alanında yaygın olarak ISAE 3402, Third Part Memorandum ("TPM"), SAS 70 ve ISO 27001 standartları kullanılmaktadır.

FRANSA'da destek hizmetleri alanında ulusal düzeyde bir yasa bulunmamakla birlikte; finansal hizmetler sektörü özelinde, banka ve finansal kuruluşlar düzenleyicisi Comité de la Reglementation Bancaire et Financiere tarafından yayımlanan mevzuatta destek hizmeti kullanımına atıfta bulunulmaktadır. Söz konusu mevzuatta, iş sürekliliği, bilgi güvenliği, hizmet kalitesi ve yasal düzenlemelere uyum gibi konular ön plana çıkarılmaktadır. Bunlara ek olarak, destek hizmeti kuruluşunun, düzenleyici otorite ve hizmet alan kuruluşlara bilgiye erişim ve yerinde inceleme imkanlarının sağlaması gerektiği belirtilmektedir.

FİNLANDİYA'da finansal hizmetleri düzenleyici otorite olan Financial Supervisory Authority'in ("FIN-FSA") destek hizmetleri ile ilgili yayımladığı Regulations and Guidelines 1/2012 düzenlemesinde destek hizmetleri kapsamına kredi kuruluşları, yatırım firmaları, yönetim şirketleri, borsa, Avrupa Birliği dışındaki yabancı kredi kuruluşlarının Finlandiya şubeleri ve ödeme kuruluşları girmektedir. Destek hizmetlerine konu olan faaliyetlerin sorumluluğu destek hizmeti alan kuruluşa ait olup, destek hizmeti alan kuruluşun iç kontrol ve risk yönetiminin destek hizmeti faaliyetlerinin içerecek şekilde kurgulanması gerekmektedir. Destek hizmeti alan kuruluşun FIN-FSA düzenleyici otoritesine destek hizmeti içeriğinin kritikliğine göre bildirimde bulunması gerekmektedir. Taraflar arası sözleşme içeriğinin ne şartlarda olacağı düzenlemede belirtilmektedir. Ayrıca alınan destek hizmetinin Banka iç kontrolünü, risk yönetimini ve kritik faaliyetlerini sekteye uğratmadığı ve FIN-FSA'nın etkin denetimini engellemediği, düzenleyici kuruluş olan FIN-FSA tarafından değerlendirilmektedir.



İTALYA'da destek hizmetleri alanında, İtalya Merkez Bankası tarafından yayımlanmış ve bankalar için geçerli Circular letter no. 229/1999 sayılı bir genelge bulunmaktadır. Genelge kapsamında, hizmet alımında sağlanması gereken gereksinimlere yer verilmiş olmakla birlikte; risk yönetimine ilişkin hükümler bulunmamaktadır. Genelgenin uygulanacağı kapsam; iç kontrol, uyum, risk yönetimi, kara para aklama, bilgi sistemleri ve ödeme sistemleri alanlarında alınacak hizmetlerle sınırlandırılmıştır.

POLONYA'da 29 Ağustos 1997 yılında düzenlenen Bankacılık Kanunu kapsamında iki tip destek hizmeti tipi tanımlanmaktadır.

- Bankacılık hizmetleri,
- Bankacılık faaliyetlerini ilgilendiren etkinlikler.

Düzenlemede banka yönetimi ve banka iç kontrolünün destek hizmetine konu olamayacağı belirtilmektedir. Bankacılık kanununda, destek hizmeti kuruluşu ile gerçekleştirilecek sözleşme gereksinimleri belirtilmemektedir.

AVUSTURYA'da bankacılık kanunu (Bankwesengesetz, BWG), kredi ve finansal servislerin destek hizmeti edinimini açıkça engellememiş veya izin vermemiştir ancak destek hizmeti kullanımı konusunda belirli prensipleri düzenlemiştir. Bankaların ve portföy yöneticilerinin ana faaliyetlerine etki etmeyen destek hizmetleri ve iş faaliyetlerine az önem arz edecek şekilde etki eden destek hizmetleri faaliyetlerine izin verilmektedir. (Örn. BT ile ilişkili destek hizmetleri ve çağrı merkezleri vasıtasıyla müşteri destek hizmeti) BWG lisansı altında işleyen bankacılık faaliyetlerinin (portföy ve risk yönetimi, menkul kıymetler işlemleri, mortgage ve kredi işlemleri vb.) destek hizmeti kapsamına alınmasına müsaade edilmemektedir. Destek hizmetleri kapsamında olan tüm finansal hizmetlerin gözetimi için destek hizmeti kapsamına alınan verilere the Financial Services Agency ("Finanzmarktaufsicht") ve the Austrian National Bank'ın ("Österreichische Nationalbank") erişiminin olması gerekmektedir. Destek hizmetleri kapsamında olan tüm finansal hizmetlerin bankacılık gizlilik prensiplerini ihlal etmemesi gerekmektedir.Destek hizmeti alan kuruluşun, destek hizmeti veren kuruluşu izlemesi gerekmektedir.

2 Tedarikçi Firma Güvence ve Denetim Alanında Kullanılan Standartlar

2.1 ISO 27001

Bilgi Güvenliği Yönetim Sistemi ("BGYS") pazarında uluslararası standardizasyonu sağlamak üzere 2005 yılında sunulan ISO 27001 sertifikasyonu (ISO/IEC 27001:2005), 90'lı yılların ortasında yürürlüğe girmiş olan BS 7799 standardı temeli üzerine inşa edilmiştir. ISO 27001 sertifikasyonu, firma bünyesinde bilgi güvenliği yönetim sistemini kurmak, işletmek, izlemek, gözden geçirmek, sürdürülebilirliğini sağlamak ve iyileştirmek için sahip olunması gereken yapının kurulduğuna ve ilgili gereksinimlerin belirlendiğine ilişkin güvence verme amacını taşımaktadır.

Tablo 4'te yer verildiği gibi; IS0 27001, uluslararası arenada kabul görmüş ve başta Amerika ve Avrupa ülkeleri olmak üzere birçok ülkede kullanımı yaygınlaşmakta olan bir sertifikasyondur.

Yıl	2006	2007	2008	2009	2010	2011
Tüm Dünya	5797	7732	9246	12935	15626	17509
Türkiye	10	27	33	86	117	100
İsviçre	34	32	58	57	61	66
Hollanda	41	41	56	76	97	125
Birleşik Krallık	486	519	738	946	1157	1360
Almanya	95	135	239	253	357	424
Amerika Birleşik Devletleri	69	94	168	252	247	313

Kaynak: 2011 Survey Data ISO/IEC 27001 Data. http://www.iso.org/iso/home/standards/certification/iso-survey.htm (2011).

Tablo 4. Ülke Bazında ISO 27001 Sertifikasyon Sayısı

2.2 ISO 37500

ISO 37500 standardı, iletişime uyum sağlamak ve tüm kilit iş aktivitelerinin dış kaynak kullanımının daha iyi anlaşılmasını arttırmak amacıyla; yeni bir standart olarak geliştirilmektedir.

Yeni standart, müşterilere, servis sağlayıcılara ve üçüncü taraf danışmanlara dış kaynak edinimi konusunda yardımcı ve destek olarak; dış kaynak kullanımı anlaşmalarının başarıya ulaşma oranını arttırmayı hedeflemektedir.

ISO 37500, yürürlükte olan diğer standartlardan farklı/yeni olarak

- Dış kaynak kullanımı sırasında organizasyonlar arasındaki iletişimi arttırarak birlikte işlerliğin artırılması,
- Tüm taraflar için dış kaynak kullanımı sürecinde terminoloji, kavram ve prosedürlerin taraflar arası uzlaşmanın arttırılması için tanımlanması,
- Ortak bir sözlük oluşturarak yanlış anlaşılmaların, yanlış veya gerçek dışı beklentilerin önlenmesi ve işlem maliyetlerinin azaltılmasını gündeme getirmektedir.

Geliştirmeyi yürüten ve kararlar alan ISO/TC259 Dış Kaynak Kullanımı Komitesi'ne iştirak eden ülkeler, gözlemci ülkeler yan tarafta belirtilmiştir.

İştirak eden ülkeler:

- Bulgaristan
- Danimarka
- Finlandiya
- Fransa
- Almanya
- Hindistan
- İspanya
- İsveç
- Güney Kore
- Rusya
- Malezya
- Hollanda
- Birleşik Krallık

Gözlemci ülkeler:

- Avustralya
- İsrail
- İtalya
- Norveç
- Polonya

SAS 70 standardı, 15 Haziran 2011 tarihinden itibaren revize edilerek, SSAE 16 standardına geçilmiş ve SAS 70 standardı geçerliliğini yitirmiştir.

2.3 SAS 70

SAS 70, en temel ifadeyle hizmet organizasyonları için American Institute of Certified Public Accountants ("AICPA") tarafından hazırlanmış bir üçüncü taraf denetim rapor ve tasdik standardıdır. Bu standart kapsamındaki denetim, hizmet kuruluşunun sunduğu hizmetleri destekleyen bilgi teknolojileri ve ilişkili süreçlerinin ayrıntılı biçimde incelenmesini içermektedir. Müşterilerine ait bilgiyi işleyen veya barındıran servis sağlayıcılar ve diğer hizmet kuruluşları yeterli kontrollerin bulunduğunu ispat etmekle yükümlüdürler. Denetimlerde, ayrıca organizasyonun finansal durumu ve riskleri, insan kaynakları, iş sürekliliği uygulamaları ve felaketten kurtarma gibi uygulamalarına güvence verilebilmektedir.

İki tür SAS 70 raporu mevcuttur. Birinci tür; servis sağlayıcıyı denetçisinin iş sürekliliği, müşteri memnuniyeti ve diğer operasyonel süreçler hakkındaki görüşlerini içermektedir. İkinci tür ise, birinci tür rapora benzemekle birlikte, ek bölümler ve ölçütler içermektedir. Bunların başında raporun en az altı aylık periyotlarla yapılması, planlara ne kadar uyulduğuna dair kayıtların, finansal verilerin ve insan kaynakları uygulamalarının da incelenmesi gelmektedir. Birinci tür sadece kontrol ölçütleri ile ilgilenirken, ikinci türde işletmenin işleyişinde daha derinlemesine bir denetim yapılarak, kontrollerin etkinliği de test edilmektedir.

SAS 70 standardı, 15 Haziran 2011 tarihinden itibaren revize edilerek, SSAE 16 standardına geçilmiştir.

2.4 ISAE 3000

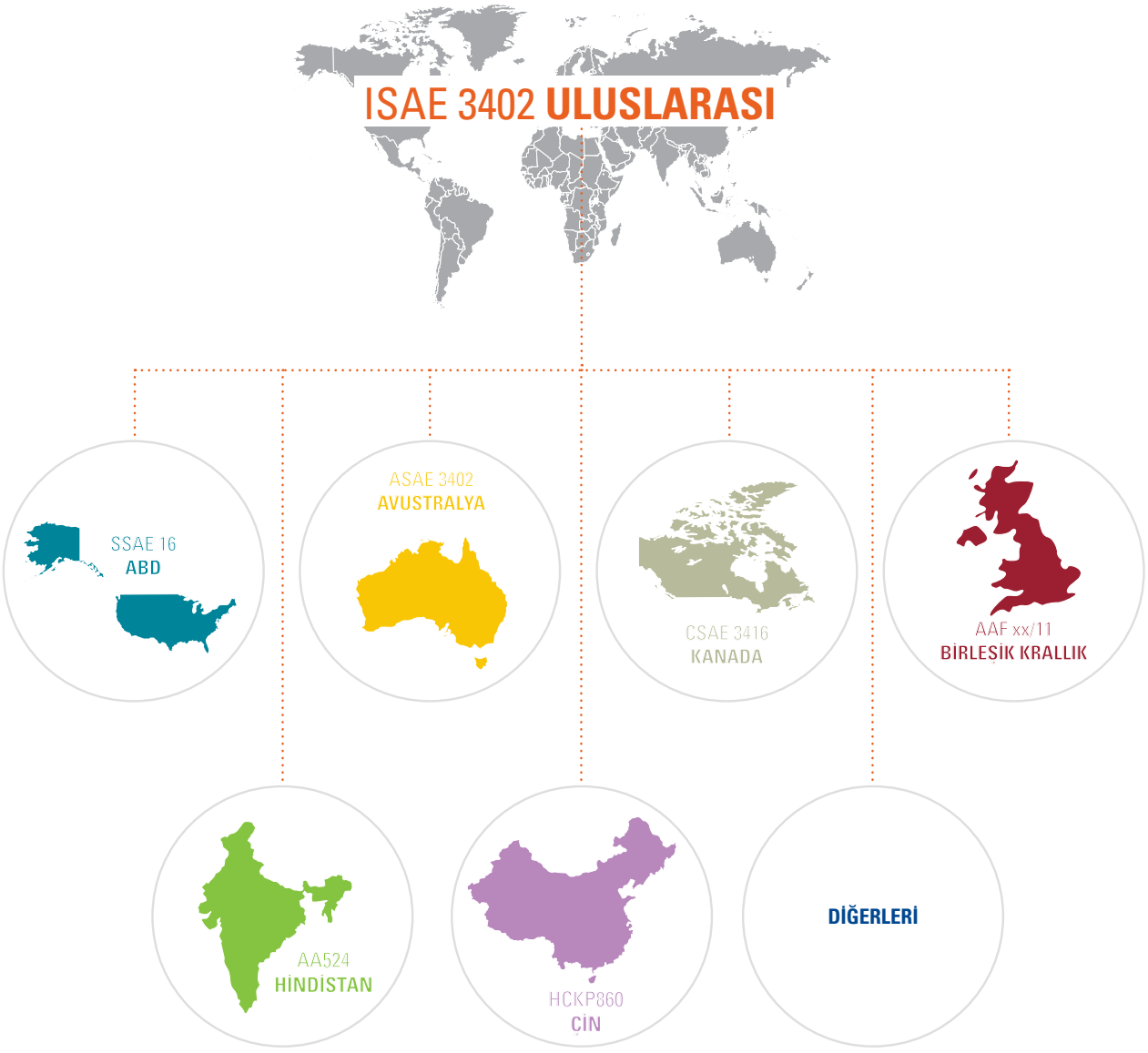
ISAE 3000 güvence standardı, The International Auditing and Assurance Standards Board ("IAASB") tarafından Aralık 2003'te yayımlanmıştır. ISAE 3000 ("Assurance Engagements Other Than Audits or Reviews of Historical Financial Information") standardının amacı, uzmanların Uluslararası Denetim Standartları ("ISA") ve Uluslararası Değerlendirme Uygulamaları Standartları ("ISRE") tarafından da kapsanmakta olan denetim ya da tarihsel finansal verilerin incelenmesi çalışmaları dışındaki güvence uygulamalarının gerçekleştirilmesi için rehberlik sunma ve gerekli prosedürlerin ve prensiplerin oluşturulmasıdır.

Bu standart, denetçinin gerçekleştirebileceği güvence uygulamalarının sınırlarını belirleyebilmek için "makul güvence" ve "sınırlı güvence" olmak üzere iki çeşit uygulama yönteminin tanımını yapmıştır. Makul güvence uygulamalarının hedefi, denetçinin görüşünün olumlu bir biçimde ifade edilmesi sağlanacak şekilde, güvence uygulamasına ilişkin risklerin kabul edilebilir bir seviyeye düşürülmesidir. Sınırlı güvence uygulamasının hedefi ise, uygulamanın riskinin kabul edilebilir bir seviyeye düşürülmesi, ancak riskler makul bir güvence seviyesinin altında ise, denetçinin görüşünün olumsuz bir biçimde ifade edilmesidir.

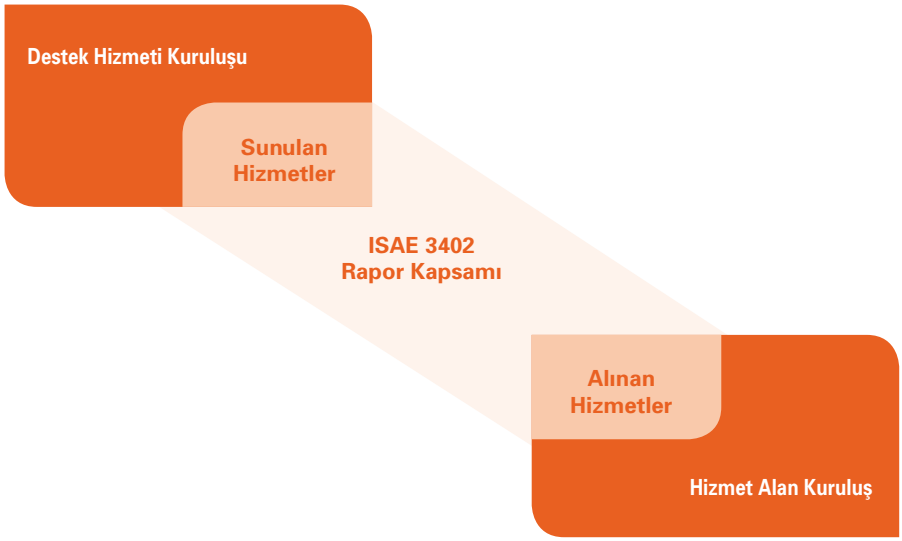
2.5 ISAE 3402

ISAE 3402, 2009 yılında International Federation of Accountants ("Uluslararası Muhasebeciler Federasyonu, IFAC) tarafından yayımlanmış; destek hizmeti kuruluşlarının sağladıkları hizmetlerin gerçekleşmesi sırasındaki iç kontrol ortamının yeterliliğine güvence vermeyi amaçlayan bir güvence ve denetim standardıdır.

ISAE 3402, uluslararası bir standart olmasına karşın farklı gereksinim ve mevzuatlara istinaden bazı ülkeler tarafından temel olarak kabul edilerek ulusal standartlara dönüştürülmüştür.



ISAE 3402 ve benzeri güvence, denetim ve raporlama standartlarında yer alan en önemli konulardan birisi olan denetim konusu ("subject matter") standardın değişik hizmet gruplarındaki firmaların ve hizmet alan kuruluşlarının ihtiyaçlarına cevap verebilen bir standart haline gelmesinde önemli bir rol oynamaktadır.



Üç Taraflı Yapı ("Three Party Relationship"):

ISAE 3402 güvence uygulamalarına göre üç taraflı yapı, sorumlu taraf (örn. Destek Hizmeti Kuruluşları), denetçi (Bağımsız Denetim Firması), hedeflenen kullanıcılardan (örn. Bankalar) oluşmaktadır. Genel olarak, ISAE 3402 çalışmaları ve denetim raporu, bağımsız denetim firması tarafından ("Denetçi"), destek hizmeti sunan firmaların ("Sorumlu Taraf") sundukları hizmetler üzerindeki kontrol ortamı hakkında, hizmet alan kuruluşların ve bu kuruluşların denetçilerinin ("Hedeflenen Kullanıcılar") güvence edinmelerini desteklemeyi hedeflemektedir. ISAE 3402 standardına göre, güvence raporunun hazırlanacağı destek hizmetleri kuruluşlarının faaliyet gösterdiği hizmet grubuna, boyutuna ya da taşıdığı önem ya da risk seviyesine göre bir kısıtlama bulunmamaktadır. Güvence uygulamaları, denetim faaliyetlerini standart ile uyumlu olarak yürüten bağımsız denetçi firmalar tarafından gerçekleştirilir.

Denetim Konusu ("Subject Matter"):

Denetim konusu, firma tarafından yürütülen Yönetim Beyanı ve bağımsız denetçi tarafından yürütülen güvence çalışmalarının, hizmet alan kuruluşlara sunulan hizmet ve belirlenen denetim kapsamına göre şekillendirilebilmesini sağlamaktadır. Denetim konusu, finansal performans ve koşullar (ör. tarihsel ya da öngörülen finansal durum, finansal performans ya da nakit akışı), finans dışı performans ve koşullar (ör. herhangi bir birimin faaliyetlerinin performansı), denetlenen destek hizmet kuruluşunun fiziksel karakteristiği (ör. tesis kapasitesi), kuruluşun sistem ve süreçleri (ör. işletmenin iç kontrolleri ya da BT sistemi) ve belirli bir konudaki tutumu (ör. kurumsal yönetişim, mevzuata uyum, insan kaynakları uygulamaları) gibi farklı unsurlardan oluşabilmektedir.

ISAE 3402 ve benzeri güvence, denetim ve raporlama standartlarında yer alan en önemli konulardan birisi olan denetim konusu ("subject matter") standardın değişik hizmet gruplarındaki firmaların ve hizmet alan kuruluşlarının ihtiyaçlarına cevap verebilen bir standart haline gelmesinde önemli bir rol oynamaktadır. Denetim konusu aynı zamanda destek hizmeti firmasının Yönetim Beyanı hazırlamasında önemli bir rol oynamaktadır. Denetim konusu belirlenirken, destek hizmetleri sunan firma tarafından sunulan hizmetlerin, sözleşmesel ve prosedürel düzenlemelere dayandırılarak doğru ve tam olarak belirlenmesi ve bu yolla oluşturulacak güvence raporunun, hedeflenen kullanıcıların güvence gereksinimlerini karşılaması gerekmektedir.

Uygunluk Kriteri ("Suitable Criteria"):

Uygunluk kriteri, güvence raporlarında denetim konusu üzerinde gerçekleştirilen incelemede, görüşe temel olacak çalışmalarda kullanılan ölçütleri belirlemektedir. En bilinen haliyle, uygunluk kriteri, destek hizmeti firmasının kontrol ortamının uygun şekilde tasarlanmasını (Tip 1 raporunda olduğu gibi) veya kontrol ortamının denetim dönemi boyunca uygun bir şekilde tasarlanması ve uygulanmasını (Tip 2 raporunda olduğu gibi) sağlar. Uygunluk kriteri bunların dışında mevcudiyet, bütünlük, güvenilirlik, tarafsızlık ve anlaşılabilirlik gibi bir çok farklı ölçütten oluşabilmektedir. Denetim konusunda belirtildiği gibi, uygunluk kriteri de, standarda esneklik kazandıran ve hem güvence çalışması sonucunda oluşan görüşün dayanağını oluşturması, hem de Yönetim Beyanı çalışmasına temel teşkil etmesi açısından önemli bir rol oynamaktadır.

Denetim Kanıtları ("Audit Evidence"):

Bağımsız denetçinin güvence uygulamasının amaçlarını doğru şekilde yerine getirebilmesi için yeterli uygunlukta kanıt alması gerekmektedir. Denetim kanıtlarının, profesyonel şüphecilik yaklaşımı ile oluşturulmuş, kontrollerin etkin işletimini teminen yeterli ve ikna edici, takip edilebilir, denetim prosedürlerinin yapı, zamanlama ve kapsamını içerecek şekilde olması beklenmektedir.

Denetim Raporu ("Independent Service Auditor's Report"):

ISAE 3402 güvence raporları görüş belirtme temelli raporlar olup, rapor temeli ana olarak beş bölümden oluşmaktadır:

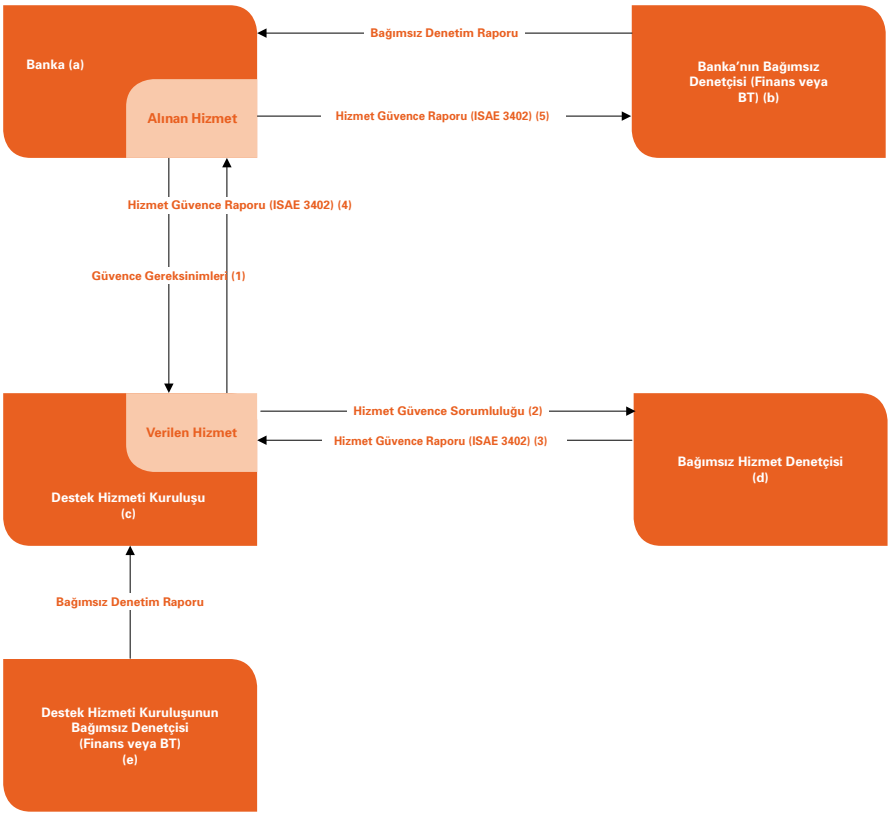
- destek hizmeti kuruluşu bağımsız denetçisi raporu - "Görüş",
- destek hizmeti kuruluşu tarafından gerçekleştirilen açıklama,
- destek hizmeti kuruluşu tarafından sağlanan iç kontrol ve kontrol hedeflerinin açıklamaları,
- destek hizmeti kuruluşu bağımsız denetçisi tarafından sağlanan bilgi (Tip 2 raporu için gerçekleştirilen test ve etkinlik çalışmaları sonucunu da dahil edecek şekilde),
- destek hizmeti kuruluşu tarafından isteğe bağlı olarak sağlanan diğer bilgiler

Ek olarak denetim raporlarında denetçinin sorumlu taraf tarafından hazırlanan yönetim beyanını değerlendirmesi ve doğrudan doğruya denetim konusu ve kriterlerinin değerlendirilmesi sonucu denetçinin bağımsız görüşünü belirtmesi beklenmektedir.

ISAE 3402 raporlarının amacı, sunulan hizmetlerin, hizmet alan kuruluşların iç kontrol ortamına olası etkisi üzerinde güvence sağlamaktır. Ayrıca, bu standardın temelini oluşturan ISAE 3000 standardı, finansal denetim ve tarihi finansal bilgilerin gözden geçirilmesi dışındaki güvence uygulamaları açısından uyulması gereken kuralların ve prensiplerin tanımlanmasını hedeflemektedir. Bu açılardan değerlendirildiğinde, ISAE 3402 raporları, hizmet sunan firmaya ait bir finansal denetim ya da salt hizmet sunan firmaya ait finansal durumun değerlendirildiği bir rapor niteliğinde değerlendirilmemelidir. Denetim raporlarında destek hizmeti alan kuruluşlara ait gizli bilgilere ve hizmetin sunulduğu kuruluşların adlarına yer verilmemesi esastır. Bu yöntemle, raporun dağıtımının yapıldığı tarafların, diğer bir hizmet alan kuruluşa ait kontrol ortamı hakkındaki riskler, kontrol zayıflıklar, vb. gizlilik arz eden bilgilere erişiminin engellenmesi sağlanır.

Destek hizmeti kuruluşu denetiminde raporu oluşturabilecek servis denetçisinin uyması gereken kurallar International Ethics Standards Board for Accountants ("IESBA") tarafından "IESBA Code" rehberinde A ve B bölümleri içinde yayımlanmıştır. Bununla birlikte, ISAE 3402 standardı içerisinde denetçinin, bağımsızlık koşulunu sağlaması gerektiği ve bu kuralların diğer sınırlayıcı ulusal gereksinimlerle birlikte geçerli olduğu belirtilmiştir. Buna bağlı olarak "IESBA Code" rehberi tanımına göre bağımsız herhangi bir kuruluş IFAC'ın IESBA Etik Kuralları'na uyduğu sürece güvence standardı denetimini gerçekleştirebilir. Ayrıca, bu rehbere göre, servis denetçisinin, hizmet sunulan firmaların her biri ile bağımsızlık ilkesini sağlama zorunluluğu bulunmamaktadır.

ISAE 3402 raporları, hizmet sunan firmaya ait bir finansal denetim ya da salt hizmet sunan firmaya ait finansal durumun değerlendirildiği bir rapor niteliğinde değerlendirilmemelidir.



2.5.1 Örnek Güvence Modeli

Banka, gerekli gördüğü durumlarda destek hizmeti aldığı kuruluşa gereksinimlerini iletir (1).

Destek hizmeti kuruluşu, gereksinimlerin kapsama alındığı bir denetim ihtiyacını bağımsız bir denetçiye iletir ve hizmet güvence sorumluluğunu bu kuruluşa verir (2).

Bağımsız hizmet denetçisi, denetim faaliyetlerinin sonucunda oluşturulan hizmet güvence raporunu (ISAE 3402) destek hizmeti kuruluşuna sunar (3).

Destek hizmeti kuruluşu, denetim çıktılarının bulunduğu bu raporu, Banka'ya iletir (4).

Banka, raporu iç denetim faaliyetleri kapsamında değerlendirebileceği gibi, aynı zamanda gerekli durumlarda kendi bağımsız finansal ve bilgi sistemleri denetçisine sunabilir (5).

Destek hizmeti kuruluşunun bağımsız denetçisi (e), firmanın finansal denetimini gerçekleştirir ve sunulan hizmet hakkında doğrudan bir güvence sunmaz. Diğer yandan, Bağımsız Hizmet Denetçisi (d), destek hizmeti kuruluşunun Banka'ya sunduğu hizmet hakkında bir güvence sunarken, kuruluşun finansal denetimi ya da finansal raporlama süreci hakkında bir güvence sunmaz.

Bu diyagramda (b), (d) ve (e) aynı ya da farklı denetim firmaları olabilir.

Rapor İçeriği	Tip 1 Raporu	Tip 2 Raporu
Destek hizmeti kuruluşu bağımsız denetçisinin denetim raporu (Görüş)	İçeriyor	İçeriyor
Destek hizmeti kuruluşu kontrol tanımları	İçeriyor	İçeriyor
Destek hizmeti kuruluşu bağımsız denetçisinin sağladığı bilgi; denetçinin ilgili kontrol ve kontrollerin etkinliğine ilişkin açıklamaların yer alması	İsteğe Bağlı	İçeriyor
Destek hizmeti kuruluşu tarafından sağlanan ek bilgi (Terimler sözlüğü vb. bilgiler)	İsteğe Bağlı	İçeriyor

Tip 2 raporu, Tip 1'den farklı olarak belirli bir denetim dönemi için hazırlanır.

2.5.2 ISAE 3402 Rapor Tipleri

Rapor, Type 1 ("Tip 1") ve Type 2 ("Tip 2") olarak 2 ayrı formatta hazırlanabilir.

Tip 1 raporunda; (a) Hizmet veren şirketin tanımladığı sistemin uygun bir biçimde tasarlanmış ve uyarlanmış olduğuna ve (b) şirketin sistemi tanımlarken belirlemiş olduğu kontrol hedeflerine uygun kontrollerin tasarlanmış olduğuna güvence verilir.

Tip 2 raporunda; Tip 1 raporunda belirtilmiş olan maddelere ek olarak test edilen kontrollerin yeterli etkinlikte çalıştığına ve kontrol hedeflerine erişildiğine ilişkin güvence verilir. Tip 2 raporu, Tip 1'den farklı olarak belirli bir denetim dönemi için hazırlanır.

Tip 1 raporu belirli bir dönemdeki destek hizmeti kuruluşuna ait kontrol açıklamalarını tanımlar. Tip 2 raporu ise destek hizmeti kuruluşuna ait kontrol açıklamalarını içermenin yanı sıra kontrollerin asgari olarak altı aylık periyotlarda detaylı olarak test edilmesini içerir.

2.5.3 SAS 70 ve ISAE 3402 Standartları Arasındaki Farklar

ISAE 3402 ve SAS 70 arasındaki farkların irdelenmesinde öne çıkan farklılıkların başında şu anda yürürlükte olmayan SAS 70 standardının Amerika Birleşik Devletleri içinde değerlendirilmesi, ISAE 3402 standardının ise uluslararası bir standart olması gelmektedir. Diğer bir husus ise ISAE 3402 standardının finansal raporlama/denetim çalışması kapsamı ile kısıtlanmadığı ve destek hizmeti kuruluşundaki kontrollerin etkinliğinin denetlendiği bir güvence standardı olmasıdır.

ISAE 3402 standardının getirdiği üç önemli yeni gereksinim:

1. Destek hizmeti kuruluşu yönetimi, kontrollerin tasarımının uygunluğu ve kontrollerin etkinliğinin sağlandığına dair uygun ortamın oluşturulduğunu doğrulamalıdır.

2. Bağımsız denetçinin, iç kontrole ilişkin gerçekleştirilen çalışmalara itimat ederek görüş bildirdiği raporda bahsedilmelidir.

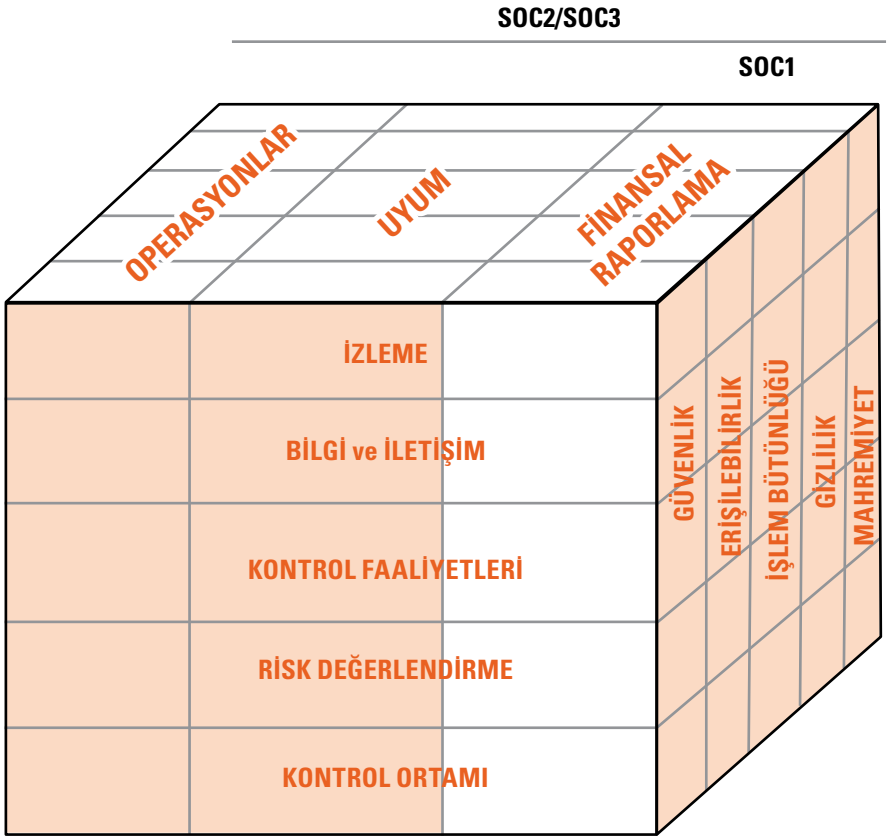
3. Denetim konusu içerisinde destek hizmeti kuruluşunun alt yüklenicilerini dahil etme kararı verilirse, Yönetim Beyanı ve denetim çalışmaları için geçerli kurallar alt-yüklenici hizmetleri için de geçerlidir.

2.5.4 SOC 1, 2 ve 3

ISAE 3402 standardının altındaki farklı denetim konularının ve uygunluk kriterlerinin çeşitli güvence gereksinimlerine uygun olarak kullanımını sağlamak için, American Institute of Certified Public Accountants ("AICPA") tarafından finansal raporlama ve diğer ilişkili süreçler üzerindeki işletilen kontrollere güvence sunma amaçlı ISAE 3402 standardını baz alan SOC1, SOC2 ve SOC3 rapor çeşitleri geliştirilmiştir.

SOC1 raporu servis sağlayıcının finansal raporlama üzerindeki iç kontrol mekanizmasına ilişkin kontrolleri üzerinde güvence verilmesini sağlamaktadır. SOC1 ("Type 1" ve "Type 2") raporu SSAE 16 kılavuzu kapsamı içerisinde değerlendirilmektedir. Ek olarak, raporlama standardı SSAE 16 veya ISAE 3402 standardı olduğunda raporlama sonucunda hazırlanan çalışmanın sonucu SOC1 raporu olacaktır.

SOC1 raporunda sunulan güvence açısından, finansal raporlama süreçleri üzerindeki iç kontrol ortamı (ICOFR), hizmet sunulan firma yönetiminin finansal raporlama faaliyetlerinin ve finansal tablolarının güvenilirliği açısından makul güvence sunulmasını sağlayan süreçlerini ve kontrollerini ifade etmektedir. Bu açıdan düşünüldüğünde, SOC1 raporu, doğrudan firmanın finansal raporlama faaliyetleri ve finansal tablolarından öte, sunulan hizmetin, hizmet alan kuruluşun finansal raporlamasına etkisi üzerinde bir görüş içerir. Bu görüş oluşturulurken, hizmetin sunulmasını destekleyen süreçlerin (operasyonel, uyum, BT, vb.) üzerindeki kontrollerin, önemlilik kriteri baz alınarak denetim konusu kapsamına alınması gerekmektedir.



SOC2 raporları "Trust Services" prensiplerine dayalı şekilde politika, iletişim, prosedür ve izleme modelleri üzerinde şekillenmiştir. Her bir prensip içinde belirli kontroller tanımlı olmakla birlikte ve tüm kontrollerin prensiplere bağlı şekilde denetim süresince kayda değer şekilde istisnai bir durum olmayacak şekilde görüş belirtilmesi gerekmektedir. "Trust Services" prensipleri için en önemli durumlardan biri faaliyetlere ilişkin ölçütlerin önceden tanımlı olmasıdır. SOC2 raporunun SOC1 raporundan farkı, piyasalardaki talepleri adresleyecek şekilde, kullanıcı kuruluş üzerinde finansal etkisi olmadığı değerlendirilen hizmetler için SOC1 denetiminden farklı olarak güvenlik, bütünlük, gizlilik, mahremiyet ve erişilebilirlik gibi kriterler kullanılarak güvence verilmesinin sağlanmasıdır.

SOC1 raporu, servis sağlayıcının finansal raporlarına ve iç kontrol mekanizmasına ilişkin kontrollerini; SOC2 ve SOC3 raporları ise erişebilirlik, veri güvenliği, gizlilik ve işlem bütünlüğü alanlarına etki eden operasyonel kontrolleri kapsamaktadır.

SOC2 ve SOC3 raporları arasındaki fark ise SOC3 raporlarının kontrollere ilişkin testler hakkında detay içermemesi, pazarlama amacıyla kullanılabilmesi ve paylaşımı açısından bir engel bulunmamasıdır.

WebTrust, American Institute of Certified Public Accountants ("AICPA") ve Canadian Institute of Chartered Accountants ("CICA") tarafından ortaklaşa geliştirilmiş olan bir güvence raporu çeşididir. WebTrust, internet üzerinden işlem gerçekleştiren şirketlerle tüketiciler arasındaki güveni sağlamayı hedefleyen bir dizi prensip ve kriterden oluşmaktadır. AICPA ya da CICA'dan WebTrust lisansı alan serbest muhasebeciler ve denetçiler, bir web sitesinin belirlenen "Trust Services" prensiplerini sağlayıp sağlamadığını değerlendirebilir ve test edebilirler. Denetim çalışması sonrasında, denetlenen kuruluşun söz konusu web sitesine WebTrust damgası eklenmekte ve bu damga denetçinin olumlu görüşünü ifade etmektedir.

SysTrust, benzer şekilde AICPA ve CICA tarafından ortaklaşa oluşturulmuş bir güvence raporu çeşididir. WebTrust'dan farkı ise, bu raporlama çeşidiyle; firma yöneticileri, müşteriler ve iş ortakları arasında yürütülen işleri ve faaliyetleri destekleyen sistemler hakkında güvence sunulmasıdır. SysTrust denetimlerinde, söz konusu sistemlerin erişilebilirlik, güvenilirlik ve bütünlük kriterleri açısından değerlendirmesi gerçekleştirilmektedir.

2.5.5 SOC (1, 2, 3) Karşılaştırma

SOC Karşılaştırma Tablosu	SOC1	SOC2	SOC3	WEBTRUST/SYSTRUST
		Trust Service Prensipleri ve Kriterleri		
Kılavuz	• ISAE 3402 • SSAE 16 • Tip 1ve Tip 2 Raporları	• AT101 • ISAE 3000	• AT101	• İlgili webtrust ve systrust ölçütleri
Kullanım / Dağıtım	• Kısıtlı kulanım (Tip 1 veya 2 Raporları)	• Genel olarak kısıtlı kullanım (Tip 1 veya 2 raporları)	• Genel kullanıma açık (Resmi mühür ile birlikte)	• Genel kullanıma açık (Resmi mühür ile birlikte)
Kontrol Noktaları	• Finansal Risk ve Raporlama	• Güvenlik • İşlem Bütünlüğü • Gizlilik • Mahremiyet • Erişilebilirlik	• Güvenlik için Trust Services Prensipleri ve Kriterleri • Mahremiyet • Gizlilik • Erişilebilirlik • Güvenlik	Systrust için: • Güvenlik • Erişilebilirlik • İşlem Bütünlüğü • Gizlilik Webtrust için: • Webtrust • Webtrust Çevrimiçi Mahremiyeti • Webtrust Müşteri Koruması • WebTrust Sertifika Yetkilileri
Raporlama Amacı	• Finansal servis denetimlerinin üzerindeki kontroller	• Uyumluluk veya operasyonla ile ilgili kontroller • Trust services ölçütleri kapsamında tanımlanan prensiplerin gerçekleştirilmesi		
Standart Seviyesi	• Kontrol hedefleri servis sağlayıcısı tarafından tanımlanır ve tedarik edilen hizmete göre değişiklik gösterebilir	• Prensipler servis sağlayıcısı tarafından seçilmesi • Kontrol hedefleri yerine daha önceden tanımlanmış ölçütlerin kullanılması • Kontrol hedefleri olarak Trust Servisleri ile ilgili ölçütlerin seçilmesi		

2.5.6 Standardın Türkiye Mevzuatına Uygulanabilirliği

Destek Hizmetleri Yönetmeliği'nin çeşitli maddelerinde yer alan gereksinimler incelendiğinde, ISAE 3402 standardında "Denetim Konusu" olarak yer alabilecek gereksinimler aşağıdaki tabloda sunulmuştur. Bu tabloda görülmektedir ki, doğrudan firmanın sunduğu hizmete ait yeterlilik ya da risk seviyesini belirten kriterler (ör. İş Sürekliliği, Teknik Donanım ve Altyapı, vb) ISAE 3402 güvence raporunda adreslenebilirken, doğrudan firmanın kuruluşu ya da yapılanması ile ilgili kriterlerin (ör. Mali Güç, Yöneticilerin İtibarı, vb) hizmet güvencesi kapsamında oluşturulacak görüşe dayanak oluşturma açısından "Denetim Konusu" olarak adreslenmesinin söz konusu güvence açısından uygulanabilir olmadığı değerlendirilmiştir.

Buradan anlaşılıyor ki, ISAE 3402 raporu, denetim konusu ("subject matter") kapsamında esnek olup; destek hizmet kuruluşunun ve finansal verilerinin denetlenmesinden ziyade, destek hizmeti sunulan firmanın finansal raporlama sürecine ve iç kontrol ortamına etkisi olabilecek destek hizmet kuruluşu bünyesindeki insan kaynağı, süreç, sistem ve altyapının denetimini ve raporlanmasını içermektedir. Ülkemizde yürürlükte olan destek hizmetleri mevzuatı göz önüne alındığında, ISAE 3402 standardının yukarıda bahsedilen özellikleri ve esnek yapısı nedeniyle, destek hizmeti sunan kuruluşların iç kontrol ortamlarının denetlenmesi çerçevesinde kolaylıkla kullanılabileceği düşünülmektedir.

Destek Hizmetleri Yönetmeliği	ISAE 3402
Destek hizmetinden doğabilecek riskler ile bunların yönetilmesinde, beklenen fayda ve maliyetin değerlendirilmesi (Madde 5)	x
Destek hizmeti alınmasında bankanın iç sistemlerinin etkin ve yeterli bir şekilde işletilmesini veya iç kontrol ya da iç denetim faaliyetlerinin yürütülmesini engelleyici ya da risk doğurucu herhangi bir hususun oluşup oluşmadığı (Madde 9)	√
Teknik Donanım ve Altyapı (Madde 5)	√
Mali Güç (Madde 5)	x
Tecrübe, Bilgi Birikimi (Madde 5)	√
İnsan Kaynağı (Madde 5)	√
Sermaye şirketi seklinde kurulmuş, ortaklık yapılarının şeffaf ve açık olması (Madde 6)	x
Destek hizmetini gerçekleştirebilecek yönetim yapısına sahip olması (Madde 6)	√
Yeterli sayı ve nitelikte personele sahip olması (Madde 6)	√
Gerekli teknik donanıma sahip olması (Madde 6)	√
Uygun belge ve kayıt düzenine sahip olması (Madde 6)	√
İş devamlılığı planına sahip olması (Madde 6)	√
Güvenlik risklerine, yangın ve doğal afetler gibi acil durumlara karsı gerekli önlemleri almış olması (Madde 6)	√
Firmanın sorumluluk sigortası yaptıracağını taahhüt etmesi (Madde 6)	x
Yurt dışında ya da Türkiye'deki yetkili otoritelerce faaliyette bulundukları alanla ilgili yetkilerinin iptal edilmemiş veya kısıtlanmamış olması (Madde 6)	x
İsin gerektirdiği mali güç ve itibara sahip bulunmaları (Madde 6)	x
Yurt dışında ya da Türkiye'deki yetkili otoritelerce bulunduğu alanla ilgili yetkileri iptal edilmiş veya kısıtlanmış destek hizmeti kuruluşlarında ortak, yönetim kurulu başkanı, üyesi veya denetçi ya da yönetici olmamaları veya çalışan olarak yetki iptaline veya kısıtlamaya neden olan işlemlerde sorumluluklarının tespit edilmemiş olması (Madde 6)	x
Nitelikli pay sahiplerinin, yönetim kurulu başkan ve üyeleri ile şirketi temsil ile yetkili yöneticilerinin Kanunun 8 inci maddesinin birinci fıkrasının (a), (b), (c) ve (d) bentlerinde belirtilen nitelikleri haiz olmaları (Madde 6)	x

Notlar

Kısaltmalar

AICPA American Institute of Certified Public Accountants, Amerikan Serbest Muhasebeciler Odası

AFM Autoriteit Finaciele Markten, Finansal Piyasalar Kurulu

APRA The Australian Prudential Regulatory Auhtority, Avurstralya Yetkili Düzenleyme Kurulu

ASAE Assurance Reports on Controls at a Service Organisation, Hizmet Kuruluşları Kontrol Güvence Raporları

AUASB Auditing and Assurance Standards Board, Denetim ve Güvence Standartları Kurulu

BAFIN German Federal Supervisory Authority, Alman Federal Düzenleme Kurulu

BDDK Bankacılık Düzenleme ve Denetleme Kurumu

BGYS Bilgi Güvenliği Yönetim Sistemi

DNB De Nederlandsche Bank, Hollanda Merkez Bankası

FDIC The Federal Deposit Insurance Corporation, Federal Mevduat Sigortaları Kuruluşu

FED The Federal Reserve Bank of New York, New York Federal Rezerv Bankası

FFIEC The Federal Financial Institutions Examination Council, Federal Finansal Kuruluşlar İnceleme Konseyi

FINMA Swiss Financial Market Supervisory Authority, İsviçre Finansal Piyasalar Düzenleme Kurulu

FINRA The Financial Industry Regulatory Authority, Finansal Sektör Düzenleme Kurulu

FSA Financial Services Authority, Finansal Hizmetler Kurlu

ICAEW Institute of Chartered Accountants in England and Wales, Galler ve İngiltere Yeminli Mali Müşavirler Enstitüsü

IFAC Internatinal Federation of Accountants, Uluslararası Muhasebeciler Federasyonu

IAASB International Auditing and Assurance Standards Board, Uluslararası Denetim ve Güvence Standartları Kurulu

IESBA International Ethics Standards Board for Accountants, Uluslararası Muhasebeciler için Etik Standartlar Kurulu

ISA International Standards on Auditing, Uluslararası Denetim Standartları

ISAE International Standard on Assurance Engagements, Uluslarası Güvence Uygulamaları Standartları

ISRE International Standard on Review Engagement, Uluslarası Gözden Geçirme Uygulamaları Standartları

NIVRA Nederlands Instituut van Registeraccountants, Hollanda Kayıtlı Danışmanlar ve Denetçiler Birliği

NOVAA Nederlandse Orde Van Accountants, Hollanda Muhasebeciler Birliği

NOREA Nederlandse Orde van Register EDP-Auditors, Hollanda Bilgi Sistemleri Denetçileri Birliği

OCC Office of the Controller of the Currency, Döviz Kuru Düzenleme Bürosu

PCAOB Public Company Accounting Oversight Board, Halka Açık Şirketler Muhasebe Düzenleme Kurulu

SAS Statement on Auditing Standards, Denetim Standartları Beyannamesi

SFSA The Swedish Financial Supervisory Authority, İsveç Finansal Kuruluşlar Düzenleme Kurulu

SOC Service Organization Control, Hizmet Kuruluşu Kontrolü

SSAE Statement on Standards for Attestation Engagements, Tasdik Uygulamaları Standartları Beyannamesi

SYSC8 Senior Management Arrangements, Systems and Controls, Üst Yönetim Düzenlemeleri, Sistemler ve Kontrolleri

TPM Third Party Memorandum, Üçüncü Taraf Memorandumu

TSP Supervision of Technology Service Providers, Teknoloji Hizmeti Sağlayıcıları Düzenlemeleri

Referanslar

FSO Knowledge Exchange. Financial Services Outsourcing Deals – 2011. (2012).

Basel Comitee on Banking Supervision. Outsourcing in Financial Services. (2005).

German Federal Data Protection Act (Bundesdatenschutzgesetz (BDSG)). (2009).

BaFin Circular Letter 11/2010 (BA). (2010).

Institut der Wirtschaftsprüfer. IDW PS 951 (2010). http://www.idw.de (2013).

FINRA Regulatory Notice, Third Party Service Providers. (Mart 2011).

OCC Advisory Letter. (Kasım 2000).

FDIC Compliance Manual Third Party Procedure. (Aralık 2012).

Guidance for Managing Third-Party (FIL-4408). (Haziran 2008).

FFIEC Supervision of Technology Service Providers. (TSP) Booklet. (Ekim 2012).

The Federal Reserve Bank. Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks. (Ekim 1999).

PCAOB Auditing Standard No. 5. An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. (2007).

AICPA. AT Section 801. Reporting on Controls at Service Organization: SSAE 16. (Haziran 2012).

Comité de la Réglementation Bancaire et Financière Regulation No. 97-02. (2010).

Banca d'Italia Circulare N. 229. (1999).

Prudential Standards CPS 231 Outsourcing. (Ocak 2013).

Prudential Practice Guide. PPG231- Outsourcing. (Ekim 2006).

Cross-border Outsourcing and Risk Management for Banks. (Mayıs 2002).

Auditing and Assurance Standards Board. Standard on Assurance Engagements ASAE 3402. (June 2010).

Auditing and Assurance Standards Board. Auditing Standard ASA 402 Audit Considerations Relating to an Entity Using a Service Organisation. (Haziran 2011).

FSA Handbook SYSC 8 Outsourcing. (2007).

ICAEW AAF 01/06. (2006).

FIN-FSA Regulations and Guidelines 1/2012. (2012)

National Bank of Poland. The Bank Act of 29 August 1997. (1997).

The Swedish Financial Supervisory Authority. Banking and Financing Business Act (SFS 2004:297). (2004).

The Swedish Financial Supervisory Authority. Investment Funds Act (SFS 2004:46).

The Swedish Financial Supervisory Authority. Securities Market Act (SFS 2007:528).

FINMA-RS 08/7 Outsourcing Banken vom 01 (Ocak 2009)

Committee of European Banking Supervisors, Outsourcing Guideline, Guideline 9.

Quayle, A. (2012) Better Outsourcing. ISO Focus.

2011 Survey Data ISO/IEC 27001 Data. http://www.iso.org/iso/home/standards/certification/iso-survey.htm (2011).

Katkıda Bulunanlar

Sinem Cantürk
Direktör, Bölüm Başkanı
Bilgi Sistemleri Risk Yönetimi,
KPMG Türkiye
T: +90 216 681 90 00 - 9037
E: scanturk@kpmg.com

Servet Gözel
Müdür,
Bilgi Sistemleri Risk Yönetimi,
KPMG Türkiye
T: +90 216 681 90 00 - 9176
E: servetgozel@kpmg.com

Ehtiram İsmayılov
Müdür,
Bilgi Sistemleri Risk Yönetimi,
KPMG Türkiye
T: +90 216 681 90 00 - 9161
E: eismayilov@kpmg.com

Herman van Gils
Kıdemli Müdür, Danışmanlık,
KPMG Hollanda
T: +31206568026
E: VanGils.Herman@kpmg.nl

Raffael Schweitzer
Kıdemli Müdür, Danışmanlık,
KPMG İsviçre
T: +41582495288
E: rschweitzer@kpmg.com

Paul Felstead
Kıdemli Müdür, Danışmanlık,
KPMG İngiltere
T: +44 113 2313789
E: paul.felstead@kpmg.co.uk

Hakan Sadıkoğlu
Bilgi Sistemleri Risk Yönetimi,
KPMG Türkiye
T: +90 216 681 90 00 - 9969
E: hsadikoglu@kpmg.com

Hakan Ercin
Bilgi Sistemleri Risk Yönetimi,
KPMG Türkiye
T: +90 216 681 90 00 - 9968
E: hercin@kpmg.com

Ofis Adresleri

KPMG İstanbul
Kavacık Rüzgarlı Bahçe Mah.
Kavak Sok. No:29
Beykoz 34805 İSTANBUL
T: +90 216 681 90 00
F: +90 216 681 90 90

KPMG Ankara
Turan Güneş Bulvarı,
Galip Erdem Cad. No: 41
Yıldızevler Çankaya
06650 Ankara
T: + 90 312 491 72 31
F: + 90 312 491 71 31

KPMG İzmir
Heris Tower, Akdeniz Mah.
Şehit Fethi Bey Cad. No:55
Kat: 21 Alsancak 35210 İZMİR
T: + 90 232 464 20 45
F: + 90 232 464 21 45

kpmg.com.tr