**Risk Merkezi Verilerinin Güvenliğine İlişkin**

**İyi Uygulama Rehberi**

İÇİNDEKİLER

[BİRİNCİ KISIM 2](#_Toc535834562)

[1-Amaç ve Kapsam 2](#_Toc535834563)

[İKİNCİ KISIM 2](#_Toc535834564)

[2-Tanımlar 2](#_Toc535834565)

[ÜÇÜNCÜ KISIM 3](#_Toc535834566)

[3- RM Süreçlerine İlişkin Strateji ve Standartların Belirlenmesi 3](#_Toc535834567)

[DÖRDÜNCÜ KISIM 3](#_Toc535834568)

[4- RM Süreç Sorumluları Tarafından Belirlenen Önlemlerin Alınması 3](#_Toc535834569)

[A. Yetki ve Sorumlulukların Belirlenmesi: 4](#_Toc535834570)

[B. Sorguların İncelenmesi 4](#_Toc535834571)

[BEŞİNCİ KISIM 5](#_Toc535834572)

[5- Risk Merkezi Süreçlerinde Bilgi Sistemleri Sorumluları Tarafından Belirlenen Önlemlerin Alınması 5](#_Toc535834573)

[A- Risk Merkezi verilerinin gizliliğinin ve bütünlüğünün sağlanması 5](#_Toc535834574)

[C- RM Verilerinin İşlendiği ve Saklandığı Sistemlerde Değişiklik Yönetiminin Sağlanması 7](#_Toc535834575)

[D- RM Verilerinin İşlendiği ve Saklandığı Sistemlerde Denetim İzlerinin Yönetimi 8](#_Toc535834576)

[E- Destek Hizmeti Alımı ve Yönetimi 9](#_Toc535834577)

[ALTINCI KISIM 9](#_Toc535834578)

[6- RM Süreçlerine İlişkin Gözetim Faaliyetlerinin Tasarlanması 9](#_Toc535834579)

[7- RM Süreçlerine İlişkin Gözetim Faaliyetlerinin İşletilmesi 10](#_Toc535834580)

[A - İş Süreçlerinde Kontrollerin Gözden Geçirilmesi 10](#_Toc535834581)

[B - Bilgi Sistemi Süreçlerinde Kontrollerin Gözden Geçirilmesi 11](#_Toc535834582)

# BİRİNCİ KISIM

## 1-Amaç ve Kapsam

Bu rehberin amacı; Risk Merkezi Üyelerinin, Risk Merkezinden sorgulama yoluyla veya toplu paylaşım yöntemleriyle elde etmiş oldukları verilerin güvenli bir şekilde saklanması, işlenmesi ve bütünlüğünün korunması için uygulanması gereken kontrollerin ve alınması gereken önlemlere ilişkin iyi uygulamaların tanımlanmasıdır.

Üye ile paylaşılan Risk Merkezi Verilerinin güvenliğini sağlamak adına iyi uygulama rehberinde tarif edilen süreçlerin Üyeler nezdinde tesis edilmesi ve işletilmesi beklenmektedir.

Rehber, Risk Merkezi Yönetiminin 18 Nisan 2018 tarih ve 40 no.lu kararına istinaden hazırlanmıştır.

# İKİNCİ KISIM

## 2-Tanımlar

Risk Merkezi(RM): Risk Merkezi: Kanunun 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 veya tüzel kişiler ile de paylaşılmasını sağlamak üzere Türkiye Bankalar Birliği nezdinde kurulan, ayrı bir tüzel kişiliği bulunmayan Türkiye Bankalar Birliği Risk Merkezini,

Risk Merkezi Verisi: Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği ve Risk Merkezi Genelgesi kapsamında Risk Merkezi tarafından toplanan ve paylaşılan bilgileri,

Risk Merkezi Sorgulamaları(Sorgu): Üyelerce Risk Merkezinin İnternet Sitesi ve/veya sistem entegrasyonu (mainframe/Webservis vb.) vasıtasıyla Risk Merkezi verilerinin münferiden veya toplu sorgulanmasını,

Risk Merkezi Süreçleri: Üye nezdinde Risk Merkezi verilerinin tamamen veya kısmen otomatik olan veya olmayan yollar ile oluşturulduğu, elde edildiği, alındığı, kaydedildiği, depolandığı, muhafaza edildiği, işlendiği, yönetildiği, iletilir hale getirildiği ve iletildiği süreçleri,

DTS: Risk Merkezinin Dosya Transfer Sistemi olarak tanımlanan FTP‘sini,

Trend Raporu: Risk Merkezi tarafından üyelere sunulan, üyelerin günlük, aylık ve yıllık olarak uygulama bazında yaptıkları münferit sorgulama adetleri, kullanıcı ve ürün bazlı özet ve detay trend raporlarını,

RM Kontrol Hedefleri: Risk Merkezi Üye Denetim Genelgesi'nde tariflenen Risk Merkezi Tarafından İletilen ve Saklanan Bilgilerin Doğruluğunun, Güvenliğinin ve Güncelliğinin Sağlanmasına Yönelik Üyeler Tarafından Alınması Gereken Önlemler ile Üyeler Tarafından Alınacak Önlemlerin Denetlenmesinde Kullanılacak Kontrol Hedefleri Dokümanını,

Bilgi Güvenliği Politikası: Risk Merkezi Genelgesi’nin ekinde yer alan Bilgi Güvenliği Politikasını,

Üye Denetçileri: Üyenin İç Sistemler bünyesinde faaliyet gösteren Teftiş Kurulu / İç Denetim/ İç Kontrol Ekiplerini,

ifade eder.

# ÜÇÜNCÜ KISIM

## 3- RM Süreçlerine İlişkin Strateji ve Standartların Belirlenmesi

Risk Merkezi Üyeleri, RM Kontrol Hedefleri Dokümanı ve Bilgi Güvenliği Politikasına uygun olarak RM sorgularının işlenmesi, saklanması ve denetim izlerinin alınmasına ilişkin stratejilerini oluşturur ve iç politikalarında RM Verilerinin izlenmesi, saklaması ve yetkilendirmesine yönelik standartları belirler. Üye, üst yönetimi tarafından onaylanmış standartlara ve RM Kontrol Hedefleri kapsamında alınması gereken tedbirlere uyum konusundaki kontrol / denetim süreçlerinde sorumluluk ataması yapar ve bu çalışmaların belirli periyotlarda gerçekleştirilmesini sağlar.

Üye, Risk Merkezi’nden sorgu ve/veya FTP yöntemi ile elde etmiş olduğu verileri bünyesinde tutma kararı vermesi durumunda bu veriler hakkında, RM Kontrol Hedefleri Dokümanında belirtilen “Veri İletimi - Alımı Esnasında Dikkate Alınması Gereken Önlemler” ’e uygun olacak şekilde veri stratejilerini belirler.

Üye, iç politikalarında RM verilerine ilişkin asgari standartları aşağıda listelenen şekilde belirler.

1. Personelin bilgi güvenliği farkındalığını arttırmaya yönelik faaliyetler düzenler, bu faaliyetlerin sürekliliğini sağlar ve farkındalığın gelişimini takip eder.
2. RM süreçlerinde belirlenen stratejilere uyuma dair kontrol veya denetim sorumlularını ve bu çalışmaların periyodunu belirler.
3. Verilerin tutulduğu sistemler arasındaki iletişimi, iletişim protokollerini ve bu protokollerdeki minimum güvenlik standartlarını belirler.
4. RM verisinin saklandığı, işlendiği ve iletildiği sistemler özelinde erişim standardı belirler.
5. RM Verisi bulunan sistemlerden alınması gereken denetim izlerini belirler.
6. Veri depolama ve saklama sürelerine dair standartları belirler.
7. RM verisinin gizlilik kriterleri doğrultusunda; iş ihtiyacı dışındaki personele, müşteriye veya 3. Parti kullanıcılara iletilmemesine yönelik standartlar belirler.
8. Yazılım geliştirme süreçlerini, RM verilerinin gizliliğini, bütünlüğü ve erişilebilirliğini sağlayacak şekilde oluşturulmasını ve işletilmesini sağlar.
9. RM verisinin üretim ortamı dışına aktarılmamasına, aktarım ihtiyacı bulunması durumunda ise verilerin maskelenmesine(anonim hale getirilmesine) yönelik standartları belirler.
10. Veri depolama ve saklama sürelerine dair standartları belirler.
11. İş sürekliliği planlaması kapsamında RM verisi bulunan sistemlerin ikincil sistemlere(Olağan Üstü Durum Merkezi’ne) güvenli bir şekilde aktarılması ve bu ortamlarda güvenli bir şekilde saklanmasına yönelik standartları belirler.

# DÖRDÜNCÜ KISIM

## 4- RM Süreç Sorumluları Tarafından Belirlenen Önlemlerin Alınması

Risk Merkezi Üyeleri, RM süreçlerinin RM Kontrol Hedefleri ve Bilgi Güvenliği Politikasına uygun olacak şekilde oluşturulmasını ve stratejilerinde/politikalarında belirlemiş olduğu koşullar çerçevesinde işletilmesini sağlar.

Üye, Risk Merkezi süreçlerinden sorumlu iş birimi / birimleri tarafından asgari olarak aşağıdaki konularda süreçler oluşturur ve bu süreçlerin kontrollü bir şekilde işletilmesini sağlar.

### Yetki ve Sorumlulukların Belirlenmesi:

Üye, RM verileri için erişim politikalarında belirlemiş olduğu standartların sağlanması adına erişimleri düzenler ve üst yönetimi tarafından onaylanmış prosedürleri doğrultusunda, uygular. Yetki ve sorumlulukların atanmasında organizasyonel birim ve unvan kısıtlarını göz önünde bulundurur. Yetki ve/veya sorumluluk atanan organizasyonel birimlerde, verilerin depolandığı ve işlendiği her ortamda görevlerin fonksiyonel ayrımına yer verilir.(Örneğin veritabanı üzerinde analiz rolünde çalışan personele sadece gözlem -Select- yetkisi verilirken operasyon rolünde çalışan personele iş çalıştırma -Execute- yetkisi tanımlar vb.)

Risk Merkezi Süreçlerinde yetki ve sorumluluk atanan çalışanlar için Üye, aşağıda belirtilen konularda gerekli önlemleri alır.

1. Çalışanlarına bilgi güvenliği politikası kapsamındaki rol ve sorumluluklarını bildirir ve bu konularda periyodik olarak eğitim almasını sağlar.
2. Çalışanlarının işe başlangıcı ile birlikte gizli verilerin kurum dışına çıkartılmamasına yönelik sözleşme (non-disclosure) imzalanmasını sağlar.
3. Çalışanlarının ve üçüncü tarafların, Üye güvenlik politikaları, Prosedürleri ve bu dokümanlardaki değişikliklerden haberdar olmasını sağlar.
4. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde yapılması gerekenleri (Bilgi varlıklarının tahsisi/iade alınması/değiştirilmesi, erişim yetkilerinin kapatılması vb. konularda) açıkça belirler ve bu konularda ilgili kişilere sorumluluk atar.

### Sorguların İncelenmesi

Üye, Risk Merkezi sorgulama yetkisi bulunan bölüm/birim özelinde sorgulama adetlerinin incelenmesine yönelik süreç işletir. Sorgulama yetkilerinin incelenmesinde RM ile entegre çalışan sistemler (entegre sistemler) ve RM Web Sitesi ([www.riskmerkezi.org.tr](http://www.riskmerkezi.org.tr)) üzerinde tanımlı yetkiler ve bu yetkiler ile gerçekleştirilen sorgulamalar kıstas alınır.

Sorgulama yapan birimler, entegre sistem vasıtasıyla ve RM Web Sitesi üzerinden gerçekleştirilen sorgulamaların incelemesini yapar. Bu kontrollerde dikkate alınması gereken işlemler asgari olarak aşağıdaki kontrolleri içerir.

1. Sorgu sayısı, birim ortalamasının üzerinde olan kullanıcılar.
2. İş ihtiyacı kapsamında sorgulama gereksinimi bulunmayan kullanıcılar ve işlemler.
3. Sorgu sayısı bir önceki dönemlere göre artış gösteren (trend analizi pozitif çıkan) kullanıcılar.
4. Üye’nin potansiyel müşteri segmenti dışında şirket / şahıs sorgulaması yapan kullanıcılar.
5. TBB Risk Merkezi Rapor hizmeti sağlayan Üyelerde Rapor hizmetine aracılık edilirken gerçekleştirilen işlemlerin başvuru talebi ile ilişkisi (örneğin, başvuru evraklarının kontrolü).

Sorgulama yapan birimler, bu kontrollerde tespit edilen uyumsuzlukların Üye Denetçilerine bildirilmesi, Üst Yönetime raporlanması ve sorunların giderilmesi adına aksiyon planı oluşturulmasından sorumludur. Bahsi geçen kontrollerde görev dışı kullanımın, suistimalin veya suistimal şüphesinin tespit edilmesi durumunda ilgili iş birimi, Üye Denetçilerine ve Bilgi Güvenliği Politikasında yer alan E.2 ve F.3 maddeleri kapsamında Risk Merkezi’ne bildirimde bulunur.

# BEŞİNCİ KISIM

## 5- Risk Merkezi Süreçlerinde Bilgi Sistemleri Sorumluları Tarafından Belirlenen Önlemlerin Alınması

Üye, bilgi sistemlerinde bulunan Risk Merkezi verilerinin güvenliğini, bütünlüğünü ve erişilebilirliğini sağlamak için gerekli önlemlerin alınmasını ve bu süreçlerin sürekliliğine yönelik gözetim süreçlerini oluşturur. Bu süreçlerin tasarımı, işletimi ve kontrolüne/denetimine yönelik sorumlulukları organizasyonel seviyede belirler.

### A- Risk Merkezi verilerinin gizliliğinin ve bütünlüğünün sağlanması

Üye, Risk Merkezi süreçleri kapsamındaki bilgi sistemlerinde verilerde gizliliğin ve bütünlüğün sağlanması adına gerekli bilgi sistemleri süreçlerini oluşturur. Bu süreçlerin Politika ve Prosedürlerinde yer almasını sağlar.

Bu kapsamda Üye,

1. Bilgi güvenliği kapsamında maruz kalabileceği risklerin önceden tespiti, ölçümlenmesi ve yönetimi konularını kapsayacak şekilde bir bilgi güvenliği metodolojisi oluşturur. Bilgi güvenliği metodolojisinin periyodik olarak test edilmesi için kurumun risk iştahı, sektörel risk alanları ve geçmiş denetim bulgularını değerlendirir ve metodolojinin risk politikası ile uyumu konusunda güvence sağlar.
2. Bilgi sistemlerinde güncel güvenlik gereksinimlerini karşılayacak şekilde kullanıcı yönetimi ve kimlik doğrulama altyapısını oluşturur. Kullanıcılar, türlerine göre (örneğin: yönetici, operatör, son kullanıcı gibi) sınıflandırılarak farklı güvenlik önlemlerine tabi tutulmaları sağlanır. Bilgi sistemlerinde tutulan Risk Merkezi verilerine erişimlerin iş ihtiyacı doğrultusunda olması, minimum yetki ve görevler ayrılığı prensipleriyle uyumlu olması sağlanır.
3. Bilgi sistemi ortamlarının tamamında kullanıcı şifrelerinin genel kabul görmüş güvenlik standartları ile uyumlu olmasını sağlar. Şifrelerin herhangi bir ortamda açık şekilde(cleartext) yer almasını önler ve şifre saklanan ortamların en güncel algoritmayla şifrelenmesini sağlar. Dışarıdan erişimlerde bu önlemlere ek olarak iki faktörlü doğrulama mekanizması kullanır.
4. Bilgi sistemlerinde ortak kullanıcı hesabının kullanılmaması esas olmakla birlikte, teknik gereksinimlerden dolayı genel kullanıcı hesabı kullanılması durumunda; bu hesap ile gerçekleştirilen her işlem için, bu dokümanın 5-D maddesinde belirtilen hususlarda denetim izi tutulmasını ve gerçekleştirilen işlemlerin gözden geçirilmesini, sağlar.
5. Farklı görev ve sorumlulukları bulunan birimlerde iş ihtiyaçları çerçevesinde tek bir sorgu ekranı yerine ihtiyaca özel ekranlar/raporlar/yetkilendirme seviyesi tasarlar. Yetki seviyelerinin tasarımında verilerin/raporların uygulama dışına çıkartılmasına yönelik fonksiyonlar (çıktı alınması, pdf, doc, formatlarında bilgisayara indirilmesi gibi) dahil edilir ve bu şekilde iş ihtiyacı dışında verilerin uygulama dışına çıkartılması sınırlandırılır.
6. Risk Merkezi verilerinin iş ihtiyacı dışında erişime açık alanlarda tutulmaması sağlanır. Dosya sunucusu (File Server), çıktı saklama/işleme sunucuları (Print Server) ve benzeri alanlar düzenli aralıklarda taranarak gizli verilerin ortak erişim alanlarından kaldırılmasına yönelik süreçler işletilir.
7. Risk Merkezinden aldığı bilgileri saklamak ve işlemek amacıyla kullandığı sistemlerin tutulduğu iletişim altyapısının (kurumsal ağ), dış ağlar ile iletişimde bulunması durumunda, bu dış ağlardan gelebilecek tehditlerin tespit edilmesini, önlenmesini, dış ağdan iç ağa erişimlerin kontrol altında tutulmasını ve bu erişimlerin kontrollü geçişinin sağlanmasını temin etmek amacıyla gerekli ağ kontrol ve güvenlik sistemlerini tesis eder.
8. Risk Merkezi verisi bulunan bilgi sistemlerinde iletişim altyapısının dış ağlar ile etkileşimi konusunda gerekli güvenlik önlemlerini almaktan sorumludur. Bu önlemler; genel kabul görmüş kuralları, güncel sistem zafiyetlerini ve RM Kontrol Hedefleri Dokümanının 4.2 alt başlığında tarif edilen kontrol hedefleri göz önünde bulundurularak oluşturulur.
9. Kurum ağı dışından gerçekleştirilen tüm uzaktan erişimlerde erişim sağlayan istemcilerin işletim sistemi, yama ve antivirüs kontrolünün yapılması (host checker) sağlanır. Ek olarak VPN ile erişimlerdeki bağlantının şifreli olması ve şifreleme yönteminin güncel olması sağlanır.
10. Bilgi sistemlerinin güvenliğini sağlamak adına düzenli periyotlarda sızma testi yaptırır. Sızma testi sonuçlarında etki olasılığı değerlendirilerek kritik risklerin makul sürelerde bertaraf edilmesini sağlar.
11. Üye, bilgi sistemlerinde kullanılabilecek güvenli uygulamaları belirler. Bu uygulamalar dışında bulunan ve zararlı nitelikli olduğu değerlendirilen programların çalıştırılması ve kurulması merkezi politikalar ile engellenir. Bu politikaya ek olarak üye, sistem yöneticileri dışındaki personele lokal yönetici hakkı tahsis etmez.
12. İkincil merkeze iletilen Risk Merkezi verilerinin güvenli iletişim protokolleri ile gönderilmesine yönelik konfigürasyonları yapar ve iletişim kanalında uygulanan şifreleme mekanizmasının günümüz standartlarına uygun olmasını sağlar.
13. Üye Kuruluş bünyesinde veri sızıntısı önlemeye yönelik sistemlerin bulunması durumunda RM verilerinin kurum dışına çıkarılması ile ilgili senaryo bazında RM verisine özel kurallar ve izleme yöntemleri belirlenir.
14. Toplu veya münferit sorgu yöntemiyle temin edilen Risk Merkezi verisinin sistem dışına çıkartılmasını engelleyecek önlemler alınır. Sistem dışına çıkartılmaya çalışılan kritik belgelerin gözden geçirilmeden iletilmemesi sağlanır. Dışarıya veri çıkışı olabilecek ortamlar (USB, CD, DVD, Printer, Mail veya internet sitesine/bulut servisine veri yükleme vb..) ve bu ortamlardaki veri çıkış senaryoları (şifreli ve parçalı .zip dosya gönderimi, dosya uzantısı değiştirilerek iletimi, taranan dosyaları printer üzerinden mail atma vb ..) periyodik olarak gözden geçirilir ve veri sızıntısını engelleyici sistem politikalarının (DLP -Data Leakage Prevention, Firewall-Güvenlik Duvarı kuralları, Proxy -Ağ geçidi, Active Directory -Aktif Dizin vb..) güncellenmesi sağlanır.
15. Risk Merkezi verisinin mobil cihaz vasıtasıyla iletilmesi, görüntülenmesi veya depolanması kurumsal çözümler vasıtası ile (Mobil cihaz yönetim uygulamaları vasıtasıyla) sağlanır. Mobil cihaz yönetim uygulamaları özelinde konfigürasyonların genel kabul görmüş kriterler çerçevesinde uygulanması ve güncellenmesi zorunlu tutulur. Kişisel kullanım amaçlı cihazlar üzerinden Risk Merkezi verilerine erişimler engellenir.
16. Risk Merkezi verisi bulunan sunucuların internet erişimleri, iş ihtiyacı ile sınırlı olacak şekilde sağlanır. Aksi durumlar için engelleme politikaları uygulanır. Uygulamaların otomatik güncellenmesi, güvenli olmayan network bağlantıları, zararlı sitelere erişimler ve benzeri bağlantı taleplerini engellemeye yönelik konfigürasyonlar uygulanır.
17. Üye, bilgi sistemlerinin güvenliğini sağlamak amacıyla son kullanıcı bilgisayarlarında, mobil cihazlarda ve sunucularda kullandığı güvenlik uygulamalarının güncel olmasını sağlar. Zararlı yazılım bulunan sistemlerin erken keşfedilebilmesi için bilgi sistemlerinin her katmanında(Firewall, Antivirüs, Proxy vb..) imzaların güncel olmasını ve son kullanıcıların bu sürece müdahalesinin engellenmesini sağlar.
18. Uygulamaların güvenlik denetimlerini periyodik olarak gerçekleştirir. Güncel tehditleri göz önüne alarak gerekli olan sistem güncellemelerinin yapılmasını sağlar.
19. Bilgi güvenliği vakalarının yönetimi konularını kapsayan Olay Yönetimi Sürecini tanımlar ve bu kapsamda gerçekleşen veya gerçekleşme riski olan vakaların sürekli değerlendirilmesini sağlar.
20. Bilgi güvenliği alanında sürekliliğinin sağlanması için asgari güvenlik konfigürasyonları belirler ve en az yıllık periyotlarda bu standartlara uyumun gözden geçirilmesini sağlar.

B- RM Verilerine Erişilebilirliğin Sağlanması

Üye, Risk Merkezi süreçleri kapsamındaki bilgi sistemlerinde erişilebilirliğin üst seviyede tutulması için gerekli bilgi sistemleri süreçlerini oluşturur. Bu süreçlerin Politika ve Prosedürlerinde yer almasını sağlar.

Bu kapsamda Üye,

1. Birincil sistemlerin kullanılamaz hale gelmesi ihtimaline karşın ikincil sistemlerini kurar. İkincil sistemlerin, birincil sistemler ile aynı fiziksel ve çevresel riskleri taşımamasını sağlar.
2. Yedeklenen verilerin geri dönüş testlerini(recovery test) belirli aralıklarda planlar ve söz konusu planlar doğrultusunda bu yedeklerin bir felaket durumunda işletilebilmesini garanti altına almaya yönelik kontrol ortamı kurar.
3. Risk Merkezi tarafından acil durum ve kurtarma faaliyetleri kapsamında planlanan ve tüm üyelerin katılımıyla gerçekleştirilecek olan testlerin tamamına zamanında katılım sağlar. Üye, test süresince ve test sonrası sonuçların değerlendirilmesine ilişkin gerekli operasyonel desteği sağlar.
4. Dış hizmet alımı ile gerçekleştirilen yazılım geliştirme faaliyetlerinde üçüncü bir firma ile kaynak kod saklama(escrow) sözleşmesi yapar. Saklanan kaynak kodların güncelliğini belirli periyotlarda kontrol eder.

### C- RM Verilerinin İşlendiği ve Saklandığı Sistemlerde Değişiklik Yönetiminin Sağlanması

Üye, Risk Merkezi süreçleri kapsamındaki bilgi sistemlerinde etkin bir değişiklik yönetimi süreci oluşturur. Bu süreçlerin Politika ve Prosedürlerinde yer almasını sağlar.

Bu kapsamda Üye;

1. Kurum politikalarında ve Prosedürlerinde RM verilerinin tutulduğu ve işlendiği uygulamalardaki geliştirmelerini, test ve işletim faaliyetlerine yönelik süreç adımlarını, sorumluluklarını ve yetki seviyelerini tanımlar. Yetkilerin tanımlanmasında; görevler ayrılığı prensibini, minimum yetki prensibini ve giriş-onay mekanizmasını göz önünde bulundurur. Bu kapsamda yazılım geliştirme personelinin ve dış hizmet sağlayıcı firma personelinin üretim ortamında Risk Merkezi verilerine erişmemesini sağlar.
2. RM verilerinin tutulduğu uygulamalarda üretim ortamının, test ve geliştirme ortamından ağ seviyesinde mantıksal ve/veya fiziksel olarak ayrıştırılmasını sağlar. Bununla birlikte üretim ortamı dışındaki ortamlarda RM verisinin bulunmamasını sağlar.
3. Uygulama geliştirmelerinin, değişikliklerinin veya konfigürasyonların aktarma/taşıma uygulaması vasıtasıyla üretim ortamına alınmasını sağlar. Aktarma/taşıma işlevi gören uygulama üzerindeki işlemlerin takip edilmesi için, Rehberin 4. maddesinde belirtilen detayda, denetim izlerinin oluşturması sağlanır.
4. Üretim ortamına taşınması planlanan paketlerin sistemsel onay mekanizmalarına tabi olması ve onaysız paketlerin üretim ortamına aktarılmaması sağlanır. Üretim ortamına taşınan uygulama geliştirmeleri ve/veya değişiklikleri versiyonlama yöntemi ile kayıt altına alınarak değişikliklerin analiz edilebilir yapıda olması sağlanır.
5. Dış hizmet alımı ile veya iç sistemlerinde işletilen uygulama geliştirme süreçlerinin asgari olarak; “Talep”, “Analiz”, “Geliştirme”, “Fonksiyon Testi”, “Kullanıcı Kabul Testi” ve “Güvenlik Testi” süreçlerini kapsaması sağlanır. Bahsi geçen süreçlerin kayıt altında olması ve üretim ortamına geçiş için kurgulanması gereken sistemsel onay mekanizmasına dahil olması sağlanır. Geliştirmelerin üretim ortamına geçebilmesi için bu süreçlerin tamamlanmış olması sağlanır.
6. Dış hizmet alımı ile geliştirilen uygulamaların veya uygulama değişikliklerinin, yetkili kurum çalışan(lar)ı tarafından üretim ortamına aktarılması sağlanır.
7. Uygulamalardaki yetki seviyelerinin RM verilerinin/raporlarının uygulama dışına çıkartılmasına yönelik fonksiyonların(Ekran Görüntüsü, Çıktı -print- alınması, kopyala/yapıştır, pdf/doc/xls raporu indirilmesi... gibi) farklı yetki gruplarına atanacak şekilde ayrıştırılması sağlanır.
8. RM verilerinin sorgulanması için serbest sorgu ekranı yerine sorgulamanın Üye Kuruluşun bir faaliyeti ile ilişkilendirilerek yapılmasını sağlayacak süreç ve ekranlar tasarlanır.(Örneğin, kredi başvuru sürecinde sorgulama yapılan ekran ile tahsis sürecinde sorgulama yapılan ekranın farklı olması)
9. Uygulama tarafından RM verilerinin iletiminde; istemci, sunucu ve veri tabanı arasında güncel şifreleme yöntemleri kullanılır.
10. İç politikalarında uygulama değişiklik süreçleri kapsamındaki acil değişiklik yönetimini tanımlar. Acil değişikliklerin asgari olarak bir GMY tarafından onaylanmış olmasını ve değişiklik sonrası gerekli testlerin yapılmasını ve onayların alınmasını sağlar.

### D- RM Verilerinin İşlendiği ve Saklandığı Sistemlerde Denetim İzlerinin Yönetimi

Üye, Risk Merkezi süreçleri kapsamındaki bilgi sistemlerinde yeterli detayda denetim izi (log) oluşturmasını, belirli periyotlarda saklanmasını ve güvenliğini sağlar. Üye, bilgi sistemlerinde üretilen denetim izlerinin gizliliği, bütünlüğü ve erişilebilirliğini sağlamak için bünyesinde etkin bir denetim izi (log) yönetimi süreci işletir.

Bu kapsamda Üye;

1. RM verilerinin tutulduğu sistemlerin tüm kullanıcılar için denetim izi tutmasını sağlar. Denetim izlerinin uygulama, işletim sistemi, veritabanı ve iletişim sistemlerinden toplanmasını ve toplanan denetim izlerinin, bütün iş sürecini kapsayacak şekilde ve her bir süreç için uçtan uca izlenebilir bir yapıda olmasını sağlar. Denetim izleri asgari olarak;
2. RM verilerinin sorgulanması, değiştirilmesi veya silinmesi,
3. RM verilerine yetkisiz erişim teşebbüsü,
4. RM Süreçleri kapsamındaki sistem konfigürasyonlarının değişikliği,
5. RM verisi bulunan programların taşınması/ aktarılması,

RM verisi üzerinde yetki tanımı, değişikliği ve iptali süreçlerini kapsamalı ve en az aşağıdaki detayları içermelidir.

1. İşlemin gerçekleştirildiği uygulama.
2. İşlemin gerçekleştirildiği cihazı tanımlayan bilgiler.
3. İşlemi gerçekleştiren kişi bilgisi, mümkün olmadığı durumlarda ip bilgisi.
4. Yapılan işlemin detayı (izleme, çıktı alma, değiştirme, silme, ekleme... gibi).
5. Yapılan işlemin hangi müşteriye/müşterilere yönelik olduğu.
6. Yapılan işlem zamanı(sistemlerde zaman senkronu yapılması veya zamanın son kullanıcı tarafından değiştirilememesine yönelik konfigürasyon yapılması gerekmektedir).
7. Denetim izlerinin merkezi yönetim aracı vasıtasıyla alınması ve saklandığı alanların müdahaleye kapalı olması, acil veya istisna müdahalelerin ise tespit edilmesi ve kayıt altına alınması sağlanır. Denetim izlerinin üye bünyesinde sürekli takip edilmesi, kritik ve bilgi güvenliği vakası oluşturabilecek durumlarda ise sistemin otomatik alarm üretmesi sağlanır.
8. Denetim izlerinin alınmasında asgari olarak aşağıdaki sistem elemanlarını kapsama alır.
9. Database ve Database Server (veritabanı sunucusu ve veritabanı)
10. Domain Policy (Etki alanı politikaları)
11. Firewall (Güvenlik duvarı)
12. Proxy (vekil sunucu)
13. VPN (Sanal Özel Ağ)
14. File Server (dosya sunucusu)
15. Merkezi denetim izi toplama ve yönetim uygulamaları

### E- Destek Hizmeti Alımı ve Yönetimi

Üye, Bilgi sistemlerinde üçüncü tarafların destek amaçlı yerinden veya uzaktan erişimlerinden kaynaklanabilecek riskleri belirler. Bahsi geçen riskleri, erişim hakkı verilmeden önce değerlendirir ve bu konularda tedbirler alır(yetki seviyesi, denetim izleri, veri çıkışının engellenmesi, eşlik etme, gözetim, denetim izlerinin izlenmesi vb.). Destek hizmeti alımına yönelik sözleşmelerde, üçüncü parti tarafında yürütülen süreçlerin denetlenebileceğine, gizliliğine ve güvenliğine yönelik maddelere yer verir.

Bununla birlikte, Destek Hizmeti kuruluşlarının, RM verilerinin yer aldığı sistemlere erişimleri hususunda Kanunlarda düzenlenen gizli verilerin üçüncü taraflar ile paylaşılması hususları göz önünde bulundurularak gerekli önlemlerin alınması sağlanır. Ayrıca Acil durumlardaki erişimlerin süreli olması, kuruluş gözetiminde gerçekleştirilmesi ve denetim izlerinin tutulması sağlanır.

# ALTINCI KISIM

## 6- RM Süreçlerine İlişkin Gözetim Faaliyetlerinin Tasarlanması

Üye, Risk Merkezi Süreçlerine yönelik alınması gereken tedbirlere uyum konusunda Kontrol / Denetim çalışmaları için organizasyonel seviyede sorumluluk ataması yapar.

Üye, iç sistemlerinin yönetiminde genel kabul görmüş kuralları, iç politikaları / prosedürleri kapsamındaki süreçlerin tasarımını ve işletimi konusunda güvence sağlamak adına denetim/kontrol faaliyetlerini ve periyodunu belirler. Bu faaliyetler, iş süreçlerini ve bilgi sistemleri süreçlerini kapsar.

RM verilerinin üye bünyesine alınması esnasındaki yöntemler göz önünde tutularak(Webservis üzerinden münferit sorgu çalıştırma, toplu sorgu çalıştırma, toplu sorguların üye uygulamaları/veritabanları/Raporlama araçları üzerinden sorgulanması vb..), her bir sorgulama şekli için ayrı yöntemler kullanılarak kontrol faaliyetleri gerçekleştirilir. Sorgulamaların mahiyetinin, sorgu sayılarındaki tutarsızlıkların ve yetkisiz erişimlerin erken tespiti için gereken önlemler alınır. Alınan önlemler asgari olarak aşağıdaki yöntemleri içerir;

**Kontrollerin / Denetimlerin Planlanması**

1. Kontrol ortamının belirlenmesinde, verilerin sorgulama yöntemleri, bilgi sistemlerine kaydedilmesi ve farklı uygulamalarda kullanımı amaçlı aktarılması durumları göz önünde bulundurularak saklama, işleme ve iletilme alanlarında kullanılan sistemler belirlenir.
2. Sistemler üzerindeki kontrol yöntemi ve sorgulama adetlerinin belirlenmesi ile birlikte kontrollerin hangi sıklıkla ve hangi yöntemle yapılacağı planlanır.
3. RM verilerinin sorgulanma yöntemleri(RM Web Ekranı -www.riskmerkezi.org veya ftp üzerinden toplu veri alınması) ve bu yöntemlerde yetkili kullanıcılar tepspit edilir.
4. RM verilerine erişim yetkisi sağlanan organizasyonel birimlerin ve erişimlerdeki iş ihtiyacının değerlendirilmesi sağlanır.
5. Kontrollerin işletilmesi için elde edilen bu verilerin değerlendirilmesi ile birlikte, periyodik gerçekleştirilecek kontrol planı oluşturulur. Plan kapsamında sorguların adetsel, yüzdesel veya trend yöntemi ile kontrolüne yönelik standartlar belirlenir.
6. RM sorgulamalarının hangi iş birimlerinde ve hangi yöntemler ile gerçekleştirileceğine dair Üye politikalarının iç sistemlerinde uygulandığına dair güvence verilmesi sağlanır.
7. Yapılan tüm sorguların (geçmişe dönük) analiz edilebildiği yapıların doğru işlediğine dair güvence verilmesi için; Üye Denetçileri tarafından düzenli inceleme faaliyeti yürütülür.
8. Üye denetçileri tarafından temin edilen kanıt dokümanların ve Üst yönetim raporlamalarının kayıt altına alınması ve asgari 2 yıl süreyle saklanması sağlanır.

## 7- RM Süreçlerine İlişkin Gözetim Faaliyetlerinin İşletilmesi

### A - İş Süreçlerinde Kontrollerin Gözden Geçirilmesi

RM süreçleri kapsamında planlanan kontrollerin "RM Kontrol Hedefleri" dokümanında belirtilen kontrol maddeleri ile uyumlu olması teyit edilir. Kontrol çalışmalarında, sorgu kanalları(RM ile entegre çalışan iç sistemler, RM Web sitesi -www.riskmerkezi.org.tr- gibi) da dikkate alınarak asgari olarak aşağıdaki konular incelenir;

1. Üye'nin risk algısı, risk iştahı, müşteri sayısı, ciro bilgileri, sorgulama yapan personel sayısı, sorgu yapılan müşteri türü ve geçmiş dönem sorgu sayıları göz önünde bulundurularak, sorgu kanalı ve organizasyonel birimler özelinde tahmini sorgulama sayıları belirlenir.
2. Kullanıcı ve kurum nezdinde RM verisi sorgulama adetlerinin trendi ölçümlenir. Bu ölçümleme, RM’den alınan Trend Raporları ile de karşılaştırılır. Sorgulamaların dönemsel olarak artışında veya azalışında etkili kullanıcılar ve en fazla sorgulama yapan kullanıcılar tespit edilerek sorgulamaların iş ihtiyacı ile ilişkisi sorgulanır.
3. RM verilerine sürekli erişim ihtiyacı olmayan kullanıcıların (istisnai) gerçekleştirmiş olduğu sorgulamalar incelenir. Bahsi geçen süre içerisinde kullanıcının erişim yetkisi bulunan istemci veya dosya sunucularına veri aktarımı yapılmadığına dair kontrol gerçekleştirilir.
4. Yapılan sorgulamaların mahiyeti; sorguyu gerçekleştiren personelden bilgi alınarak (müşteri/kredi ilişkisine dayalı olup olmadığına yönelik incelenmesi gibi) kontrol edilir. İşlem adetinin yüksek olması durumunda istatistiki modelleme yöntemiyle seçilebilecek örnekler üzerinden kontrol faaliyeti işletilir.(Örneğin; Trend Raporu kişi bazında alınarak sorgu sayısı standart kabul edilen değerin üzerinde olan örnek işlemler için sorgulama faaliyeti yürütülür)
5. Üye, bünyesinde RM ile entegre çalışan sistem bulunması durumunda, RM Web Sitesi (www.riskmerkezi.org.tr) üzerinden sadece belirli iş ihtiyacı doğrultusunda sorgu çalıştırılmasına yönelik kontrol noktası tanımlar. Bahsi geçen durumda web sitesi üzerinden gerçekleştirilen sorguların mahiyeti ayrıştırılarak iş ihtiyacına uygunluğu(Farklı kanallardan alınan verilerin sistemde kayıtlı veri ile mutabakatı gibi) kontrol edilir. Web sitesi sorgulamalarının iş ihtiyacı ile uyuşmaması durumlarında Risk Merkezi'ne bilgi verilerek kullanıcıların iptal edilmesi sağlanır.
6. Müşteri veya iş ilişkisi bulunmayan sektördeki kişilerin / firmaların sorgulanması ayrıca kontrol edilir.
7. Sorgulama yetkisi tanımlanan birimlerin en az yıllık periyotlarda süreç denetimleri kapsamına dahil edilmesi sağlanır. Bahsi geçen organizasyonların, işlevsel görev ayrımını sağlayacak şekilde oluşturulduğuna dair kontrol/denetim çalışması gerçekleştirilir.
8. Kontrol / Denetimler vasıtasıyla tespit edilen ve Şüpheli sınıfında değerlendirilen kullanıcıların sorgu kanallarındaki yetkilerinin iç sistemlerde ve RM Web Sitesi üzerinde(Risk Merkezi'ne bilgi verilerek) iptal edilmesi sağlanır.

**TBB Risk Merkezi Raporuna ilişkin Kontroller**

TBB Risk Merkezi tarafından gerçek ve tüzel kişilere yönelik sunulan TBB Risk Merkezi Raporuna aracılık eden üyeler, aşağıda belirtilen kontrol maddelerini ayrıca uygular. Üye,

1. Müşteriden alınacak bilgi ve belgeler müşteri bazında kolayca erişilebilecek şekilde saklar.
2. Müşteri başvuru kabulü ve rapor teslimi süreçlerinde kontrollü bir yapı oluşturulur.(örneğin, şube tarafından alınan başvuru ve evrakların merkezi operasyon yönetimi tarafından kontrol edilmesi, müşteri imzası alınmadan rapor teslimi yapılmadığına dair kontrol yapılması)
3. Üye bünyesinde RM’ye bildirimden sorumlu personelin, TBB Risk Merkezi Genelgesinde yer alan usul ve esaslara uygun bildirim yapılması konusunda düzenli aralıklarda eğitim almasını sağlar.
4. RM süreçlerinde görev alan personelin ve ilgili diğer kişilerin, bilgi ve bilgi teknolojileri güvenliği uygulamalarının önemini kavramalarına ve sorumluluklarına ilişkin uygun ve gerekli bilgi güvenliği eğitimlerini almalarını sağlar.
5. RM Sorgulamalarında kullanıcı ve işlem tespitine yönelik denetim kanıtlarının yer alması durumu kontrol edilir.

### B - Bilgi Sistemi Süreçlerinde Kontrollerin Gözden Geçirilmesi

Üye, Risk Merkezi Süreçleri kapsamındaki iç kontrol ortamının değerlendirilmesi ve sürekli gelişimi için bilgi sistemlerinde işletilen kontrol/denetim politikalarını düzenler. Bu düzenlemeler kapsamında RM Verisi bulunan bilgi sistemlerinde Üye denetçileri;

1. Kontrol ortamının RM Kontrol Hedefleri dokümanındaki maddeler ile uyumu konusunda düzenli periyotlarda (günlük/haftalık/aylık/yıllık) kontrol/denetim faaliyeti işletir. Bu çalışmaların belirli periyodlarda üst yönetime raporlanmasını sağlar.
2. Erişimlerin görevler ayrılığı ve minimum yetki prensibi ile uyumlu olduğunu kontrol eder.
3. Her kullanıcı türü için şifrelerin genel kabul görmüş kuralları sağlamasını ve şifreleme altyapısının güncelliğini kontrol eder.
4. Kurumsal ağ üzerinde dış ağlardan gelen tehditlerin tespit edilmesi, önlenmesi ve iç ağa erişimleri kontrol eder, ağ konfigürasyonlarının güncelliğini ve genel kabul görülmüş standartlara uygun olarak yapılandırıldığını kontrol eder.
5. Sunucu konfigürasyonlarında internet erişiminin engellenmesini veya sadece belirli iş amaçlarına uygun olarak yetkilendirilmesini kontrol eder.
6. Erişim alanlarının taranması ve ortak erişim alanlarında RM Verisi bulunmadığını kontrol eder.
7. Sistem şifrelerinin erişime açık alanlarda tutulmadığını, güvenli metotlarla saklandığını kontrol eder.
8. Kişisel kullanım amaçlı cihazların RM Süreçlerinde kullanılması durumunda mobil aygıt yönetim (MDM – Mobile Device Management) uygulaması kullanılmasını ve bu uygulama üzerinde veri sızıntısını önleyen güvenlik önlemlerinin uygulandığını kontrol eder.
9. Kullanıcı bilgisayarlarında bilinmeyen uygulamaların veya dosyaların çalıştırılmasını engelleyen kuralların güncelliğini kontrol eder. Kullanıcılara bu dosyaları çalıştırmak için lokal veya ağ üzerinde yetki verilmediğini kontrol eder.
10. Güvenlik duvarı (Firewall), antivirüs ve ağ geçidi (proxy) gibi zararlı yazılımları tespit eden ve/veya önleyen sistem imzalarının güncel olduğunu kontrol eder.
11. Belirli periyotlarda sızma testi yapıldığını kontrol eder. Gerçekleştirilen sızma testi sonuçlarında tespit edilen kritik bulguların makul sürelerde kapatıldığını teyit eder.
12. Kurum ağının misafir ağı ile ayrıştırıldığını kontrol eder. Kurum bünyesinde kayıtlı olmayan cihazlar ile kurum ağına, kablolu veya kablosuz, bağlantıların güvenlik politikaları ile engellenmiş olması durumunu kontrol eder.
13. Kurum ağına bağlanan cihazlardaki uygulamaların sistemsel politikalarla kontrol edilmesi ve belirlenen güvenlik standartları ile uyumlu olmayan cihazların kurum ağı ile bağlantısının engellendiğini kontrol eder.
14. Veri sızıntısını tespit eden ve önleyen sistemlerde (DLP – Data Leakage Prevention) gerçekleştirilen çalışmalar ve bu sistemlerdeki kural tanımlamalarını gözden geçirir ve güvenlik gereksinimleri ile uyumlu olduğunu kontrol eder. Bahsi geçen sistemde tanımlı kuralların üst yönetim onayı olmaksızın değiştirilmediğini kontrol eder.
15. Kullanılmayan ve güvenli olmayan servis ve bağlantı noktalarının(portların) kapatıldığını kontrol eder.
16. VPN ile dış ağdan kurum ağına bağlantılarda gerekli güvenlik önlemlerinin alınması durumu kontrol edilir. Güvenli olduğu teyit edilmeyen bilgisayarlardan kurum ağına erişimlerin engellendiğini kontrol eder.
17. Toplu sorgulamaların gerçekleştirildiği altyapılarda(İşletim Sistemi/ Veritabanı/ Network/FTP/ File Server gibi) sistem güvenlik prosedürlerinin uygulandığını  
    kontrol eder.
18. Denetim iz (log) kayıtlarının sistem yöneticisi dahil olmak üzere değiştirilemediği, değiştirilmesine yönelik faaliyetlerde ise alarm üretilmesi, durumları kontrol edilir.
19. Denetim izlerinin bu rehberin “Denetim İzlerinin Yönetimi” başlığı altında belirtilen koşullara uyumluluğunu kontrol eder.
20. Toplu çalıştırılan işlerin (job) tasarımı ve çalıştırılması, suistimal riskine karşın düzenli periyotlarda kontrol edilir. Üst yönetim onayı bulunmayan işlerin çalıştırılmadığı teyit edilir.
21. Sistem yedeklerinden geri dönüş testlerinin(recovery test) belirli aralıklarla yapılması ve bu çalışmalarda tespit edilen uyumsuzlukların makul sürelerde giderilmesini kontrol eder.
22. Yazılımcı rolünde çalışan personelin veya dış hizmet personelinin canlı(Prod) ortama erişimlerinin kısıtlanmış olduğunu kontrol eder.
23. Uygulama geliştirmelerinin veya değişikliklerinin test edilmeden canlı(Prod) ortama aktarılmadığını kontrol eder.
24. Test sürecinden geçen geliştirmelerin veya değişikliklerin üretim ortamına aktarılmadan önce değiştirilmediği ve üst yönetim onayı dahilinde canlı ortama aktarıldığını kontrol eder.
25. Yazılım geliştirme aşamalarındaki tüm adımların (talep, analiz, geliştirme, fonksiyonel test, güvenlik testi, taşıma vb.) kayıt altında olduğu ve kritik adımların sistemsel onaysız tamamlanmadığını kontrol eder.
26. Dış hizmet kapsamında gerçekleştirilen yazılım değişikliklerinin ve/veya geliştirmelerinin üye personeli tarafından üretim ortamına aktarıldığını kontrol eder.
27. Dış hizmet alımı sürecinde verilerin gizliliği, doğruluğu ve bütünlüğü açısından (alınan hizmetin mahiyetine göre erişim, yazılım, veri ve sistem güvenliği vb.... ) kontrol/denetim çalışmaları yapar.
28. Dış hizmet sözleşmelerinde Üye prosedürlerinde işletilen güvenlik, gizlilik ve denetim maddelerine yer verilmesi kontrol edilir.
29. RM sistemindeki sorgu denetim izleri ile üye nezdindeki sorgu denetim izlerinin mutabakatı sağlanır. RM sistemindeki aylık sorgu adetleri ile üye sistemindeki aylık sorgu sayısı ve örnek seçilen sorgulamalar karşılaştırılarak bu iki sistem arasında fark olmaması durumunu kontrol eder.
30. Sistem odalarına erişimlerin kayıt alındığını, fiziksel ve mantıksal erişim güvenliğinin sağlandığını kontrol eder.
31. İkincil merkeze iletilen Risk Merkezi verilerinin güvenli iletişim protokolleri ile gönderildiği ve iletişim kanalında uygulanan şifreleme mekanizmasının günümüz standartlarına uygun olmasını kontrol eder.