TEBLİĞ

Bankacılık Düzenleme ve Denetleme Kurumundan:

BİLGİ ALIŞVERİŞİ, TAKAS VE MAHSUPLAŞMA KURULUŞLARINDA BİLGİ SİSTEMLERİ YÖNETİMİNDE ESAS ALINACAK İLKELER İLE İŞ SÜREÇLERİ VE BİLGİ SİSTEMLERİNİN DENETİMİNE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Tebliğin amacı, Risk Merkezi, bilgi alışverişi, takas ve mahsuplaşma kuruluşlarının faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esaslar ile bilgi sistemleri ve iş süreçlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ilgili esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Risk Merkezi, bilgi alışverişi, takas ve mahsuplaşma kuruluşları, bilgi sistemleri denetimini yapmaya yetkili kuruluşlar, bağımsız denetim kuruluşları ve dış hizmet sağlayıcı kuruluşlar 1 inci maddede belirtilen amaçla sınırlı olarak bu Tebliğ hükümlerine tabidir.

Dayanak

MADDE 3 – (1) Bu Tebliğ, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun Ek 1 inci maddesi, 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 27 nci maddesinin üçüncü fıkrası ve 29 uncu maddesinin ikinci fıkrası ile 10/3/2007 tarihli ve 26458 sayılı Resmî Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmeliğin 26/B maddesinin dördüncü fıkrası hükümlerine dayanılarak düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 4 – (1) Bu Tebliğde geçen;

a) Bilgi alışverişi kuruluşu: Banka Kartları ve Kredi Kartları Kanununun 4 üncü maddesi çerçevesinde faaliyet izni alarak bilgi alışverişi faaliyetinde bulunan kuruluşları,

b) Birincil sistemler: Faaliyetlerin yürütülmesini ve ilgili düzenlemelerde kuruluş için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

c) BSDHY: 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,

ç) COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedeflerinin Kurumca uygun görülen versiyonunu,

d) Denetçi: Bilgi sistemleri ve iş süreçleri denetimini yapmak üzere BSDHY kapsamında yetkilendirilmiş bağımsız denetim kuruluşu tarafından görevlendirilmiş ve unvanları bu BSDHY'nin 18 inci maddesinde sıralanan

personeli,

e) İç Sistemler: Banka Kartları ve Kredi Kartları Hakkında Yönetmelik hükümlerine tabi kuruluşlar bakımından anılan Yönetmeliğin 26/A, 26/C ve 26/Ç maddesinde tanımlanan iç kontrol, risk yönetimi ve iç denetim sistemlerini; diğer kuruluşlar için bu Tebliğ uyarınca tesis edilmesi gereken kontrol ve sistemleri,

f) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve herhangi bir kesinti durumunda personelin çalışmasına imkân tanıyacak ve birincil sistemlerin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

g) İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve ilgili kanun ve düzenlemelerde kuruluş için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistem yedeklerini,

ğ) İlkeler Tebliği: 14/9/2007 tarihli ve 26643 sayılı Resmî Gazete'de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği,

h) İş etki analizi: İş süreçlerinin ve bir faaliyet kesintisinin iş süreçleri üzerinde yaratabileceği etkilerin analizini,

ı) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

i) Kuruluş: Risk Merkezi ile bilgi alışverişi, takas ve mahsuplaşma kuruluşlarını,

j) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

k) Üst yönetim: Kuruluş yönetim kurulu ile genel müdür ve genel müdür yardımcıları, iç sistemler kapsamındaki birimlerin yöneticileri ile başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticileri,

l) Yetkili kuruluş: BSDHY kapsamında denetim yapma yetkisi verilen bağımsız denetim kuruluşunu veya BSDHY kapsamında dış hizmet alımı yöntemiyle kuruluşta bilgi sistemleri denetimi yapma izni verilen bağımsız denetim kuruluşu ile dış hizmet sağlayıcı kuruluşu,

m) Risk Merkezi: Bankacılık Kanununun Ek 1 inci maddesinde öngörülen; kredi kuruluşları ile Kurulca uygun görülecek finansal kuruluşların müşterilerinin risk bilgilerini toplamak ve söz konusu bilgileri bu kuruluşlar ile gerçek veya tüzel kişilerin kendileriyle ya da onay vermeleri koşuluyla gerçek kişiler ve özel hukuk tüzel kişileri ile de paylaşılmasını sağlamak üzere Türkiye Bankalar Birliği nezdinde kurulan, ayrı bir tüzel kişiliği bulunmayan Türkiye Bankalar Birliği Risk Merkezini,

n) Risk Merkezi Yönetimi: Risk Merkezinin görev ve faaliyetlerini sevk ve idare etmek üzere oluşturulmuş olan Türkiye Bankalar Birliği Risk Merkezi Yönetimini,

o) Üye Kuruluş: Kuruluş ile arasında bilgi alışverişi, takas ve mahsuplaşma faaliyetlerinde hizmet alışverişi bulunan tüzel kişileri,

ö) Takas ve mahsuplaşma kuruluşu: Banka Kartları ve Kredi Kartları Kanununun 4 üncü maddesi çerçevesinde faaliyet izni alarak takas ve mahsuplaşma faaliyetinde bulunan kuruluşları

ifade eder.

İKİNCİ BÖLÜM

Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Genel ilkeler

MADDE 5 – (1) Kuruluş, İlkeler Tebliğinin 4, 6, 7, 9, 10, 11, 12, 13, 14, 17, 21, 22 ve 33 üncü maddeleri ile 5 inci maddesinin birinci, ikinci, üçüncü ve dördüncü fıkralarına; 8 inci maddesinin birinci fıkrasına, ikinci fıkrasına, üçüncü fıkrasının (a), (b), (c), (ç), (d), (e), (f) ve (g) bentlerine, dördüncü fıkrasına, beşinci fıkrasına ve altıncı fıkrasına; 15 inci maddesinin birinci fıkrasının (a), (b), (c), (ç), (d) ve (e) bentlerine ve 16 ncı maddesinin ikinci fıkrasına tabidir.Bu maddelerde geçen "banka" ifadesi kuruluş; "müşteri" ifadesi kuruluştan hizmet alan üye kuruluşlar veya kişiler; "bankacılık faaliyetleri" ifadesi ise kuruluşun kendi faaliyetleri ve iş süreçleri olarak uygulanır.

(2) Kuruluşun birincil ve ikincil sistemlerini yurt içinde bulundurması zorunludur.

(3) Kuruluş, kendi alanına giren konularda sahtecilik ve dolandırıcılık olaylarını önleyici çalışmalar yapmak, güvenlik önlemleri saptamak, ilgili taraflar arasında gerekli bilgi paylaşımının sağlandığından emin olacak şekilde mekanizmalar kurmak ve sağlanan bilgi paylaşımının etkinliğini takip etmekle yükümlüdür.

(4) Sır kapsamındaki verilere ilişkin olarak kuruluş ile veri alışverişinde bulunan kişilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; kişinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenler tamamen kişinin şahsına özgü olur ve bunlar sunulmadan kimlik doğrulama gerçekleştirilemez, hizmetlere erişim sağlanamaz. 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde düzenlenen güvenli elektronik imza kullanıldığı takdirde bu fıkradaki hükümler yerine getirilmiş sayılır. Elektronik imza vasıtasıyla kimlik doğrulama gerçekleştirmede yabancı elektronik sertifikaların kullanılması halinde, anılan Kanunun "Yabancı elektronik sertifikalar" başlıklı 14 üncü maddesinde ve ilgili alt düzenlemelerde yer alan hükümler geçerlidir. Müşteri bilgilerinin üçüncü taraflar ile paylaşılması için alınması gereken müşteri rızası, iki bileşenli kimlik doğrulama yapılması ve bilgilerin paylaşımına müşterinin onay verdiğinin gerektiğinde kanıtlanabilmesine yönelik tedbirlerin alınması şartıyla elektronik ortamda alınabilir.

(5) Sızma testi yılda en az bir defa yaptırılır.

Bilgi sistemleri süreklilik, acil ve beklenmedik durum planı

MADDE 6 – (1) Kuruluşun faaliyetlerini ve önemli iş fonksiyonlarını destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere yönetim kurulu tarafından onaylanmış iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanır.

(2) Planın hazırlanması sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde belirlenen kesintilerin etkileri analiz edilir. Bu analizin sonuçlarına göre her bir servis için kabul edilebilir kesinti süreleri Kurum ve Türkiye Cumhuriyet Merkez Bankasının görüşleri de alınarak yönetim kurulunca belirlenir, bu kesinti süresi içerisinde servisin tekrar erişime açılabilmesine imkân tanıyacak alternatifli kurtarma prosedürleri geliştirilir ve buna göre gerekli önlemler alınır.

(3) Plan kapsamında, performans takip teknikleri kullanılır, kapasite planlaması yapılır, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturulur. Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir, bilgi sistemleri alt yapısının kapasitesinin ölçeklenebilirliği analiz edilir, işlem hacmi tahminleri doğrultusunda gerçekleştirilecek stres testleri ile alt yapının dayanıklılığı test edilir.

(4) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedekleri ikincil merkezde kullanıma hazır bulundurulur. İkincil sistemler ile ilgili bu Tebliğ ile getirilen hükümlere ilave yurt içinde yedek tesis edilmesi

kuruluşun kendi ihtiyarındadır.

(5) Plan, kuruluşun iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra gözden geçirilerek güncellenir. Mevcut planın etkinliğini ve güncelliğini temin etmek üzere testler yapılır, testlere varsa destek hizmeti kuruluşları da dâhil edilir ve test sonuçları üst yönetime raporlanır. Söz konusu testler kapsamında kuruluş yılda en az bir kez bütün üyelerin katılımıyla bir günlük operasyonlarının tamamını ikincil merkezi üzerinde gerçekleştirir.

(6) Kuruluş, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en aza indirmek üzere acil ve beklenmedik durum planı oluşturarak gerekli önlemleri alır, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci ile beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis eder. Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçleri ele alınır. Bilgi sistemlerine ilişkin beklenmedik olayların sonradan incelenmesine imkân tanıyacak, yetkili merciler tarafından talep edildiğinde kullanılabilecek nitelikte kayıt ve bilgileri toplayan bir mekanizma oluşturulur.

(7) Kuruluş, bilgi alışverişi, takas ve mahsuplaşma sisteminin sürekliliğinin sağlanabilmesi adına üye kuruluşlar tarafından alınması gerekli olan tedbirleri belirler ve yazılı olarak üyeleriyle paylaşır. Kuruluş, söz konusu önlemleri belirtilen tarihe kadar almayan üye kuruluşu, alınması talep edilen tedbir ve üye kuruluşa verilen süre ile birlikte en geç bir ay içerisinde Kuruma bildirir.

(8) Bu maddedeki hükümler İlkeler Tebliğinin 22 nci maddesi uyarınca sistemlerin sürekliliğinin sağlanması ile ilgili tesis edilmesi gereken kontrollere ilave hükümlerdir.

Bilgilerin doğruluğunun, güvenliğinin ve güncelliğinin sağlanması

MADDE 7 – (1) Bilgi alışverişi kuruluşları ve Risk Merkezi, üye kuruluşlar ile olan bilgi iletişiminin güvenli, doğru ve yeterli sıklıkta gerçekleşebilmesi için gerekli önlemleri alır; söz konusu önlemleri üye kuruluşa iletir ve bu önlemlerin yerine getirilmesini gözetir; bilgilerin ne ölçüde güncel tutulacağına ilişkin yönetim kurulu kararı alır ve bir ay içerisinde Kuruma ve Türkiye Cumhuriyet Merkez Bankasına yazılı olarak iletir.

(2) Kuruluş, Bankacılık Kanununun 73 üncü maddesine göre sır kapsamında olan bilgilerin üye kuruluş tarafından sorgulanmasına ilişkin işlemlere ait denetim izlerinin, bilgilerin ifşası durumunda üye kuruluş içindeki sorumluların tespitini sağlayacak nitelikte bir yıl süreyle üye kuruluş tarafından tutulmasını temin eder.

Destek hizmeti alınması

MADDE 8 – (1) İlkeler Tebliğinin 8 inci maddesinde belirtilen hükümlere ilave olarak, kuruluşun yapacağı destek hizmetlerine ilişkin sözleşmelerde:

a) Destek hizmeti kuruluşlarının gerçekleştirdiği faaliyetlere ilişkin olarak Kurumun ve kuruluşun bağımsız denetçisinin denetimine tabi olduğu,

b) Destek hizmeti kuruluşlarının gerçekleştirdiği faaliyetlere ilişkin olarak Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü elektronik, manyetik ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemeye hazır bulundurmak ve işletmekle yükümlü olduğu,

c) Kuruluşun iç sistemler birimleri ile bağımsız denetçisinin, destek hizmeti alınan konuyla ilgili olarak hizmet veren kuruluştan her türlü bilgi ve belgeyi talep etme yetkisinin bulunduğuna,

ilişkin hususların belirtilmesi zorunludur.

(2) Destek hizmeti kuruluşunun sır kapsamındaki verilere elektronik ve fiziksel ortamda erişimini önleyici ve tespit edici kontrollerin tesis edilmesi koşuluyla, ikincil merkez destek hizmeti kuruluşundan tedarik edilebilir.

Kontrollerin takibi

MADDE 9 – (1) Kuruluş, iç sistemler kapsamında yürütülen iç denetim ve iç kontrol faaliyetlerinin bir parçası olarak, bu Tebliğ uyarınca tesis edilen kontrollerin etkinlik, yeterlilik ve uygunluğunun yanı sıra kontrol ile hedeflenen risk ya da risklerin etkisini azaltmaya yönelik performansı devamlı bir şekilde takip eder ve değerlendirir. Değerlendirme neticesinde tespit edilen önemli kontrol eksikleri üst yönetime raporlanır, gerekli tedbirlerin alınması sağlanır.

ÜÇÜNCÜ BÖLÜM

Bağımsız Bilgi Sistemleri ve İş Süreçleri Denetimi

Bağımsız bilgi sistemleri ve iş süreçleri denetimi

MADDE 10 – (1) Kuruluşun bilgi sistemleri, iş süreçleri ve iç sistemlerinin denetimi ve denetim sonuçlarının raporlanması BSDHY ile belirlenen usul ve esaslar çerçevesinde, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca gerçekleştirilir.

(2) BSDHY'de geçen "banka" ifadesi kuruluş; "bankacılık süreçleri" ifadesi ise kuruluşun iş süreçleri olarak uygulanır. İş süreçlerinin belirlenmesi ve denetim kapsamına dâhil edilmesinde, BSDHY'nin 5 inci maddesinde tanımlanan önemlilik kriteri dikkate alınır.

(3) Denetçi, kuruluşun destek hizmeti alarak gerçekleştirdiği hizmetlerin bilgi sistemlerini ve iş süreçlerini nasıl etkilediğini göz önünde bulundurur, denetimini buna göre planlar ve etkin bir denetim yaklaşımı geliştirir.

(4) İş süreçleri denetimi her yıl, bilgi sistemleri denetimi iki yılda bir kez yapılır. Kurum, gerekli gördüğü hallerde denetlenenlerden herhangi biri ya da tüm denetlenenler için, bu denetimlerin kapsamını ve sıklığını farklılaştırabilir.

İş akış şemaları ve yönetim beyanı

MADDE 11 – (1) Kuruluş iş süreçleri üzerinde kontrollerin ve iş adımlarının gösterildiği iş akım şemalarını oluşturmakla ve kuruluşun iç kontrolleri hakkında denetim dönemi itibarıyla güvence veren BSDHY'nin 33 üncü maddesi ve diğer alt düzenlemelerde belirtilen yönetim kurulu onaylı yönetim beyanını her denetim döneminde hazırlamakla yükümlüdür.

Denetim görüşünün oluşturulması ve denetim mektubu

MADDE 12 – (1) Kuruluşta gerçekleştirilen denetim sonucunda BSDHY'nin 5 inci ve 7 nci maddelerinde belirtilen hükümler ile 34 üncü maddesinde belirtilen görüş çeşitleri çerçevesinde; olumlu, şartlı veya olumsuz görüşe varılması hallerinde, sırasıyla Ek-1, Ek-2, Ek-3'te yer alan örneklere uygun olarak denetim mektubu düzenlenir. Görüş bildirmekten kaçınmayı gerektirecek şartların varlığı halinde ise, denetim mektubu Ek-4'te yer alan örneğe uygun olarak düzenlenir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Kuruluşun tabi olduğu diğer düzenlemeler

MADDE 13 – (1) Tebliğde hüküm bulunmayan hallerde; kuruluşun tabi olduğu diğer düzenlemelerde ve uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan hükümler uygulanır.

Risk merkezi yönetiminin sorumluluğu

MADDE 14 – (1) Bu Tebliğ ile kuruluşun üst yönetimi ve yönetim kuruluna getirilen yükümlülükler, Risk Merkezi için Risk Merkezi Yönetiminin sorumluluğundadır.

Geçiş süreci

GEÇİCİ MADDE 1 – (1) Kuruluş mevcut faaliyet ve sistemlerini 1/1/2015 tarihine kadar bu Tebliğde yer alan hükümlere uygun hale getirir.

(2) Kuruluş, destek hizmeti aldıkları kuruluşlar ile imzaladıkları sözleşmeleri ve durumlarını birinci fıkrada belirtilen tarih itibarıyla bu Tebliğ hükümlerine uygun hale getirir.

(3) Kuruluş iş akış şemalarını 1/1/2014 tarihine, yönetim beyanını 30/1/2015 tarihine kadar hazırlar.

(4) Kuruluş 1/1/2014 tarihinden itibaren bilgi sistemleri ve iş süreçleri denetimlerini yetkili kuruluşlara yaptırmakla yükümlüdür.

Yürürlük

MADDE 15 – (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

EK-1

BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ DENETİM RAPORU
Olumlu Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ kapsamında *(bilgi sistemleri ile)** iş süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin denetlenen nezdinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri ile iş süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../.....tarih ve ……..sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ile iş süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri ile iş süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız Denetçi Görüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla (*bilgi sistemleri ile)** iş süreçleri üzerinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve Tarihi	Sorumlu Bilgi Sistemleri Baş Denetçisinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı	Sorumlu Ortak Baş Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

* Gerçekleştirilen denetimin kapsamına göre uygun ifade tercih edilir.

** Risk Merkezi dışındaki kuruluşlar için tercih edilecektir.

Not: Risk Merkezi için verilen görüş Risk Merkezi Yönetimi'ne hitaben hazırlanır.

EK-2

BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ DENETİM RAPORU
Şartlı Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ kapsamında *(bilgi sistemleri ile)** iş süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin denetlenen nezdinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri ile iş süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../.....tarih ve ……..sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ile iş süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri ile iş süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri ile iş süreçleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemleri ile iş süreçlerinin bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız Denetçi Görüşü]
Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,* denetlenenin *(bilgi sistemleri ile)** iş süreçleri üzerinde bu *hususun/hususların* muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla (*bilgi sistemleri ile)** iş süreçleri üzerinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve Tarihi	Sorumlu Bilgi Sistemleri Baş Denetçisinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı	Sorumlu Ortak Baş Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

* Gerçekleştirilen denetimin kapsamına göre uygun ifade tercih edilir.

** Risk Merkezi dışındaki kuruluşlar için tercih edilecektir.

Not: Risk Merkezi için verilen görüş Risk Merkezi Yönetimi'ne hitaben hazırlanır.

EK-3

BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ DENETİM RAPORU
Olumsuz Görüş

..... A.Ş. Yönetim Kuruluna:
..... A.Ş.'nin ...../...../..... tarihi itibarıyla ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ kapsamında *(bilgi sistemleri ile)** iş süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin denetlenen nezdinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri ile iş süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../.....tarih ve ……..sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ile iş süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri ile iş süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri ile iş süreçleri üzerindeki kontrollerin etkin, yeterli ve uyumlu bulunmama sebepleri)

[Bağımsız Denetçi Görüşü]
Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla (*bilgi sistemleri ile)** iş süreçleri üzerinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme Yeri ve Tarihi	Sorumlu Bilgi Sistemleri Baş Denetçisinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı	Sorumlu Ortak Baş Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

* Gerçekleştirilen denetimin kapsamına göre uygun ifade tercih edilir.

** Risk Merkezi dışındaki kuruluşlar için tercih edilecektir.

Not: Risk Merkezi için verilen görüş Risk Merkezi Yönetimi'ne hitaben hazırlanır.

EK-4

BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ DENETİM RAPORU
Görüşten Kaçınma

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ kapsamında *(bilgi sistemleri ile)** iş süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]
Bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin denetlenen nezdinde *(...../...../.....tarih ve ……. sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik ile)* ** ...../...../.....tarih ve …… sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]
Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri ile iş süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve ...../...../.....tarih ve ……..sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ile iş süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]
Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri ile iş süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetçinin görüş bildirmemesinin nedenleri)

[Bağımsız Denetçi Görüşü]
Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla *(bilgi sistemleri ile)** iş süreçleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme Yeri ve Tarihi	Sorumlu Bilgi Sistemleri Baş Denetçisinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı	Sorumlu Ortak Baş Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

* Gerçekleştirilen denetimin kapsamına göre uygun ifade tercih edilir.

** Risk Merkezi dışındaki kuruluşlar için tercih edilecektir.

Not: Risk Merkezi için verilen görüş Risk Merkezi Yönetimi'ne hitaben hazırlanır.