DENGE VARLIK YÖNETİM A.Ş.

1 EYLÜL 2022 - 31 AĞUSTOS 2023 DÖNEMİ RİSK MERKEZİ ÜYE DENETİM RAPORU

Rehber Bağımsız Denetim

ve

Yeminli Mali Müşavirlik A.Ş

21.09.2023

Bu rapor 89 (Seksendokuz) sayfadan oluşmaktadır.

Özel ve Gizlidir.

DENETİM MEKTUBU

EK-1

RİSK MERKEZİ ÜYE DENETİM RAPORU

Olumlu Görüş

Denge Varlık Yönetim A.Ş. Yönetim Kurulu'na:

Denge Varlık Yönetim A.Ş.'nin 08/05/2023 tarihi itibarıyla, Risk Merkezi' nin 07/01/2016 tarihli 3 no.lu Risk Merkezi Yönetimi Kararı ile yayınlanan "Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi Ve Raporlanması Hakkında Genelge" kapsamında risk merkezi süreçlerini ve bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

Risk merkezi süreçleri ve bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde 01/10/2014 tarih 51128 sayılı "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" ve 03/10/2014 tarih ve 51138 sayılı" Bilgi Güvenliği Politikası" ile belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması Denge Varlık Yönetim A.Ş. Yönetimi'nin sorumluluğundadır.

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin risk merkezi süreçleri ile bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve 07/01/2016 tarih ve 3 no.lu Risk Merkezi Yönetimi kararı ile hazırlanan "Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi ve Raporlanması Hakkında Genelgede" belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, risk merkezi süreçleri ve bilgi sistemleri ile bu süreç ve sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin Risk Merkezi Kontrol Hedefleri ve Bilgi Güvenliği Politikası doğrultusunda test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri ile risk merkezi süreçleri ve bu süreç ve sistemler 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.

Görüşümüze göre, yukarıda açıklanan husus(lar) nedeniyle, denetlenenin bütün önemli taraflarıyla, Denge Varlık Yönetim A.Ş.'nin 31/08/2023 tarihi itibarıyla risk merkezi süreçleri ve bilgi sistemleri üzerinde 07/01/2016 tarih ve 3 no.lu Risk Merkezi Yönetimi kararı ile yayınlanan "Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi ve Raporlanması Hakkında Genelge" ile 01/10/2014 tarih 51128 sayılı "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" ve 03/10/2014 tarih ve 51138 sayılı "Bilgi Güvenliği Politikası" nda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve Tarihi	Sorumlu Bilgi Sistemleri Baş Denetçisinin	Sorumlu Ortak Baş Denetçinin
Ankara,	Adı ve Soyadı, İmzası	Adı ve Soyadı, İmzası
21.09.2023	Mahir GÜNEY	Adil ÖNER
Kuruluşun Ticari Unvanı		
Rehber Bağımsız Denetim ve Yeminli Mali Müşavirlik A.Ş		

I. YÖNETİCİ ÖZETİ

a. Denetimin Amacı

Denetimin temel amacı, Türkiye Bankalar Birliği ("TBB") tarafından yayınlanan "Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi ve Raporlanması Hakkında Genelge" ("Genelge") hükümlerine uygun olarak Denge Varlık A.Ş.'nin ("Denge Varlık A.Ş." veya "Risk Merkezi Üyesi" veya Şirket) Risk Merkezi süreçleri ve bilgi sistemleri ile bu süreçlere ilişkin tasarlanan kontrollerin uyumluluğunun, tasarım etkinliğinin ve yeterliliğinin önemli kriterlere göre değerlendirilmesi ve değerlendirme sonuçlarının raporlanmasıdır.

b. Denetim Kapsamı

Gerçekleştirilen denetim; "Risk Merkezi Üyelerinin Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Denetimi ve Raporlanması Hakkında Genelge" ve bu Genelge'ye atıfta bulunan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeleri İlişkin Tebliğ" içerisinde yer alan hükümlere dayalı olarak Risk Merkezi Yönetimi ("RMY") tarafından onaylanan "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" ("Risk Merkezi Kontrol Hedefleri") ve "Bilgi Güvenliği Politikası" düzenlemelerini kapsayan Yetkili Kuruluşlar tarafından gerçekleştirilen Risk Merkezi Üye Denetim faaliyetlerini içermektedir.

Bu bağlamda, Risk Merkezi Üye denetimi sırasında ilk olarak üyenin Risk Merkezi faaliyetleri incelenmiş, bu faaliyetleri yürütmek veya desteklemek için temel süreçler ve bu süreçlere ait hassas verilerin kullanıldığı ve takip edildiği uygulamalar belirlenmiştir. Bu süreçler ve uygulamalar üzerindeki kontrollerin Risk Merkezi Üyesi'nin hassas verilerini raporlama sürecinde ve güvenli bir şekilde kullanmasına olan etkisi, "önemlilik" kriterine göre değerlendirilerek denetim çalışmasının kapsamı belirlenmiştir.

Bu nedenle, 14 Temmuz 2017 tarihli genelgede belirtilen hükme göre, Risk Merkezi Üyesinin Risk Merkezi faaliyetlerini yürütürken destek hizmeti sağlayan bir kuruluştan yardım aldığı durumda, bu destek sağlayan kuruluşun yerinde denetimden geçirilmesi ve denetim sonuçlarının denetim raporunda yer alması gerekmektedir.

Risk Merkezi Üyesi için yapılan denetim 1 Eylül 2022 - 31 Ağustos 2023 arasındaki dönemi kapsamaktadır.

c. Denetim Metodojisi

Risk Merkezi Üye Denetimi sırasında, denetim metodolojisi olarak kullanılan kontrol yaklaşımının yanı sıra, Genelge, Risk Merkezi Kontrol Hedefleri ve Bilgi Güvenliği Politikası'nda belirtilen kurallara uygun bir metodoloji benimsenmiş ve uygulanmıştır. Bu sayede denetim amacına ulaşılmıştır.Denetim sürecimizde bilgi toplama, gözlem, sorgulama ve doğrulama, inceleme, yeniden gerçekleştirme, yeniden hesaplama ve analitik inceleme gibi farklı denetim teknikleri kullanılmıştır. Kontrollerin test edilmesi sırasında, test edilecek örneklerin belirlenmesi aşamasında, test tekniği seçimi, ana kütlenin (veya alt kütlenin) ve ilgili kontrolün nitelikleri dikkate alınmıştır. Bu doğrultuda, örnek ya da örneklerin seçimi sırasında kontroller, test edilecek kontrollerin otomatik veya manuel olarak gerçekleştirilmesine göre ayrıştırılmıştır.

Manuel kontrollerin yeniden gerçekleştirme, inceleme ve yeniden hesaplama denetim teknikleri kullanılarak test edilmesi sırasında kullanılacak örnek sayısı, istatistiksel yöntemler kullanılarak hazırlanan bir tablo ile belirlenmiş ve testler uygulama sıklığına göre bu tabloya göre yapılması gereken

asgari örnek sayısına uygun şekilde gerçekleştirilmiştir. Diğer denetim tekniklerinin kullanıldığı testlerde ise örnek sayısı, ilgili süreçteki risk değerlendirme çalışmalarının sonuçları ve kontrolün öneminin göz önünde bulundurularak belirlenmiştir. Otomatik kontroller ise denetim metodolojisinin bir parçası olarak bilgi teknolojileri genel kontrol yaklaşımına uygunluk sağlandığı sürece tek bir örnek kullanılarak test edilmiştir.

Denetim sırasında kullanılan kanıt toplama, analiz ve örnekleme yöntemleri raporun II. Bölümü'nde detaylı olarak açıklanmıştır.

d. Denetim çalışmasına ilişkin genel değerlendirme

Denetimde gerçekleştirilen Risk Merkezi Üye Denetimi sırasında, denetim kapsamına dahil edilen Risk Merkezi süreçleri ve bilgi sistemleri ile bu süreçlere ilişkin tasarlanan ve uygulamaya alınmış olan kontrollerin uyumluluğu, etkinliği ve yeterliliği "önemlilik" kriteri çerçevesinde değerlendirilmiş ve raporun "VI. Üye Denetimi Hakkında Bilgi" bölümünde yer verilen bulgular tespit edilmiştir.

Denetim sırasında tespit edilen bulguları adet bazında gösteren tablo aşağıda sunulmaktadır.

Denetim Alanı[1]	**Bulgunun Önemlilik Seviyesi**	**Cari Dönem**[2]		**Geçmiş Dönemler**[3]			
		Tespit Edilen Toplam Bulgu Sayısı	Denetim Esnasında Düzeltilen Bulgu Sayısı	Düzeltilen Bulgu Sayısı	Kısmen Düzeltilen Bulgu Sayısı[4]	Devam Eden Bulgu Sayısı	Geçmiş Dönem Toplam Bulgu Sayısı
Veri İletimi - Alımı Esnasında Dikkate Alınması Gereken Önlemler	ÖK[5]	-	-	-	-	-	-
	KD[6]	-	-	-	-	-	-
	KZ[7]	-	-	-	-	-	-
	ÖK	-	-	-	-	-	-

1 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'nde tanımlanan kontrol alanlarını ifade eder.
2 Sadece cari dönemde tespit edilmiş bulguları ifade eder.
3 Denetçinin daha önceki denetim dönemlerinde tespit ettiği, ancak daha önceki denetim dönemlerinde giderildiğini ifade etmediği bulguları ifade eder.
4 Denetlenenin yaptığı çalışmalar neticesinde bulgunun taşıdığı riskte azalma olmuş ise bulgu bu sınıfa dahil olur.
5 Önemli Kontrol Eksikliği
6 Kayda Değer Kontrol Eksikliği
7 Kontrol Zayıflığı

Denetim Alanı[1]	**Bulgunun Önemlilik Seviyesi**	**Cari Dönem**[2]		**Geçmiş Dönemler**[3]			
		Tespit Edilen Toplam Bulgu Sayısı	Denetim Esnasında Düzeltilen Bulgu Sayısı	Düzeltilen Bulgu Sayısı	Kısmen Düzeltilen Bulgu Sayısı[4]	Devam Eden Bulgu Sayısı	Geçmiş Dönem Toplam Bulgu Sayısı
Üye Personelinin Farkındalığının Oluşturulması	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-
Veri İletimi - Alımı Toplam	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-
RM Bilgilerinin İşlendiği ve Saklandığı Sistemlere Erişim Kontrollerinin Düzenlenmesi	ÖK	-	-	-	-	-	-
	KD	2	2	-	-	-	-
	KZ	-	-	-	-	-	-
RM Bilgilerinin İşlendiği ve Saklandığı Sistemlerin Güvenliğinin Sağlanması	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	2	-	-	-	-	-
RM Bilgilerinin İşlendiği ve Saklandığı Sistemler Üzerinde Etkin Değişiklik Yönetiminin Gerçekleştirilmesi	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-
RM Bilgilerinin İşlendiği ve Saklandığı Sistemler Üzerinde Denetim İzlerinin Alınması	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-

Denetim Alanı[1]	**Bulgunun Önemlilik Seviyesi**	**Cari Dönem**[2]		**Geçmiş Dönemler**[3]			
		Tespit Edilen Toplam Bulgu Sayısı	Denetim Esnasında Düzeltilen Bulgu Sayısı	Düzeltilen Bulgu Sayısı	Kısmen Düzeltilen Bulgu Sayısı[4]	Devam Eden Bulgu Sayısı	Geçmiş Dönem Toplam Bulgu Sayısı
RM Bilgilerinin İşlendiği ve Saklandığı Sistemler Üzerinde Otomatik İşlerin Takibi	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-
RM Bilgilerinin İşlendiği ve Saklandığı Sistemlerin Sürekliliğinin Sağlanması	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ		-	-	-	-	-
Bilgi Güvenliği Politikası	ÖK	-	-	-	-	-	-
	KD	-	-	-	-	-	-
	KZ	-	-	-	-	-	-
Toplam	ÖK	-	-	-	-	-	-
	KD	2	2	-	-	-	-
	KZ	2	-	-	-	-	-

e. Denetim sırasında öne çıkan bulgular

Risk Merkezi Üyesi için 1 Eylül 2022 - 31 Ağustos 2023 arasındaki dönemde yapılan Risk Merkezi Üye Denetiminde herhangi bir önemli kontrol eksikliğine karşılaşılmamıştır. Ancak, dikkate değer kontrol eksikliklerini aşağıda özetlemekteyiz. Kontrol zafiyetleri raporda belirtilmemiş, ancak Risk Merkezi Üyesi'ne iletilmiştir.

2023.ERSM.0001.KD - Recall uygulaması canlı ortamında "TEST" isimli bir genel kullanıcı hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür. Aktif dizin kullanıcı listesindeki genel 6 adet test hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür.

2023.ERSM.0002.KD - Haziran 2023 İç kontrol raporunda Recall uygulamasına ait yetkilerin gözden geçirildiği görülmüştür. Ancak Aktif Dizin ve MS SQL veritabanı kullanıcı yetkilerinin gözden geçirilmediği belirlenmiştir.

f. Risk Merkezi süreçleri ve bilgi sistemlerine ilişkin kontroller ile ilgili saptanan bulgular hakkında genel değerlendirme

Risk Merkezi Üyesi'nde yaptığımız incelemelerde, denetlenen Risk Merkezi süreçleri, bilgi sistemleri ve bu süreçler için planlanan kontroller, belirlenen önemlilik ölçütüne göre tasarım etkinliği, yeterliliği ve uygunluğu açısından değerlendirilmiştir. Risk Merkezi Üyesi'nin "Kontrol Hedefleri"ne ve "Bilgi Güvenliği Politikası"nda belirtilen usul ve esaslara uygun olarak tasarım seviyesinde etkin, yeterli ve uyumlu kontrollerin tesis edildiği görüşüne varılmıştır.

g. Destek hizmeti kuruluşlarının denetimine ilişkin değerlendirme

Risk Merkezi Üyesi'nin hizmet aldığı kuruluşlar üzerinde gerçekleştirilen denetim ve değerlendirme neticesinde, 1 Eylül 2022 - 31 Ağustos 2023 tarihleri arasındaki dönemde herhangi bir önemli ya da dikkate alınası kontrol eksikliği bulunmamıştır. Destek hizmeti sağlayan kuruluşlarla ilgili değerlendirmemiz, raporun IV. bölümünde, "Üye'nin Risk Merkezi Süreçleri Hakkında Genel Bilgi" başlığı altında sunulmuştur.

h. Risk Merkezi Üyesi'nin Şube Denetimine İlişkin Genel Değerlendirme

Risk Merkezi Üyesi'nin şubesi bulunmaması sebebiyle, şube denetimlerine ilişkin bir çalışma gerçekleştirilmemiştir.

II. DENETİM ÇALIŞMASINA AİT BİLGİ

Bu bölüm, Risk Merkezi Üye Denetimi sırasında dikkate alınan varsayımlar ile uygulanan denetim teknikleri, denetimin gerçekleştirildiği birimler, denetim kapsamındaki süreçlerle ilgili sorumluların unvan ve erişim bilgileri ile denetim ekibi ve denetimin başlama/bitiş tarihlerine ilişkin özet bilgileri içermektedir.

a. Bilgi Sistemleri ve Risk Merkezi süreçleri denetimi sırasında uygulanan denetim metodolojisi

Bilgi sistemleri ve risk merkezi süreçleri denetimi sırasında, "Risk Merkezi Kontrol Hedefleri" ve "Bilgi Güvenliği Politikası" içerisinde yazılı olarak açıklanan süreç tanımları ve hedefleri esas alınmıştır.

Denetim metodolojimiz temel olarak şu şekildedir:

- Risk Merkezi Üyesi'nin mevcut genel uygulamalarının ve Risk Merkezi süreçlerinden sorumlu bölümlerinin organizasyon yapısının anlaşılmasını sağlamak için,
- Önemli uygulamalarla ilgili karşılaşılan ve Risk Merkezi'ne gönderilecek verilerin hazırlanması, sisteme girilmesi ve Risk Merkezi'den temin edilen verileri olumsuz yönde etkileyebilecek risklerin ve bu risklere karşı oluşturulmuş kontrollerin tespit edilmesini sağlamak için,
- Önemli risklere yönelik olarak belirlenen kontrollerin denetim sürecinde uygunluk, etkinlik ve yeterlilik açısından değerlendirilmesini içeren çalışmalar gerçekleştirilmiştir.

Farklı platformlarda veya farklı sistem parçalarında süreçlerin (OSI Modeli aşağıdaki tabloda sunulmaktadır) birbirinden farklı şekilde yürütüldüğü durumlarda, ilgili sistem parçasındaki işleyiş ve kontrol mekanizması incelenmiştir.

Open Systems Interconnection ("OSI") Modeli		
	Katman	**Fonksiyon**
Host	**Uygulama**	Bilgisayar ağı ve uygulama arasındaki iletişim
	Sunum	Sunum ve şifreleme
	Oturum	İletişim
	Taşıma	Bağlantı ve aktarım güvencesi
Medya	**Bilgisayar ağı**	Adresleme ve erişim
	Data bağlantısı	Fiziksel adresleme
	Fiziksel	Medya, sinyalleşme ve iletim

TBB tarafından iletilen 23/11/2016 tarihli ve RM-1 51589 sayılı yazısındaki kararlara istinaden Risk Merkezi Üyesi bünyesinde, bilgi sistemleri ve risk merkezi süreçleri ile bu sistem ve süreçler üzerinde tespit edilen bulgulara ilişkin tasarlanan ve işletilen kontrollerin bütünlüğünün etkinliği, yeterliliği ve uyumluluğu hakkında makul bir güvence sağlayacak şekilde denetim teknikleri belirlenmiştir. Kontrollerin dokümantasyonu ve test edilmesi sırasında, kontrolün türü, sıklığı, işlevi, kontrolü

gerçekleştiren kişi ve uygulamalar, kontrol sahibi ve referanslar da dikkate alınmıştır. Denetimlerimiz esnasında kullandığımız örnekleme yöntemleri bu bölümün "d) Örnekleme yöntemi" bendinde sunulmaktadır.

Yukarıda açıklandığı üzere, farklı OSI birimleri için farklı süreçler olması durumunda her bir süreç için ayrı bir test grubu belirlenmiş ve kullanılmıştır.

Bu çerçevede, yapılacak denetim çalışmalarına baz teşkil edecek detaylı bir çalışma planı oluşturulmuştur. Risk Merkezi Üye Denetimi sırasında kullanılan temel yöntemler ve varsayımlar bu plan dahilinde belirlenmiş ve uygulanmıştır.

b. Destek hizmeti kuruluşlarının denetimi sırasında uygulanan denetim metodolojisi

Denetim sırasında, Risk Merkezi Üyesi'nin destek hizmeti aldığı kuruluşlarla imzalanan sözleşmeler incelenmiş ve alınan hizmetin kapsamı ile bilgi sistemleri ve Risk Merkezi süreçlerine olan etkisi değerlendirilmiştir. Denetim kapsamında denetim yapılacak destek hizmeti sağlayan kuruluşlar ve bu kuruluşlarda yapılacak çalışmaların kapsamı, bu kuruluşların sunulan hizmetlerinin bilgi sistemleri ve Risk Merkezi süreçlerine etkisi göz önünde bulundurularak ve "önemlilik" kriteri ile yapılan risk değerlendirme çalışmaları temel alınarak belirlenmiştir.

Destek hizmeti kuruluşlarına yönelik yapılan risk değerlendirmesi çalışmasında;

- Destek hizmeti alınan kuruluşlarla yapılan sözleşmeler detaylı bir şekilde incelenerek, alınan destek hizmetinin kapsamı ve bu hizmetlerin bilgi sistemleri ve Risk Merkezi süreçlerine olan etkisi değerlendirilmiştir.

- Destek hizmeti kuruluşu tarafından sunulan hizmetin Risk Merkezi Üyesi'nin iş sürekliliğine etkisi değerlendirilmiştir.

- Destek hizmeti kuruluşu çalışanlarının, Risk Merkezi Üyesi'nin risk merkezi verilerini işlemek veya depolamak için kullandığı sistemlere veya diğer uygulamalara erişip erişmediği incelenmiştir.

- Destek hizmeti kuruluşu çalışanlarının, Risk Merkezi Üyesi'nin risk merkezi verilerini işlemek ve kullanmak için hangi yöntemlerle (VPN, FTP, doğrudan kullanıcı erişimi, vb.) sisteme veya diğer uygulamalara erişim sağladıkları incelenmiştir. Bu bilgilere dayanarak, Risk Merkezi Üye Denetimi kapsamında değerlendirilecek destek hizmeti kuruluşları ve bu kuruluşlarda yapılacak çalışmanın kapsamı ve denetim metodolojisi belirlenmiştir.

Risk değerlendirmesi sonucunda yüksek risk taşıdığı belirlenen destek hizmeti kuruluşlarına bağımsız olarak denetim uygulanmıştır.

Bağımsız olarak denetlenen destek hizmeti kuruluşlarında, test edilecek kontrollerin kapsamı belirlenirken önemlilik ilkesine uyulmuş ve bu kontroller, bilgi sistemleri ve Risk Merkezi süreçleri üzerindeki tüm kontrollerin topluca etkinliği, yeterliliği ve uyumluluğu hakkında makul bir güvence sağlayacak şekilde seçilmiştir. Bu kontrollerin uyumluluğunu, etkinliğini ve yeterliliğini değerlendirmek için kullanılacak denetim teknikleri, denetim planına dahil edilmiştir.

Denetimlerimiz sırasında kullandığımız örnekleme yöntemleri, raporun "g" bölümünde ayrıntılı bir şekilde açıklanmaktadır.

c. Şube denetimi sırasında uygulanan denetim metodolojisi

Üye kuruluşun herhangi bir şubesi bulunmaması nedeniyle, şube denetimleri kapsamında herhangi bir çalışma gerçekleştirilmemiştir.

a. Denetim Çalışmasında Dikkate Alınan Önemli Hususlar ve Varsayımlar

Genel kontrollerin doğasından kaynaklanan sınırlamalar, hataların, kötü niyetli eylemlerin, sahteciliğin, yasa dışı uygulamaların, sözleşme ihlallerinin, çift kayıt sistemlerinin veya tekrarlanan bilgi sistemlerinin meydana gelmesine ve bu tür sorunların tespit edilemeyebilmesine yol açabilir.

Denetim sürecinde talep edilen her türlü bilgi ve belgenin Şirket tarafından doğru, eksiksiz ve güncel olarak sağlandığı varsayılmaktadır.

Denetim sonuçları, test edilen dönemle sınırlıdır ve gelecek dönemleri kapsayacak şekilde yorumlanmamalıdır.

Kontroller değerlendirilirken, aynı süreçteki kontrollerin Şirket'in ilgili tüm bölüm, birim ve şubelerinde benzer şekilde uygulandığı ve işlediği varsayılmıştır.

Denetim çalışmamız, denetim dönemimiz itibarıyla yürürlükte olan 51128 sayılı "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" ve 3/10/2014 tarih ve 51138 sayılı" Bilgi Güvenliği Politikası" ile belirtilen usul ve esaslara uygun olarak tamamlanmıştır.

Şirket içindeki süreçlerin etkin bir şekilde kontrol edilmesi ve uygun bir kontrol ortamının oluşturulması, Bilgi Sistemleri Denetimi için talep edilen Bilgi Sistemleri ve İş Süreçleri kontrolleri ile ilgili her türlü bilgi, kayıt, belge ve dokümantasyonun eksiksiz ve doğru bir şekilde temin edilmesi, Şirket yönetiminin sorumluluğundadır.

Bize sunulan tüm bilgi, belge ve dokümantasyonun doğru, güncel ve geçerli olduğunu kabul ediyoruz. Ancak, bu varsayım, profesyonel şüpheciliğimiz çerçevesinde, denetim planımızın hazırlanmasını ve uygulanmasını engelleyici bir faktör olarak kabul edilmez.

Denetim sonuçları ve bulgularımız, incelenen dönemi kapsamaktadır. İş süreçlerinin içerisinde yer alan otomatik uygulama kontrollerinin etkinliği, bilgi sistemleri ortamında bulunan kontrollere bağlı olarak zaman içinde değişebilirken, manüel uygulama kontrollerinin etkinliği, kontrolü gerçekleştiren sorumluların performansına bağlı olarak değişkenlik gösterebilir.

Kontrollerin doğasından kaynaklanan sınırlamalar nedeniyle, bilgi sistemleri ve finansal veri üretimi süreçleri ve sistemleri üzerinde kontrol zayıflıkları oluşabilir ve bu zayıflıklar tespit edilmeyebilir.

Ek olarak, bulgularımıza dayalı elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerektiğini vurgulamak önemlidir. Çünkü mevcut koşulların değişebileceği, sistemlerde veya kontrollerde değişikliklerin yapılabileceği veya kontrollerin etkinliğinin azalabileceği gibi nedenlerle, bu sonuçların zaman içinde değişebileceği riski bulunmaktadır.

Denetim çalışmalarımız sırasında;

- Tarafımıza sunulan tüm belge ve bilgilerin doğru ve eksiksiz olduğu,
- Yapılan toplantılarda ifade edilenlerin **Şirket**'in görüşlerini yansıttığı,
- **Şirket** yetkililerine teyit amacıyla sunulan belgelerin okunduğu, anlaşıldığı ve mutabık kalındığı, kabul edilmiştir.

b. Denetimde Kullanılan Örnekleme Yöntemi

Gerçekleştirmiş olduğumuz denetimlerin kapsamında kullandığımız test yöntemleri ve örneklem büyüklüklerinin belirlenmesinde, aşağıdaki faktörler dikkate alınmıştır:

- Önemlilik derecesi
- Risk derecesi
- Kanıt toplama maliyeti

Önemlilik kriterine göre belirlenen süreçlerin kritik uygulamalarının tamamı denetim kapsamına dahil edilmiş ve bu uygulamaların test edilmesi sırasında iç kontrol testlerine ağırlık verilmiştir. İç kontrol sistemini belirlemek için yapılacak testlerde, iradi örnekleme yöntemi kullanılmış ve iç kontrol sisteminin değerlendirilmesi sonucunda daha detaylı testlere ihtiyaç olup olmadığı belirlenerek işlem bazlı testlerin seviyesi tespit edilmiştir.

Denetim sırasında, inceleme amacıyla hem test aşaması öncesinde hem de test aşamasında çeşitli örneklem yöntemlerinden faydalanılarak belirli belgeler talep edilmiştir. Örneğin, Temsilci Ödeme İşlemleri veya yıl sonu amortisman fişlerinin incelenmesi sırasında, katmansal örnekleme yöntemi kullanılarak belgeler ve fişler belirli meblağlar dikkate alınarak gruplandırılmış ve bu gruplardan rastgele örnekler seçilmiştir. Bazı iç kontrol testlerinde Stop-Go örnekleme yöntemi kullanılmış ve gerekli kanıt bulunana kadar ana popülasyonun belgeleri incelenmeye devam edilmiştir. Bu nedenle, kullanılan örneklem yöntemleri ile elde edilen bulguların genellikle popülasyonun tamamına uyarlanabileceği düşünülmektedir.

Denetim sırasında örnekleme işleminde, istatistiksel ve istatistiksel olmayan olmak üzere iki farklı yöntem kullanılmıştır. Her iki yöntemde de seçilen örnek birimlerden yola çıkılarak ana popülasyon hakkında bir sonuca varılmaya çalışılmıştır. Örneklemenin planlanması, planın uygulanması ve örnekleme sonucu elde edilen kanıtların değerlendirilmesi aşamalarında denetçinin mesleki deneyim ve değerlendirme yeteneği kullanılmıştır.

Tarafımızca gerçekleştirilen denetim çalışmalarında **Şirket**'in iş ve işlem hacmi, üretilen verinin büyüklüğü ve çeşitliliği, verinin yapısı, işlenmesi ve süreçler göz önüne alındığında istatistiki olmayan örnekleme yöntemlerinin yeterli ve maliyet etkin sonuçlara ulaşılması için gerekli olduğu düşünülmektedir. Bu nedenle, denetçilerimizin sahip olduğu ortalama 38 (Otuz Sekiz) yıllık mesleki tecrübeleri göz önüne alınarak istatistiki olmayan örnekleme yöntemleri ağırlıklı olarak tercih edilmiştir.

Denetimlerimizde sıkça kullanılan tesadüfi örnek seçme teknikleri aşağıda belirtilmiştir.

- Kur'a ile seçim,
- Rassal sayılar tablosu ile seçim,
- Sistematik seçim,
- Özel seçim teknikleri olan tabakalara göre seçim, kümelere göre seçim, kademeli seçim.

Bu tekniklerin uygulanmasında bir ana kütleden örnek grubun seçilme işlemi yapılmadan önce eğer göz ardı edilebilecek bir değer varsa, bu değer göz ardı edilerek bu değerin üzerindeki birimlerin tamamına örnek grubu oluşturma işlemi gerçekleştirilmiştir. Ancak göz ardı edilebilecek bir değer yoksa, o zaman ana kütlenin içindeki birimlerin tamamı örnek grubu oluşturulmaya tabi tutulmuştur.

Örneklem boyutunu belirlerken, risk faktörleri ve kontrolün tipi ve sıklığı gibi faktörler de göz önünde bulundurulmuştur. Bu nedenle, otomasyona dayalı ve otomatik kontroller için, her işlem için aynı kontrolün uygulandığı kabul edilerek, toplamda gerçekleştirilen işlem sayısından bağımsız olarak sadece 1 adet kontrol test edilmiştir.

Manüel kontrollerde ise, kontrolün gerçekleştirilmesi ve kontrol hedefine ulaşılmasındaki başarı, kontrolü gerçekleştiren kişi vb. gibi faktörlere bağlı olduğu için, örneklem boyutu, kontrolün sıklığı ve popülasyon büyüklüğü gibi faktörler göz önüne alınarak seçilmiştir. Bu şekilde örneklemenin popülasyonun bütününü temsil etmesi amaçlanmıştır.

Buna göre, ilgili manüel kontroller için eğer kontrol,

Günde birden fazla uygulanıyorsa	**20+** adet,
Günlük olarak uygulanıyorsa	**10** adet,
Haftalık olarak uygulanıyorsa	**5** adet,
Aylık olarak uygulanıyorsa	**2** adet,
Üç Aylık olarak uygulanıyorsa	**2** adet,
Altı Aylık olarak uygulanıyorsa	**1** adet,
Yıllık olarak uygulanıyorsa	**1** adet

Örnekler seçilerek test çalışmaları yürütülmüştür. Ayrıca, denetçinin mesleki bilgisi ve denetlenen süreçlerin kontrol ortamına olan etkisi göz önüne alınarak örnek sayısı, gerektiğinde artırılmış veya bir alt sıklık seviyesi için tanımlanan örnek sayısından az olmamak üzere azaltılmıştır.

Test edilecek kontrol sıklığı tanımlanmamışsa, örneklem uzayının büyüklüğü ve incelenen sürece ait kontrol ortamı hakkındaki genel değerlendirmemiz de göz önüne alınmıştır.

Buna göre, örnek sayısının belirlenmesi aşamasında, örneklem uzayı büyüklüğü değerlendirilmiş, bu büyüklüğe en yakın "işlem sıklığı ilişkili" örneklem uzayı büyüklüğüne eşleştirme yapılmıştır. Örnek olarak, örneklem uzayı büyüklüğünün **365** 'den fazla olması durumunda kontrol "günde birden fazla" sıklığına uygun kontrol olarak değerlendirilmiş ve buna göre örnek seçimi yapılmıştır.

Örnek seçimi aşamasında, seçilen örneklerin ilgili denetim dönemine ait olmasına ve olabildiğince denetim dönemine yayılmış olmasına dikkat edilmiştir. Genellikle örneklem uzayı içerisinden rastgele seçim yöntemi uygulanmış olmakla birlikte, işlem büyüklüğü, ilgili işlemlerin / işlem türlerinin kullanım yaygınlığı ve **Şirket**'in faaliyetlerine ilişkin riskler de göz önünde bulundurulmuştur.

c. Kullanılan denetim teknikleri

Çalışma sırasında aşağıda belirtilen denetim tekniklerinden biri veya birkaçı uygulanmıştır.

Bilgi Toplama: Denetim öncesi ve sırasında, hem kurum içi (prosedürler, politikalar, iş akış diyagramları vb.) hem de dış kaynaklar (piyasa verileri, sektör bilgileri vb.) kullanılarak sürecin ve kontrolün işleyişi ile ilgili bilgi elde edilmiştir.

Gözlem: Denetim sırasında mevcut kontrollerin bağımsız olarak izlenmesi sağlanmıştır.

Sorgulama ve Doğrulama: Kontrollerin işleyişinin anlaşılmasına yönelik olarak kontrolün aktörleri ve sahipleri ile yapılan görüşmeler ve bu görüşmeler sırasında elde edilen bilgi ve anlayışın doğrulanması sağlanmıştır.

İnceleme: Kontrollerin sürekli olarak uygulandığını doğrulamak için kontrolün icrası aşamasında kullanılan yazılı belgelerin veya elektronik kayıtların elde edilip incelenmesi işlemi gerçekleştirilmiştir.

Yeniden Gerçekleştirme: Kontrolün etkinliğini belirlemek için denetim kanıtları, ilgili kontrolün bağımsız olarak denetçi tarafından uygulanmasıyla elde edilmiştir.

Yeniden Hesaplama: Hesaplamaya dayalı kontrollerin etkinliği ve yeterliliğinin anlaşılması amacıyla, hesaplamaların, bu hesaplamaları gerçekleştiren sistem veya personelden bağımsız bir şekilde yeniden gerçekleştirilmesi işlemi gerçekleştirilmiştir.

Analitik İnceleme: Süreç ve kontrolle ilgili bilgilere dayalı olarak beklentilerin oluşturulması, ana kütleden gelen mevcut verilerle karşılaştırmaların yapılması, trendlerin takip edilmesi ve sapmaların tespit edilmesi gibi yöntemler kullanılmıştır.

Denetim teknikleri arasında, kontrol testlerinin bağımsız olarak yeniden gerçekleştirilmesi, inceleme ve yeniden hesaplama tekniklerinin kontrolün uyumluluğu, etkinliği ve yeterliliğine yönelik en yüksek güvenceyi sağladığı kabul edilmiştir. Belirlenen kontrollerin test edilmesi aşamasında, kontrolün işaret ettiği riskin büyüklüğü, kontrol ortamı hakkındaki genel değerlendirmemiz, kontrolün riski önlemeye yönelik etkinliği ve sağlayacağı denetim kanıtları göz önünde bulundurulmuştur. Denetçi, bu aşamada, mesleki yargı ve tecrübelerinden faydalanarak yukarıda bahsi geçen yöntemlerden biri veya birkaçını kullanmıştır.

d. Denetim Ekibi ve Denetimin Başlama / Bitiş Tarihleri

Şirket bünyesinde yürüttüğümüz denetim çalışmaları 01.09.2022 – 31.08.2023 tarihleri arasında gerçekleştirilmiştir. Denetlenen tarafından düzeltildiği beyan edilen bulgulara ilişkin gözden geçirme çalışmaları rapor tarihine kadar sürdürülmüştür. Denetim çalışmalarında görev alan denetim ekibine aşağıda yer verilmiştir.

Denetim Organizasyonu

Bilgi Sistemleri Denetimi hizmetleri için Denetim Sorumlu Ortağı **ADİL ÖNER** öncelikli olarak denetimin bütününden, **Şirket**'in ihtiyaçlarının belirlenmesi ve sorunların giderilmesini temin etmek amacıyla **Şirket** ile ilişkilerden sorumlu olmuştur. **ADİL ÖNER** denetim ekibinin **Şirket**'in ihtiyaçlarına cevap verebilmesi sorumluluğunu üstlenmiştir.

Sorumlu Bilgi Sistemleri Bağımsız Başdenetçisi olarak **MAHİR GÜNEY**, tüm çalışma planının işleyişinden sorumlu olmuştur. Kendisi, aşağıdaki hususların yerine getirilmesini sağlamıştır:

- Denetimin kabul edilen bütçe dâhilinde, zamanında tamamlanması,
- Denetim sırasında karşılaşılan sorunların çözülmesi,
- Denetimin gerçekleşmesi için gerekli olan kaynakların sağlanması.

MAHİR GÜNEY; **Rehber YMM A.Ş.**'de Bilgi Teknolojileri ve İç Denetim Bölüm Başkanı olarak çalışmaktadır. Kendisi CISA (Certified Information Systems Auditor) ve CRISC (Certified in Risk and Information Systems Control) unvanına sahiptir. **Rehber YMM A.Ş.** 'nin Bilgi Teknolojileri ile ilgili faaliyetlerinden sorumludur. 38 (Otuz Sekiz) yılı aşkın bir süre ile danışman, denetim uzmanı, bilgi işlem müdürü, bilgi işlem uzmanı, sistem analisti ve programcı olarak bilgisayara dayalı muhasebe sistemlerinin tasarımında, test çalışmasında, uygulamasında ve diğer bilgisayar sistemlerinle bağlantı kurulmasında çalışmıştır. Fizibilite ve sistem kurma çalışmalarında bulunmuştur.

AYDIN AKŞAMGÜNEŞİ; **Rehber YMM A.Ş.**'de Bilgi Sistemleri Bağımsız Baş Denetçisi olarak çalışmaktadır. **Rehber YMM A.Ş.** öncesi denetim şirketlerinde Sorumlu Bilgi Sistemleri Bağımsız Başdenetçisi unvanına sahip olarak görevler yapmıştır. 38 (Otuz Sekiz) yılı aşkın bir süre ile iş ve Bilgi Teknolojileri / Sistemleri deneyimine sahip olup danışman, denetim uzmanı, bilgi işlem müdürü, bilgi işlem uzmanı, sistem analisti ve programcı olarak bilgisayara dayalı muhasebe sistemlerinin tasarımında,

test çalışmasında, uygulamasında ve diğer bilgisayar sistemleri ile bağlantı kurulmasında çalışmıştır. Fizibilite ve sistem kurma çalışmalarında bulunmuştur.

AHMET UFUK GÜL; Kıdemli Finansal Denetçi (SMMM), **AHMET ÖZKALKAN**; Kıdemli Bilgi Sistemleri Bağımsız Denetçisi ve diğer Rehber personeli denetim çalışmalarında görev almıştır.

e. Denetim Kapsamındaki Risk Merkezi Süreçleriyle İlgili Sorumlulukların Unvan ve Erişim Bilgileri

Risk Merkezi Üyesi'nde gerçekleştirilen denetim çalışmaları, 08 Mayıs 2023 tarihinde başlamış ve 19 Eylül 2023 tarihinde bitmiştir. Risk Merkezi süreçleri ve ilgili sorumluların unvan ve erişim bilgileri aşağıdaki tabloda sunulmaktadır.

Risk Merkezi Süreçleri	**İlgili Birim**	**İlgili Birim Sorumlusu**	**Erişim Bilgileri**
Risk Merkezi Veri İletimi-Alımı Süreci	Bilgi İşlem	Onur Eren	Onur.Eren@dengevarlik.com.tr
Risk Merkezi Veri İletimi-Alımı Süreci	İç Kontrol	Gamze Oransayoğlu	Gamze.Oransayoglu@dengevarlik.com.tr

III. ÜYE'NİN SİSTEMLERİ HAKKINDA GENEL BİLGİ

a. BT Bölümü'nün çalışan profili

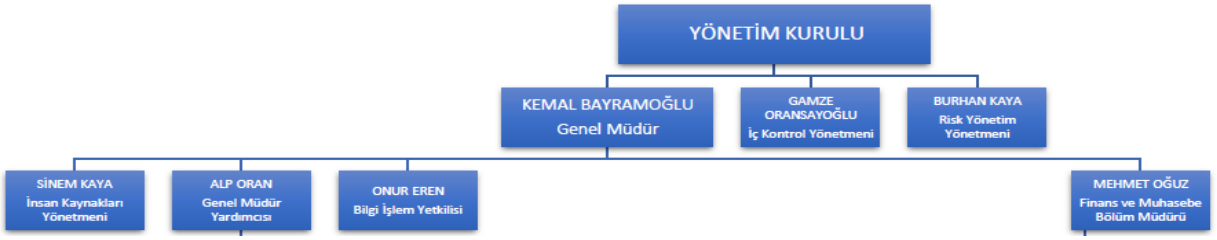
Denge Varlık Yönetim A.Ş. bünyesinde BT hizmetleri biriminde 1 personel görev almaktadır. Bilgi İşlem Sorumlusunun kısaca özgeçmişine aşağıda yer verilmiştir.

- Bilgi İşlem Yetkilisi: Onur Eren
- Diğer Tecrübeleri: Elvan Gıda (3 yıl), Eren Holding (1 yıl), Basistek Bilgi Teknolojileri (3 yıl), OMG Turkey (2 yıl)
- Toplam Tecrübe: 10 yıl
- Şirketteki Toplam Tecrübe: 9 ay

b. BT Bölümü'nün organizasyon yapısı

Denge Varlık Yönetim A.Ş.'nin BT destek ihtiyacı kuruluş bünyesinde faaliyet gösteren Bilgi İşlem Birimi'nde görev alan Bilgi İşlem Yetkilisi Onur Eren tarafından karşılanmaktadır.

Bilgi İşlem Birimi, kuruluş organizasyon yapısı içerisinde Bilgi İşlem Yetkilisi ile temsil edilmektedir. Bilgi İşlem Yetkilisi direk olarak Genel Müdür'e bağlıdır. Bilgi İşlem Yetkilisi'ni gösteren organizasyon şeması aşağıdaki tabloda paylaşılmıştır.



c. Risk Merkezi Verilerinin Oluşturulmasında, Hazırlanmasında, Raporlanmasında, İletilmesinde ve Saklanmasında Kullanılan Uygulamalar, Sistemler ve Araçlar Hakkında Genel Bilgi (Madde 41.1.b)

Denetim kapsamında değerlendirilmesi yapılan risk merkezi süreçleri ile uygulama, işletim sistemi, veritabanı ve donanım bilgileri aşağıdaki tabloda listelenmiştir:

Varlık Yönetimi Uygulaması	Recall Tahsilat Yönetim Sistemi
Veri tabanları	MS SQL Server 2019
İşletim Sistemleri	Windows 10, Windows Server 2016, Windows Server 2019
Güvenlik Duvarı	Checkpoint R77.30
DDOS Saldırı Önleme	Checkpoint R77.30
İz Kayıtları İzleme Sistemleri	Manage Engine (Event Analyzer 11, ADAudit Plus5)
Ağ Yapısı İzleme	System Center Configuration Manager 2016, Zabbix
Zararlı Yazılımlara Karşı Koruma Sistemleri	4.0 Symantec Endpoint Protection

d. Risk Merkezi Üyesi'nin Bilgi Sistemi Mimarisi (Madde 41.1.c)

Üyenin internet erişimi ve veri merkezi barındırma hizmetleri Bilgi İşlem birimi tarafından yönetilmektedir.

Üyenin sistem odası için Türk-net firmasından destek almaktadır. Türk-net firmasının Şişli'deki yerleşkesinin içerisinde Üyeye ait kabinin içerisinde sunucular saklanmaktadır.

Recall uygulaması 3 farklı sunucu üzerinde çalışmaktadır. Risk Merkezi verilerinin saklandığı sunucu sistemlerine sadece Bilgi İşlem çalışanları erişebilmektedir.

Üye bünyesinde sistemler Checkpoint R77.30 firewall sistemi ile korunmakta olup, dışarıya çıkışlar denetlenebilmekte, gerekli kısıtlamalar yapılmaktadır.

İz kayıtları yönetimi için Manage Engine uygulaması kullanılmakta olup işletim sistemi, uygulama, veritabanı iz kayıtları bu uygulama içinde tutulmaktadır.

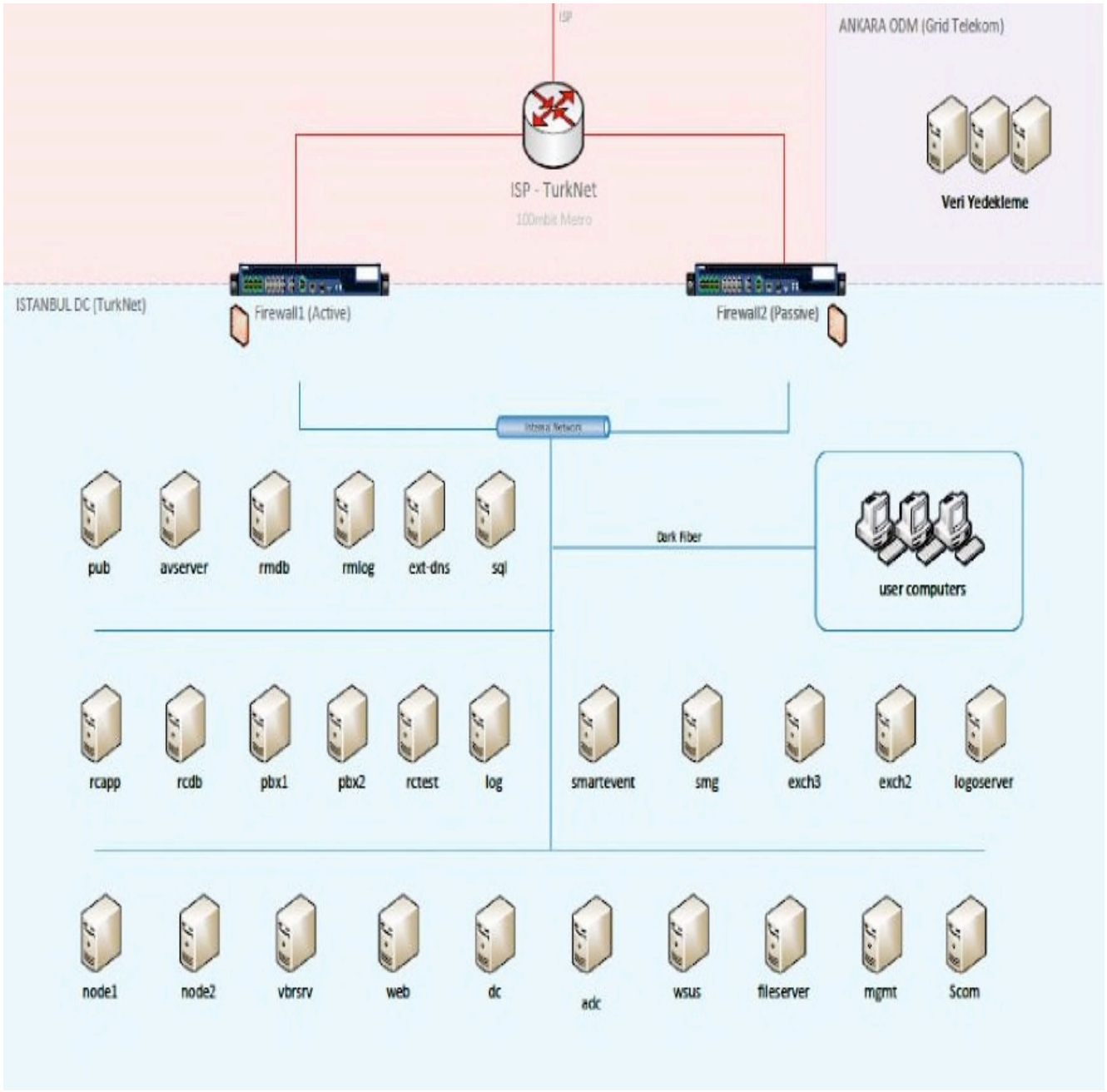
Recall uygulamasının yazılım geliştirme süreçleri için Alga firmasından destek alınmaktadır. Altyapı desteğini ise Operasist firmasından almaktadır.

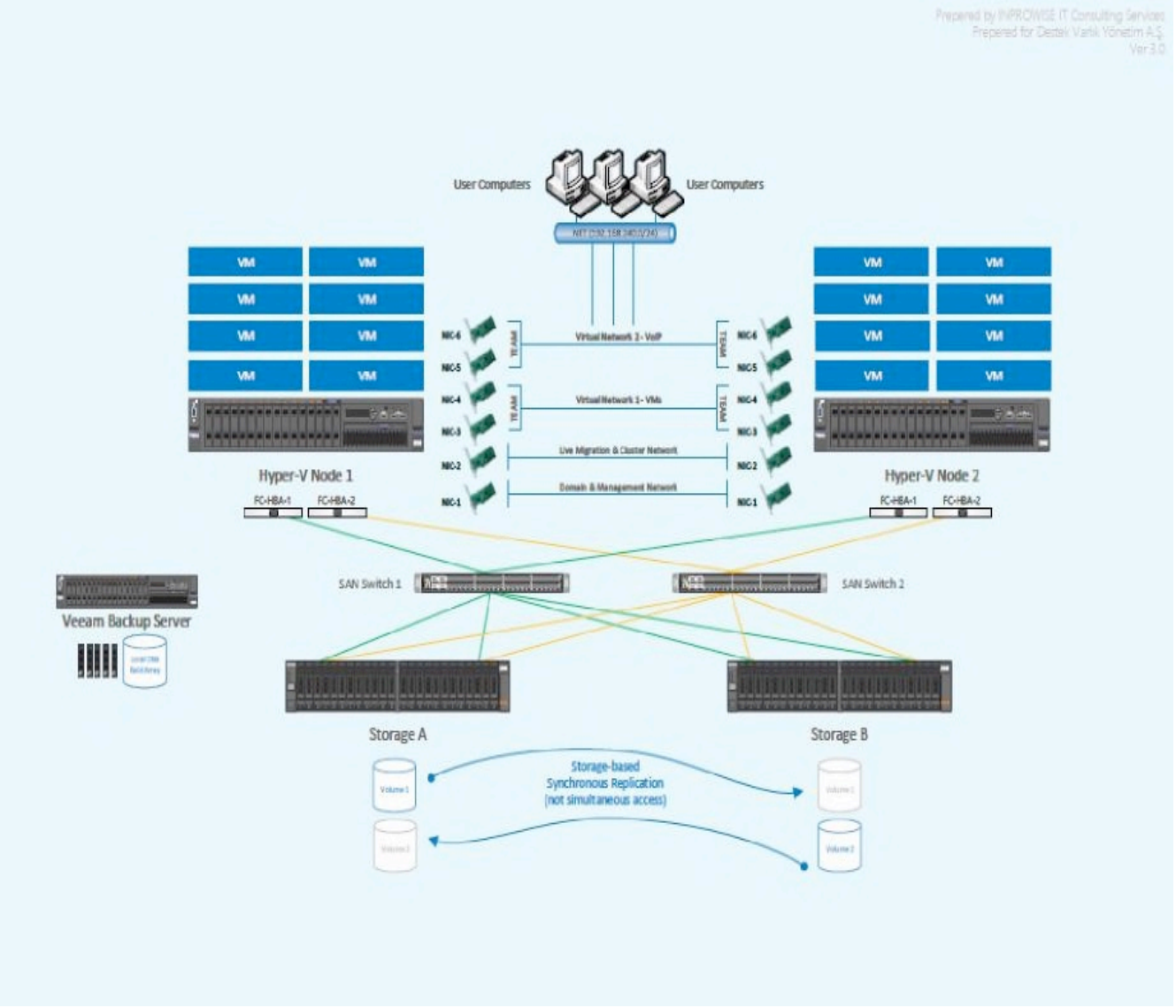
Recall uygulaması üzerinde kullanıcıların kimlik doğrulama işlemleri uygulama katmanında gerçekleşmektedir.

Recall uygulamasına ait üretim ortamı, test ortamı sanal sunucuları olarak birbirinden ayrılmıştır. Recall uygulaması üzerinde gerçekleştirilen yazılım değişiklikleri, Alga tarafından geliştirilmekte olup daha sonrasında Alga VPN üzerinden test ortamına yazılımı aktarılmaktadır. Tamamlanan değişiklik paketleri Recall uygulamasın eklenti uygulamasıyla Bilgi İşlem Yetkilisi tarafından üretim ortamına taşınmaktadır.

Recall uygulamasına ilişkin Ankara'da felaket kurtarma merkezi bulunmakta olup uygulama yedekleri ile saklanmaktadır.

Bilgi sistemleri mimarisindeki ağ topolojisi tabloda gösterilmiştir.




Prepared by INPROWISE IT Consulting Services
Prepared for Destek Varlık Yönetim A.Ş.
Ver 3.0
User Computers
User Computers
VM
Virtual Network 2 - VoIP
Virtual Network 1 - VMs
Live Migration & Cluster Network
Domain & Management Network
NIC-6
NIC-5
NIC-4
NIC-3
NIC-2
NIC-1
Hyper-V Node 1
Hyper-V Node 2
FC-HBA-1
FC-HBA-2
SAN Switch 1
SAN Switch 2
Veeam Backup Server
Storage A
Storage B
Storage-based
Synchronous Replication
(not simultaneous access)

IV. ÜYE'NİN İÇ KONTROL ORTAMI HAKKINDA GENEL BİLGİ

a. İç Kontrol Bölümü Hakkında Genel Bilgi (Madde 42.1.b)

Üye şirketin bünyesinde, iç kontrol ve uyum görevlisi olarak 1 adet çalışan bulunmaktadır.

Denetim Yönetmeni olarak görev yapan Sayın Gamze Oransayoğlu, 01.03.2022 tarihinden bu yana iç kontrol ve uyum görevlisi görevini yürütmektedir ve bunun dışında herhangi bir icra görevi bulunmamaktadır. Yönetim Kurulu'na bağlı olarak görev yapmaktadır.

İç kontrol sorumlusunun görevleri, yetkileri ve sorumlulukları, "İç Kontrol Müdürü Görev Tanımı" dokümanında aşağıdaki şekilde açıklanmıştır.

- Şirketin varlıklarının korunmasına ve işlemlerin uygulamasına yönelik operasyon el faaliyetlerin kontrolleri ile verimliliğinin ve etkinliğinin sağlanması, bu bağlamda operasyonel risklerin kontrol altına alınarak azaltılması,
- Bilgi sistemleri içinde yer alan Şirket faaliyetlerinin yürütülmesi ya da desteklenmesine yönelik iş süreçlerinde, bilginin güvenilir, izlenebilir ve gereksinmeleri karşılayabilir düzeyde olup olmadığı yönünde uygulama kontrollerinin yapılması,
- Faaliyetlerin etkin ve verimli bir şekilde yasalara ve mevzuatlara, Denge Varlık Yönetim A.Ş. politika, süreç görev tanımları ve prosedürlerine uygun olarak yürütülmesinin operasyonel yönden düzenli olarak takip edilmesi,
- Olası hatalara ve risklere karşı kısa sürede müdahale edilmesi imkânını sağlayabilmek için kontroller yapılması, tespit edilen bulguların zamanında düzeltilmesi için ilgili bölümlere uyarıda bulunması ve bunun sonuçlarının takip edilmesini sağlamaktır.

Yeni ürün ve işlemlerin bölümlerde nasıl hayata geçtiği, yasaya ve ilgili diğer mevzuata, şirket içi politika ve kurallara uyumu konusunda uygulama kontrollerinin yapılması amaçlanmaktadır.

İç Kontrol bölümü organizasyon şemasında Yönetim Kurulunun altında konumlandırılmıştır.

- Bireysel Ticari, Muhasebe, Hukuk, Operasyon ve Bilgi İşlem bölümlerince yapılan iş ve işlemlerin kontrolünü gerçekleştirmek,
- İşletme faaliyetimizin Şirket içi politika, görev tanımları ve prosedürler ile teamüllere uyumunu kontrol etmek, bölümlerde yapılan işlemlerin yasaya ve ilgili diğer mevzuata uyum içinde düzenli ve verimli bir şekilde yürütülmesini sağlamak iş akış ve uygulama sırasında Şirketi riske sokacak bir yön bulunup bulunmadığını takip etmek,
- Bölümlerde yapılan kontroller sonucunda, uygulama aksaklığı veya eksikliğinin ya da genel aksaklıkların söz konusu olması durumunda, tespitlerin ilgili birimlerle paylaşılarak düzeltici ve önleyici faaliyet uygulanmasını talep etmek, her yıl Haziran ve Aralık aylarında tespit içeren raporu Yönetim Kurulu ile paylaşmak,
- Bölümlerdeki eksiklikler ve farklı uygulamalar ile ilgili olarak da eksik dokümantasyonların, düzeltici ve önleyici faaliyetlerle ilgili alınacak aksiyonları takip etmek,
- Yapılan tahsilat işlemlerinin kontrolü ile Kara paranın Aklanmasının Önlenmesi konusunda katkı sağlamak ve uyum fonksiyonuna bu anlamda destek vermek.

V. ÜYE'NİN RİSK MERKEZİ SÜREÇLERİ HAKKINDA GENEL BİLGİ

a. Kapsam dahilinde yer alan Risk Merkezi süreçleri hakkında bilgi ve özet (Madde 43.1.a)

i. Risk Merkezi Veri İletim Süreci

Üye tarafından Risk Merkezi'ne iletilen verilerle ilgili süreçler, Finans ve Muhasebe Müdürü ile İç Kontrol Yönetmeni tarafından yönetileceği şekilde planlanmıştır. Tüm bu işlemlerin, bilgi sistemleri prosedürlerinde belirtildiği gibi güvenli bir şekilde gerçekleştirilmesi planlanmıştır.

Risk Merkezine iletilen bilgilerin İç Kontrol Yönetmeni tarafından denetlenerek onaylanması ve ardından Risk Merkezine gönderilmesi planlanmıştır.

Recall RM sürecinin görev ve sorumluluklar açısından değerlendirildiğinde, aylık bildirim raporlarının Finans ve Muhasebe Bölümü Müdürü/Müdür Yardımcısı tarafından alınması, İç Kontrol birimi tarafından onaylanması gerektiği ve bu sürecin Genel Müdürün sorumluluğu altında yürütülmesi planlanmıştır.

Risk merkezi veri iletim süreçleriyle ilgili planlanan temel konular aşağıda özetlenmiştir.

- RM Raporlarının oluşturulması
- RM Raporlarının kontrolü ve denetlenmesi
- RM Raporlarının gönderilmesi

Risk Merkezi verilerine, Alga Bilişim tarafından sağlanan veritabanı desteği, Operasist Bilgi Teknolojileri ve Danışmanlık Hizmetleri Şirketi tarafından sunulan altyapı desteği ve TurkNet İletişim Hizmetleri A.Ş. tarafından sağlanan sunucu barındırma hizmeti ile erişim mümkün değildir. Bu sunucunun altyapı ve veritabanı işlemleri, iç kaynaklar tarafından yönetilmektedir.

Operasyonel faaliyetlerin gerçekleştirildiği iki sunucudan ilki olan Recall Uygulaması sunucusunun işletim seviyesinde Operasist Bilgi Teknolojileri ve Danışmanlık Hizmetleri şirketi ile uygulama seviyesinde acil durumlar için destek sağlayan Alga Bilişim firmaları; grup yetkileri çerçevesinde, uygulama seviyesinde herhangi bir erişime sahip olmadan gerekli bakım işlemlerini yürütmek için sistemlere erişebilmektedir. Bu erişimler:

- Yetki talep süreci ve onay kontrolü gerçekleştirilmiş,
- Süreli erişim sistemi kurgulanmış,
- Tüm erişimler video kayıt mekanizması izleme kontrolleri kurgulanmış,
- İz kayıtlarının gözden geçirilmesi kontrolü kurgulanmış,

ek kontroller ile izlenebilmektedir.

Sunucu barındırma hizmeti veren TurkNet İletişim Hizmetleri A.Ş'nin hiçbir sunucuya erişimi bulunmamaktadır .

Risk Merkezi faaliyetleri dahil olmak üzere tüm süreçler, tek bir uygulama olan "Recall" üzerinde yürütülmektedir. Kullanıcılar, bu uygulamaya erişim sağlamadan önce "Bilgi Güvenliği Uyum Taahhütnamesi"ni imzalamak zorunda kalmıştır. Ayrıca, her kullanıcı, edindikleri Bilgi Güvenliği Politikası'na uygun olarak belirlenen yetki seviyeleri doğrultusunda verilere erişebilir.

Kullanıcıların her bir işlemine dair Recall uygulaması üzerinde iz kayıtları tutulmasına ilişkin kontroller tasarlanmıştır.

ii. Risk Merkezi Veri Alım Süreci

Üye tarafından Risk Merkezi'nden alınan geri bildirim verileriyle ilgili süreçler, Genel Müdür/Genel Müdür yardımcısı ile İç Kontrol Yönetmeni tarafından yönetileceği şekilde planlanmıştır. Tüm bu işlemlerin, bilgi sistemleri prosedürlerinde belirtildiği gibi güvenli bir şekilde gerçekleştirilmesi planlanmıştır.

Risk Merkezinden alınan geri billdirim bilgileri İç Kontrol Yönetmeni tarafından denetlenerek Recall'a aktarılması planlanmıştır.

Recall RM sürecinin görev ve sorumluluklar açısından değerlendirildiğinde, aylık geri bildirim raporlarının Genel Müdür / Genel Müdür Yardımcısına bildirerek, İç Kontrol birimi tarafından Recall'a aktarılması gerektiği ve bu sürecin Genel Müdürün sorumluluğu altında yürütülmesi planlanmıştır.

Risk merkezi veri alım süreçleriyle ilgili planlanan temel konular aşağıda özetlenmiştir.

- RM Geri Bildirim Raporlarının yüklenmesi
- RM Geri Bildirim Raporlarının yüklensinin kontrolü ve denetlenmesi

Risk Merkezi verilerine, Alga Bilişim tarafından sağlanan veritabanı desteği, Operasist Bilgi Teknolojileri ve Danışmanlık Hizmetleri Şirketi tarafından sunulan altyapı desteği ve TurkNet İletişim Hizmetleri A.Ş. tarafından sağlanan sunucu barındırma hizmeti ile erişim mümkün değildir. Bu sunucunun altyapı ve veritabanı işlemleri, iç kaynaklar tarafından yönetilmektedir.

Operasyonel faaliyetlerin gerçekleştirildiği iki sunucudan ilki olan Recall Uygulaması sunucusunun işletim seviyesinde Operasist Bilgi Teknolojileri ve Danışmanlık Hizmetleri şirketi ile uygulama seviyesinde acil durumlar için destek sağlayan Alga Bilişim firmaları; grup yetkileri çerçevesinde, uygulama seviyesinde herhangi bir erişime sahip olmadan gerekli bakım işlemlerini yürütmek için sistemlere erişebilmektedir. Bu erişimler:

- Yetki talep süreci ve onay kontrolü gerçekleştirilmiş,
- Süreli erişim sistemi kurgulanmış,
- Tüm erişimler video kayıt mekanizması izleme kontrolleri kurgulanmış,
- İz kayıtlarının gözden geçirilmesi kontrolü kurgulanmış, ek kontroller ile izlenebilmektedir.

Sunucu barındırma hizmeti veren TurkNet İletişim Hizmetleri A.Ş'nin hiçbir sunucuya erişimi bulunmamaktadır .

Risk Merkezi faaliyetleri dahil olmak üzere tüm süreçler, tek bir uygulama olan "Recall" üzerinde yürütülmektedir. Kullanıcılar, bu uygulamaya erişim sağlamadan önce "Bilgi Güvenliği Uyum Taahhütnamesi"ni imzalamak zorunda kalmıştır. Ayrıca, her kullanıcı, edindikleri Bilgi Güvenliği Politikası'na uygun olarak belirlenen yetki seviyeleri doğrultusunda verilere erişebilir.

Kullanıcıların her bir işlemine dair Recall uygulaması üzerinde iz kayıtları tutulmasına ilişkin kontroller tasarlanmıştır.

b. Kapsam dahilinde yer alan Risk Merkezi süreçleri bölümlerinin organizasyon yapısı ve bölümlerin çalışan profili hakkında bilgi (Madde 43.1.b)

Denetim çalışmasının gerçekleştirildiği Üye birimlerine ilişkin bilgilere aşağıda yer verilmiştir.

- Genel Müdür
- İç Kontrol
- Finans ve Muhasebe Müdürü/Müdür Yardımcısı

Genel Müdür: Kemal Bayramoğlu

- Eğitim: Bahçeşehir Üniversitesi İşletme, İstanbul Üniversitesi İktisat
- Diğer Tecrübeler: Deren Varlık Yönetimi A.Ş (1.5 Vil) , Tam Faktoring (1 Vil), Girişim Varlik Yönetimi (6 Vil), Garanti Bankasi (4 Vil), Osmanli Bankasi (3 Vil), Sümerbank (6 Ay), Bagfai Bandirma Gübre Fabrikalari A.Ş
- Toplam Tecrübe: 25 yıl
- Üye Bünyesinde Toplam Tecrübe: 9,5 yıl

İç Kontrol Yönetmeni: Gamze Oransayoğlu

- Eğitim: Haliç Üniversitesi İşletme
- Diğer Tecrübeler: Denizbank A.Ş (10 yıl) , Aksen Hukuk Bürosu (2,5yıl)
- Toplam Tecrübe: 13 yıl
- Üye Bünyesinde Toplam Tecrübe: 1,5 Yıl

Finans ve Muhasebe Müdürü: Mehmet Oğuz

- Eğitim: Eskişehir Anadolu Üniversitesi - İşletme
- Diğer Tecrübeler: Mali Müşavir
- Toplam Tecrübe: 20 yıl
- Üye Bünyesinde Toplam Tecrübe: 6 yıl

c. Kapsam dahilinde yer alan Risk Merkezi süreçleri kapsamında destek alınan destek hizmeti kuruluşlarına ilişkin bilgi ve denetim sonuçları (Madde 31.1 ve Madde 31.2)

Risk Merkezi Üyesi'nin Risk Merkezi süreçlerini yürütürken destek aldığı destek hizmeti kuruluşlarına ve alınan hizmetlerin içeriğine ilişkin bilgilere aşağıda yer verilmiştir:

- **Alga Bilişim**

  Denge Varlık, Recall Tahsilat Yönetim Sistemi'nin teknik destek, arıza giderme, ek geliştirmeler yapma, tahsilat ve çalışan performansını izlemek için raporlama altyapısı sunma, yeni raporlar hazırlama, yeni kullanıcılara eğitim verme, portföy ve arama hizmetlerinden gelen verileri sisteme aktarma gibi hizmetleri almakta ve bu hizmetlerin Alga Bilişim tarafından sağlandığı gözlemlenmektedir. Ayrıca, tedarikçi firmanın kullanıcı hesaplarının Risk Merkezi'ne iletilen verilerin olduğu klasöre ve dosyalara erişim yetkisinin bulunmadığı belirlenmiştir.

- **Turknet İletişim Hizmetleri A.Ş**

  Denge Varlık tarafından kullanılan sunucuların barındırılması ve sunuculara ilişkin destek ve bakım hizmetinin sağlandığı tespit edilmiştir. Ancak, tedarikçi firmanın Risk Merkezi verilerine erişimi olduğuna dair herhangi bir kanıt bulunmamaktadır.

- **Operasist Bilgi Teknolojileri ve Danışmanlık Hizmetleri**

  Denge Varlık tarafından kullanılan BT donanımları ve yazılımlarının işletilmesi, ayarlanması ve sorunların giderilmesine yönelik destek hizmetinin sağlandığı tespit edilmiştir. Ancak, tedarikçi firmanın Risk Merkezi verilerine erişimi olduğuna dair herhangi bir kanıt bulunmamaktadır.

  Risk Merkezi Üyesi'nin destek hizmeti aldığı kuruluşlara ilişkin yapılan değerlendirme çalışması sonucunda 1 Eylül 2022 - 31 Ağustos 2023 dönemine ilişkin önemli ya da kayda değer bir kontrol eksikliğinin bulunmadığı görülmüştür.

VI. ÜYE DENETİMİ HAKKINDA BİLGİ

1 Eylül 2022 - 31 Ağustos 2023 dönemine ait Risk Merkezi Denetimi, Risk Merkezi Üyesi'nin Risk Merkezi Kontrol Hedefleri'ne karşılık gelen başlıklar altında her kontrol hedefine ilişkin detay kontrol testlerini mevcut kontrollerin önemlilik kriterini esas alarak uyumluluk, etkinlik ve yeterlilik açısından incelenmesini ve Bilgi Güvenliği Politikası değerlendirmelerini içermektedir.

Risk Merkezi Üye Denetimi sırasında tespit edilen ve önemli veya kayda değer kontrol eksikliği olarak sınıflandırılmayan kontrol zayıflıklarını içeren bir rapor Üye yetkilileri ile paylaşılmıştır.

Risk Merkezi Denetimi sırasında incelenen Üye'nin kontrol hedefleri ile mevcut kontrollerine ilişkin tablo aşağıda özetlenmektedir.

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
1.1	1	RM üyesi, RM'ne iletmek üzere hazırladığı risk verilerine ilişkin olarak, iç prosedür haline gelmiş bir "Gönderilecek Veri Akış ve Oluşturma Şeması" hazırlar ve güncel tutulmasını sağlar.	Risk Merkezi veri iletimi sürecindeki kontrollerin düzgün bir şekilde uygulanmaması ve yasalara uyumsuzluk riskine yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Aylık	BS Destekli Manuel	Recall	1	-	-	Başarılı	0
1.2	2	RM üyesi, RM tarafından kendisine iletilen verilerin, kendi sistemleri üzerinde nasıl akış ile dağıtıldığını, saklandığını ve işlendiğini	Risk Merkezi veri alımı sürecindeki kontrollerin düzgün bir şekilde uygulanmaması, yasalara	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Aylık	Otomatik	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		gösterecek şekilde ve iç prosedür haline gelmiş "Alınan Veri Akış ve Dağıtım Şeması"nı oluşturur ve güncel tutulmasını sağlar.	uyumsuzluğa yol açabilir.									

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
1.3	3	Canlı kredilerin sistemdeki limit ve riski ile Risk Merkezi'ne bildirilen kredi limit ve riski birbirini tutmaktadır. Canlı krediler için sistemde yer alan ve Risk Merkezi'ne raporlanan kredi riski ile mizandaki kredi riski rakamlarının mutabakatı yapılmaktadır.	Kredi risk bakiye bilgilerinin Risk Merkezi'ne hatalı bir şekilde iletilmesine neden olabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
1.3	4	Tasfiye olunacak alacaklar hesabında izlenen krediler için sistemde yer alan ve Risk Merkezi'ne raporlanan kredi limiti ve riski ile mizandaki kredi limit ve riski rakamlarının mutabakatı yapılmaktadır ve Risk Merkezi'ne bildirilen kredi limit ve riski birbirini tutmaktadır.	Tasfiye edilecek kredi risk bakiye bilgilerinin Risk Merkezi'ne hatalı bir şekilde iletilmesine ve geçmişe yönelik kontrol çalışmalarının gerçekleştirile memesine yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
1.3	5	Zarar niteliğindeki alacaklar hesabında izlenen krediler için sistemde yer alan ve Risk Merkezi'ne raporlanan kredi limit ve riski ile mizandaki kredi ve limit riski rakamlarının mutabakatı yapılmaktadır. Sistemdeki kredi limit ve riski ile Risk Merkezi'ne bildirilen kredi limit ve riski birbirini tutmaktadır.	Risk Merkezi'ne gönderilen zararlı alacak hesap bakiyesi bilgilerinin yanlış iletilmesine ve geçmişe dönük denetim faaliyetlerinin yapılamamasına yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
1.3	6	Risk Merkezi'ne yapılan raporlama verileri ile raporlamanın doğruluğuna ilişkin kontrollere ait dokümantasyon minimum 2 yıl süreyle saklanmaktadır.	Yetersiz dokümantasyon oluşturulmasına ve geçmişe yönelik denetimlerin gerçekleştirilememesine, aynı zamanda mevzuata uyumsuzluğa neden olabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Aylık	BS Destekli Manuel	FileServer	4	-	-	Başarılı	0
1.4	7	RM tarafından kullanıma sunulan güvenli veri iletim kanallarının kullanılmasına, söz konusu iletim kanalları dışında herhangi bir iletim kanalı doğrultusunda verinin dış taraflar ya da	Risk Merkezi üyesi ve Risk Merkezi arasındaki iletişim kanallarının güvenliği yeterince sağlanamadığında ve buna bağlı olarak gerekli kontrol ortamları oluşturulmadığında, Risk Merkezi	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Günlük	BS Destekli Manuel	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		RM ile paylaşılmaması na ilişkin kontrol ortamları oluşturulmalıdır.	verilerinin iletim sırasında kötüye kullanılması veya yetkisiz kişilerin bu verilere erişmesi riski artabilir.									
1.4	8	Veri alış verişinde RM üyesine ait alış-veriş noktasının da olası yetkisiz erişimlere karşı güvenliği sağlanmalıdır.	Risk Merkezi verisine yetkisiz erişimler meydana gelebilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Otomatik	Recall	1	-	-	Başarılı	0
1.5	9	RM raporları, Rapor bildirim tarihine kadar Risk Merkezi sistemine yüklenmektedir. Raporların hazırlanmasına ve verilerin iletilmesine	RM'ine raporların hatalı şekilde iletilmesine, raporların zamanında gönderilmemesine ve geçmişe dönük herhangi bir tespitin	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Günlük	BS Destekli Manuel	-	1	-	-	Başarılı	0

		ilişkin kontroller oluşturulmalı, düzenli olarak gerçekleştirilmeli ve kontrole ilişkin kayıtlar tutulmalıdır.	yapılamamasına yol açabilir.									
1.5	10	Veri alışverisi kapsamında manuel işler olması halinde, bir iş listesi oluşturulmalı, yığın işlerin yönetimine ilişkin RM üyesi bünyesinde atanmış bir personel bulunmalı ve kullanılan uygulama üzerinden gerçekleştirilen tüm işlemleri oluşturulan iş listesi ile etkin	Risk Merkezi üyesi tarafından Risk Merkezi'ne iletilmesi gereken verilerin zamanında hazırlanması ve iletilmesi konusunda kontrol mekanizmalarının eksik olması, Risk Merkezi'ne iletilen verinin bütünlüğünün ve doğruluğunun sağlanamamasına yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Günlük	BS Destekli Manuel	-	1	-	-	Başarılı	0

		kontrolünü sağlamalıdır.										

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
2.1	11	Risk Merkezi üyesi bünyesinde Risk Merkezi verilerinin güvenliğini sağlamaya yönelik Veri Güvenliği ve Erişimine yönelik politika porsedürler oluşturulur.	Risk Merkezi verilerinin güvenliğini sağlamak için gerekli politika ve prosedürlerin oluşturulmaması, Risk Merkezi verilerinin güvenliğinde zayıf noktaların ortaya çıkmasına neden olabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Manuel	MS	1	-	-	Başarılı	0
2.2	12	Risk Merkezi üyesinde çalışan ve konuyla ilgili yetkilendirilmiş personele bilgi güvenlik taahhütnamesi imzalatılarak sorumlulukları beyan edilir.	Risk Merkezi verilerine erişen, işleyen veya ileten personelin bilgi güvenliği taahhütnamesini imzalamaması, verilerin yetkilendirilmemiş kişilerin eline geçme riskini artırabilir ve veri ihlallerine yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	İşlem Bazlı	Manuel	-	4	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.1	13	Oluşturulan kimlik doğrulama altyapısı (kullanıcı hesap adı, şifre parametresi vb.) güncel durum itibariyle iyi uygulamalar ile uyumlu yapıda oluşturulur.	Risk Merkezi verilerinin bulunduğu ortamlara erişimde kullanılan kimlik doğrulama altyapısının yeterli güvenlik standartlarına sahip olmaması, bu ortamlara yetkisiz erişimlerin ve mevcut erişimlerdeki güvenlik zafiyetlerinin oluşmasına yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Otomatik	Recall Aktif Dizin MS SQL Veritabanı	3	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.2	14	Uygulanacak kimlik doğrulama mekanizması, kullanıcıların ve personelin bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilir. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.	Kimlik doğrulama bilgisinin oturum boyunca doğru bir şekilde sürdürülmesini sağlayacak tedbirlerin alınmaması, Risk Merkezi veri güvenliğinde zayıf noktaların oluşmasına neden olabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Otomatik	Recall Aktif Dizin MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.3	15	Uygulamaların, veritabanlarının ve işletim sistemlerinin kullanıcı hesapları içerisinde genel kullanıcı hesapları bulunmamaktadır.	Genel kullanıcı hesaplarının kullanılması ve bu hesaplar üzerinden gerçekleştirilen aktivitelerin izlenmemesi, yetkisiz işlemlerin kim tarafından, ne zaman ve hangi işlemlerle gerçekleştirildiğini belirleme açısından izlenemezlik çerçevesinde sorunlara yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı	1	Recall uygulaması canlı ortamında "TEST" isimli bir genel kullanıcı hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür. Aktif dizin kullanıcı listesindeki genel 6 adet test hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür.	KD	Başarısız	300

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.4	16	Firma bünyesinde her sistem ve uygulama için test, geliştirme ve üretim ortamlarına erişimler görevler ayrılığı ilkesi doğrultusunda tanımlanır.	Uygulama geliştirme yetkisine sahip personelin, gerçek ortama erişim ve değişiklik yapabilme yetkilerine sahip olması, sistem bütünlüğünü ve veri doğruluğunu tehlikeye atabilecek potansiyel riskleri beraberinde getirebilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	Recall Aktif Dizin MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.5	17	İlgili risk merkezi süreçlerine ilişkin görev tanımları ve yetkiler görevler ayrılığı göz önünde bulundurularak belirlenmiş, dokümante edilmiş, yönetim tarafından onaylanmış ve ilgili personele duyurulmuştur.	Etkin bir görevlerin ayrılması ortamının sağlanamaması, aynı zamanda mevzuata uymama riskini artırabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	Recall Aktif Dizin MS SQL Veritabanı Windows İşletim Sistemi	1	-	-	Başarılı	0
3.5	18	İlgili risk merkezi süreçlerine ilişkin sistemsel yetkiler düzenli aralıklarla gözden geçirilmekte, onaylanan görev tanımları ile uyumlu olup	Etkin bir görevlerin ayrılması ortamının kurulmaması, aynı zamanda mevzuata uyumsuzluğa yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı Windows İşletim Sistemi	3	-	-	Başarılı	-

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		olmadıkları değerlendirilmekte ve gerekli düzeltmeler yapılmaktadır(Sistemlere, servislere ve verilere ilişkin yetkilendirme düzeyi ve erişim haklarının ilgili unsurlara atanmasında gerekli olan en düşük yetkinin ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır).										

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.6	19	Hiç bir kullanıcı ya da sistemin kendi yetkilendirme düzeyini ve erişim haklarını önceden tanımlanmış düzeyin üzerine çıkartmasına izin verilmemektedir. Risk Merkezi verilerine erişebilen kişi/kişilerin kendilerine tesis edilen yetkileri bir üst seviyeye çıkartılamayacak şekilde güvenli ortamın oluşturulması sağlanır.	Personelin mevcut rol ve görev tanımları ile sistem üzerinde verilen yetkiler arasında tutarsızlık olması, personelin aslında sahip olmaması gereken yetkilere sahip olabilme riskini artırabilir ve Risk Merkezi verilerine yönelik güvenlik açıklarının oluşmasına neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı Windows İşletim Sistemi	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.6	20	Destek Hizmeti Firma/Personeli'nin üretim ortamlarına erişimlerine ilişkin kontrol ortamı oluşturulur: - Uzaktan erişimler de dahil tüm erişimler kayıt altına alınır ve gözden geçirilir. - Destek Hizmeti Firma/Personeli'nin erişimleri engellenir ya da süreli olarak gözetim altında verilir.	Risk Merkezi bilgilerinin ifşası mümkün olabilir. Yetkisiz erişimler nedeniyle sistemler üzerinde onaysız değişiklikler meydana gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı Windows İşletim Sistemi	2	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.7	21	RM üyesi, Risk Merkezi bilgilerinin işlendiği ve tutulduğu sistemler üzerinde oluşturulmuş olan ayrıcalıklı yetkiye sahip kullanıcılarının, yetkilerinin başka kişiler tarafından kullanımının önlenmesini teminen yeterli düzeyde farkındalıklarını sağlar. Bu kapsamdaki kullanıcı hesaplarının kullanımı sınırlandırılır.	Kullanıcı hesaplarının ne sistemsel ne de manüel kontrollerle sınırlanmaması, Risk Merkezi verilerine yetkisiz erişimlerin gerçekleşmesine yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı	2	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
3.8	22	Risk Merkezine iletilecek bilgilerinin işlendiği ve tutulduğu sistemler dâhilinde gerçekleşen kritik faaliyetlere ilişkin her türlü veri tabanı, uygulama ve sistemde oluşan değişiklik, ekleme ve silme işlemleri kayıt altına alınır ve saklanır.	Bilgi sistemleri içinde gerçekleşen kritik faaliyetlerle ilgili her türlü veritabanı, uygulama ve sistem loglarının silinmesi, kritik sistemlerde yapılan uygun olmayan işlemlerin artmasına ve izlenememesine yol açabilir. Ayrıca, denetim izlerinin doğruluğu ve bütünlüğünün korunmaması, olası yetkisiz veya kötüye kullanıma neden	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Otomatik	Recall Aktif Dizin MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			olabilecek olayların meydana gelmesi durumunda kim tarafından, ne zaman, ne yapıldı gibi bilgilere ulaşılamamasına ve olayın nedenlerinin belirlenememesine neden olabilir.									
3.9	23	Görevler ayrılığı ilkesine uyumu kontrol etmek amacıyla işletim sistemi, veritabanı ve uygulamalara erişim yetkilerinin en az yılda bir defa gözden geçirilmesine ve	Yetki gözden geçirme çalışmalarının gerçekleştirilmemesi veya yetersiz olması, mevcut yetkilerin kullanıcıların yetkinliklerine ve görev ayrılığına	Gamze Oransayoğlu – İç Kontrol Yönetmeni	3 Aylık	Manuel	Recall Aktif Dizin MS SQL Veritabanı	3	Haziran 2023 İç kontrol raporunda Recall uygulamasına ait yetkilerin gözden geçirildiği görülmüştür. Ancak Aktif Dizin ve MS SQL veritabanı kullanıcı yetkilerinin	KD	Başarısız	300

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		onaylanmasına yönelik çalışmalar yapılır.	uygun bir şekilde verildiğinden emin olma konusunda güvence sağlayamamaya ve ilişkili durumla ilgili gereken aksiyonların zamanında alınmamasına neden olabilir. Bunun yanı sıra, bilgilerin güvenilirliği, tutarlılığı ve bütünlüğü ile ilgili sorunlar yaşanabilir ve bilgilere yetkisiz kişiler tarafından erişim sağlanabilir.						gözden geçirilmediği belirlenmiştir.			

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
4.1	24	Güvenlik alanındaki güncel gelişmeler ve yeni açıkları takip etmek, gerekli yazılım güncellemeleri yapmak ve gerekli yamaları uygulamak amacıyla çalışmalar gerçekleştirilir.	Güvenlik yama yönetiminin uygulanmaması, güncel tehditlere karşı güvenlik açıklarının ortaya çıkmasına yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı	1	-	-	Başarılı	0
4.2	25	İç ağın farklı güvenlik hassasiyetine sahip alt bölümleri birbirinden ayrılır ve kontrollü geçişi temin etmek üzere güvenlik duvarları kullanılır.	RM üyesi dışına verilerin iletilirken güvenlik duvarının kullanılmaması ve RM üyesi iç ağı yapısının güvenli olmaması, RM verilerinin içeride veya	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Otomatik	Checkpoint	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			dışarıda yetkisiz kişilerin erişimine açık hale gelmesine neden olabilir.									
4.2	26	Güvenlik kontrollerinin yeterliliğini test etmek üzere en az yılda bir kez olmak üzere, güvenlik testleri gerçekleştirilir.	Düzenli periyotlarda sızma testlerinin gerçekleştirilmesi, bilgi güvenliği açıklarının bilinmemesi ve bunun sonucu olarak önemli bir bilgi güvenliği olayının yaşanabilmesi riskine sebep olabilmektedir.	Onur Eren – Bilgi İşlem Yetkilisi	Yılda 1 kez	BS Destekli Manuel	Tüm Sistemler	-	Sızma testinin bağımsız ekiplerce yapılmadığı görülmüştür.	KZ	Başarısız	0
4.2	27	Sistemlere lokasyon içinden ve uzaktan erişen kullanıcıların mantıksal erişim kontrolleri için erişim	RM bilgilerinin işlendiği ve saklandığı sistemlere erişim için uygun yetkilendirme ve erişim	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall Aktif Dizin MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		konfigürasyonu ve kimlik onaylama kullanılır.	kontrolünün kurulmaması, RM için kritik öneme sahip sistemlerde yetkisiz işlemlerin gerçekleştirilmesine neden olabilir.									
4.2	28	Dış ağlardan gelebilecek tehditlerin tespit edilmesine ve önlenmesine yönelik saldırı tespit ve önleme sistemleri kullanılır.	Dış ağlardan gelebilecek saldırıların tespit edilmesi ve engellenmesinde sorunlar yaşanması, sistem bütünlüğünün sağlanmamasına yol açabilir. Bu durumda sistemler ve veriler saldırılara karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Checkpoint	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
4.3	29	Risk Merkezi verilerinin saklanacağı ve işleneceği tüm sistem altyapısında,toplu verinin kötü niyetle sistem dışına çıkarılmasını engellemek amacı ile CD/DVD yazıcı gibi cihazlar ve USB kullanımı onay dahilinde gerçekleşir ve yetki bazında sınırlandırmalar yapılır. Fiziksel veri depolama	Toplu verinin dış ortamlara çıkışını sınırlamamak, verinin ifşasına ve yetkisiz kişilerin verilere erişmesine yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Checkpoint Symantec Endpoint	1	Recall sisteminden çekilen ve RM verilerini içeren raporlara ait iz kayıtlarının tutulduğunu, görevler ayrılığı kapsamında sistemsel yetkilendirmelerin tasarlandığı, antivirüs ve güvenlik duvarı gibi temel güvenlik kontrollerinin bulunduğu görülmüş olmakla beraber veri sızıntısını önlemeye	KZ	Başarısız	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		araçlarını korumak için güvenli şifreleme, koruma ve teslim yöntemleri kullanılır. Veri envanteri çalışması kapsamında belirlenen risk değerlemesi doğrultusunda sistem dışına çıkışı gerçekleştirilecek veriler belirlenir. DLP kurulumu ya da kişisel posta hesaplarına ve dropbox vb. depolama alanlarına erişimin engellenmesi vb. gibi yöntemler ile kurum dışına							yönelik olarak DLP (Örnek: eposta üzerinden paylaşılabilen raporlar) gibi engelleyici bir kontrol mekanizmasının bulunmadığı görülmüştür.			

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		onaysız veri çıkışı önlenir.										
4.4	30	Sistem, sunucu ve bilgisayarlarda, virüs koruma yazılımı yüklü ve çalışır durumda bulunur.	Sistem güvenliği, kötü niyetli yazılımlara karşı proaktif koruma sağlanmaması nedeniyle tehlikeye girebilir. Bu durumda sistem bütünlüğü sağlanamayabilir ve sistemler ile veriler virüs saldırılarına karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Symantec Endpoint	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
4.4	31	Sistem, sunucu ve bilgisayarlarda, virüs koruma yazılımı düzenli virüs taramaya göre ayarlanır.	Sistem güvenliği, kötü niyetli yazılımlara karşı proaktif bir koruma ile sağlanmazsa, sistem bütünlüğü sağlanamayabilir ve sistemler ile veriler virüs saldırılarına karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Symantec Endpoint	1	-	-	Başarılı	
4.4	32	Sistem,sunucu ve bilgisayarlarda, virüs koruma yazılımı virüs tanım dokümanlarının otomatik güncellenmesine yönelik ayarlanır.	Sistem güvenliği, kötü niyetli yazılımlara karşı proaktif bir koruma ile sağlanmazsa, sistem bütünlüğü sağlanamayabilir ve sistemler ile veriler virüs saldırılarına karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Symantec Endpoint	1	-	-	Başarılı	

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
4.4	33	Sistem, sunucu ve bilgisayarlara yönelik olarak virüs tarama sonuçları güvenlik fonksiyonu tarafından konsolide bir şekilde gözden geçirilir veya otomatik alarm mekanizması (e-posta, sms vb.) güvenlik fonksiyonuna alarm gönderir.	Sistem güvenliği kötü niyetli yazılımlara karşı proaktif koruma sağlanmadığında, sistem bütünlüğü sağlanamayabilir ve sistemler ile veriler virüs saldırılarına karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Symantec Endpoint	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
4.4	34	Virüs koruma yazılımı tek bir merkezden yönetilir.	Sistem güvenliği, kötü niyetli yazılımlara karşı proaktif koruma ile sağlanamadığında, sistem bütünlüğü sağlanmayabilir ve sistemler ile veriler virüs saldırılarına karşı savunmasız hale gelebilir.	Onur Eren – Bilgi İşlem Yetkilisi	Anlık	BS Destekli Manuel	Symantec Endpoint	1	-	-	Başarılı	0
4.5	35	Risk Merkezi üyesi tarafından Risk Merkezine iletilen veya Risk Merkezinden temin edilen verinin alımı esnasında güvenli iletim kanalları ve sistemler kullanılır.	RM üyesi ve RM arasındaki iletişim kanallarının güvenliğinin yeterli seviyede sağlanamaması ve bu konuyla ilgili gerekli kontrol önlemlerinin oluşturulmaması, Risk Merkezi	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			verilerinin iletimi sırasında kötüye kullanılmasına veya yetkisiz kişilerin verilere erişmesine yol açabilir.									

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
5.1	36	Risk Merkezi verilerinin tutulduğu ve işlendiği uygulamalar için uygulama geliştirme, test ve işletme faaliyetlerine ilişkin süreç adımları ve sorumlulukları, politika ve prosedürler aracılığı ile tanımlamış olmalıdır. Buna ek olarak değişiklik sürecinin yönetilmesine ilişkin Risk Merkezi üyesi tarafından takip süreci tasarlanır ve işletilir.	Geliştirme, test ve canlı ortama erişen personelin, sistem üzerindeki yetkilerle uyumsuz olan tanımlı roller ve görevlerle veya yetkilerin net bir şekilde belirlenmemesi, değişiklik yönetimi sürecinin kötüye kullanılmasına ve güvenlik açıklarının ortaya çıkmasına neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	Recall MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
5.2	37	Her sistem ve uygulama için ayrı geliştirme, test ve üretim ortamı oluşturulur. Test ortamları, üretim ortamları ile etkileşimde olmayacak şekilde ayrıştırılır. Test ortamları üretim ortamına benzer yapıda oluşturulur.	Test ortamının canlı ortamı tam olarak yansıtması, hassas üretim verilerinin test ortamında ifşa edilmesine yol açabilir. Gerçek verilerin test ortamında herhangi bir değiştirme veya maskeleme yapılmadan kullanılması, veri gizliliğinin sağlanamamasına neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Otomatik	Recall MS SQL Veritabanı	2	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
5.2	38	Risk Merkezi verilerinin test ve geliştirme ortamlarına kopyalanırken anonimleştirilmesi sağlanır.	Test ortamının canlı ortamı tam olarak yansıtması, hassas üretim verilerinin test ortamında ifşa edilmesine yol açabilir. Gerçek verilerin test ortamında herhangi bir değiştirme veya maskeleme yapılmadan kullanılması, veri gizliliğinin sağlanamamasına neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Otomatik	Recall MS SQL Veri tabanı	1	-	-	Başarılı	0
5.3	39	Risk Merkezi üyesi bünyesinde Risk merkezi verilerinin saklandığı ve işlendiği uygulamalarda gerçekleştirilecek	Standart bir değişiklik yönetim sürecinin kurulmaması, doğrudan veya dolaylı olarak RM verisinin	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall MS SQL Veritabanı	2		.	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		yazılım ve konfigürasyon değişiklik talepleri talebin açılmasından üretim ortamına aktarıma kadarki tüm süreci talep onay sürecini kapsayacak şekilde kayıt altına alınır. Risk Merkezi verilerinin saklandığı ve işlendiği uygulamalarda gerçekleştirilecek her türlü yazılım ve konfigürasyon değişiklikleri süreç sahibi tarafından onaylanır.	güvenliğine ilişkin zafiyetlerin ortaya çıkmasına neden olabilir.									

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
5.3	40	Uygulama yazılımı ve veritabanı değişikliklerinin üretim ortamına aktarılmasına ilişkin iz kayıtları tutulur. (değişikliği gerçekleştiren kişi, gerçekleştirme zamanı, değişiklik detayıvb.)	Üretim ortamına aktarılan değişiklik taleplerine dair denetim izlerinin kaydedilmemesi, yetkisiz kişilerin uygun olmayan değişiklikleri canlı ortama aktarmasına yol açabilir. Bu durumda veri güvenilirliği sağlanamayabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall MS SQL Veritabanı	4	-	-	Başarılı	0
5.3	41	Değişiklik talepleri ile aktarım iz kayıtları eşleştirilir.	Üretim ortamına aktarılan değişiklik taleplerine ilişkin denetim izlerinin tutulmaması, yetkisiz kişilerce uygun olmayan değişikliklerin canlı ortama aktarılmasına	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Recall MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			sebep olabilir. Veri güvenilirliği sağlanamayabilir.									
5.3	42	Risk Merkezi verilerinin tutulduğu ve işlendiği uygulamalar için uygulama geliştirme, test ve işletme faaliyetlerine ilişkin süreç adımları ve sorumlulukları, politika ve prosedürler aracılığı ile tanımlamış olmalıdır. (Değişiklik yönetim prosedürü, test prosedürü vb.) Buna ek olarak değişiklik sürecinin	Üretim ortamına aktarılan değişiklik talepleriyle ilgili denetim izlerinin kaydedilmemesi, yetkisiz kişilerin canlı ortama uygunsuz değişiklikler yapmasına yol açabilir ve bu durumda veri güvenilirliği sağlanamayabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	Recall MS SQL Veritabanı	2	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		yönetilmesine ilişkin Risk Merkezi üyesi tarafından takip süreci tasarlanır ve işletilir.										
5.4	43	Test edilmiş olan değişikliğin değişmeden üretim ortamına aktarılmasına ilişkin kontroller oluşturulur.	Değişikliklerin üretim ortamına değişmeden aktarılmasını sağlayacak kontrollerin eksik veya yetersiz olması, yetkisiz değişikliklerin üretim ortamına aktarılmasına yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall MS SQL Veritabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
6.1	44	RM üyesi bünyesinde Risk Merkezi tarafından sağlanan verilerin yer aldığı sistemler ve uygulamalar üzerinde denetim izi kayıtları (kritik işlemler ve ayrıcalıklı yetkilere sahip kullanıcıların yaptığı işlemleri de içerecek şekilde) asgari olarak aşağıdaki detayda tutulur. a. Bu kapsamdaki işlemlere ilişkin yetkisiz erişim teşebbüslerine, b. İşlemi gerçekleştiren uygulamaya,	Denetim izlerinin doğruluğu ve bütünlüğü sağlanmadığında, potansiyel yetkisiz veya kötüye kullanım olayları meydana geldiğinde kim tarafından, ne zaman, ne yapıldı gibi bilgilere erişilemez ve olayın nedenleri tespit edilemez.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Recall MS SQL Veritabanı Aktif dizin Dosya sunucusu	2	-		Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		c. İşlemi gerçekleştiren kişinin kimliğine, d.Yapılan işlemlerin zamanına.										
6.2	45	Risk Merkezi tarafından sağlanan verilerin yer aldığı sistemler üzerinde alınan denetim izi kayıtlarının bütünlüğünün bozulmasını önleyici teknikler kullanılır.	Denetim izi kayıtlarının değiştirilemezliğinin ve bütünlüğünün korunmaması, tutulan denetim izlerinin doğruluğundan emin olunamamasına yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Event Log Analyzer	10	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
6.3	46	RM üyesi bünyesinde Risk Merkezi tarafından sağlanan verilerin yer aldığı sistemler ve uygulamalar üzerinde tutulan denetim izi kayıtları periyodik olarak gözden geçirilir.	Ayrıcalıklı yetkilere sahip kullanıcılar tarafından gerçekleştirilen kritik aktiviteler için gözden geçirme faaliyetlerinin oluşturulmaması, hatalı veya kasıtlı işlemlerin zamanında tespit edilememesine yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Aylık	BS Destekli Manuel	MS SQL veritabanı Dosya sunucusu	10	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
7.1	47	Risk Merkezi üyesi ile Risk Merkezi arasında gerçekleştirilen veri alışverişine yönelik sürecin etkin işlemesi adına kontroller oluşturulmalıdır. Veri alışverişi süreci kapsamında otomatik işler olması halinde söz konusu işlere yönelik iş listeleri hazırlanması, yığın işlerin etkin olarak yönetimi sağlanmalı ve süreç takip edilmelidir.	Otomatik işlerin takip edilmesine yönelik bir sürecin tasarlanmamış olması, otomatik işlerde oluşabilecek potansiyel hataların ve arızaların zamanında tespit edilememesine yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
8.1	48	RM üyesi, Risk Merkezi verilerinin tutulduğu ve işlendiği ve Risk Merkezi tarafından sağlanan verilerin saklandığı üretim ortamını barındıran tüm sistem bileşenlerinin uygun/belirli aralıklar ile yedekleri alınır.	RM verilerinin bulunduğu alanlarda yedekleme işlemlerinin belirli bir süreci takip etmeksizin veya hiç yapılmaksızın gerçekleştirilmesi, RM verilerine erişim sorunlarının ortaya çıkmasına yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Günlük	Otomatik	VMware Backup	2	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
8.1	49	Olağanüstü durum esnasında sistemlerin devamlılığını sağlamak amacıyla bir olağanüstü durum merkezi (Tam donanımlı, yarı donanımlı, az donanımlı) oluşturulur.	Hizmet sürekliliğinin sağlanamaması, sistem kesintilerinin yaşanmasına ve dolayısıyla müşteri kayıplarının meydana gelmesine neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall MS SQL Veritabanı	1	-	-	Başarılı	0
8.2	50	Yedekten geri dönüş testleri Risk Merkezi üyesi bünyesinde oluşturulan plan doğrultusunda periyodik olarak gerçekleştirilir.	Veri yedeklerinin düzenli olarak alınmadığı, yedeklerin periyodik ve kapsamlı bir şekilde denetlenmediği ve/veya veri yedeklerinin güvenliği sağlanmadığı durumlarda, RM Üyesi veri kaybı riskiyle karşı	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall MS SQL Veritabanı	6	.	-	Başarılı	-

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			karşıya kalabilir ve bu durum RM Üyesi'nin iş sürekliliğini ve verimliliğini olumsuz yönde etkileyebilir. Ayrıca, yedeklerden geri dönüş testlerinin yapılmaması, veri kaybı olasılığını artırabilir.									
8.3	51	Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa olağanüstü durum merkezi üzerinden testler yapılır, testlere varsa dış hizmet sağlayıcılar da dahil edilir, test sonuçları üst	Felaket kurtarma testlerinin gerçekleştirilemesi durumunda, bir felaket anında, iş sürekliliğini sağlamak için uygun süreçlerin devreye alınmamasına, iş kayıplarının oluşmasına,	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall MS SQL Veritabanı	1	-	-	Başarılı	-

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		yönetime raporlanır ve bu sonuçlara göre plan güncellenir.	itibar kayıplarına ve finansal kayıplara yol açabilir.									

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
9	52	Risk Merkezi üyesi bünyesinde verilerin hassasiyet derecelerinin belirlenerek uygun güvenli önlemlerinin alınabilmesine yönelik veri sınıflandırma çalışmaları gerçekleştirilir. Gizlilik sınıflandırmasında en az aşağıdaki sınıflandırmanın kullanılması beklenmektedir. - Gizli Bilgi - Dahili Kullanıma İlişkin Bilgi - Kamuya Açık Bilgi Risk Merkezi verilerinin "Gizli	RM üyesine ait tüm RM verilerinin bulunduğu bilgi varlıkları için bir envanterin oluşturulmaması ve bu varlıkların sahiplerinin tanımlanmaması, üye organizasyonun hangi varlıklara sahip olduğunu bilememesine ve varlıkların yönetilmesi gereken sorumlulukların belirlenememesine yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Manuel	-	-	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		Bilgi" olarak değerlendirilmesi esastır.										
9	53	Risk merkezi üyelerinin ve hizmet veren kuruluşların sorumlulukları açıkça tanımlanmalıdır.	Risk merkezi üyelerinin ve hizmet sağlayıcı kuruluşların sorumlularının belirlenmemesi, görevlerin ayrılmasının sağlanamamasına ve RM verisiyle ilgili işlerin etkin bir şekilde yürütülememesine yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Manuel	-	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
9	54	Risk Merkezi üyesi bünyesinde Risk Yönetim Politikası ve prosedürleri oluşturulur ve periyodik olarak güncellenir.	Risk yönetimi sürecinin tasarlanmaması, RM üyesinde bulunan ve RM verisini etkileyen BT risklerinin etkili bir şekilde yönetilememesine ve bu risklere karşı gerekli önlemlerin alınamamasına yol açabilir.	Gamze Oransayoğlu – İç Kontrol Yönetmeni	Yıllık	Manuel	-	-	-	-	Başarılı	0
9	55	Risklerin, risklere yönelik kontrollerin ve aksiyon plalarının belirlendiği, Kurum ile Risk Merkezi arasında mantıksal veya fiziksel veri alışverişlerinde verinin güvenliğini ve	Mevcut risklerin belirlenmemesi, RM üyesi ile Risk Merkezi arasındaki mantıksal veya fiziksel veri alışverişlerinde verinin	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	-	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		değiştirilemezliğini sağlamaya yönelik riskleri de içeren bir risk envanteri çalışması gerçekleştirilir ve güncel tutulması sağlanır. (Bu kapsamda özellikle iletilen ve alınan verilere yönelik risk değerleme çalışması da gerçekleştirilir).	güvenliğini ve değiştirilemezliğini sağlamaya yönelik risklerin değerlendirilmemesine yol açabilir. Bu durum doğru stratejik ve taktik kararların alınmasını engelleyebilir.									
9	56	Risk Merkezi üyesi bünyesinde bilgi güvenliği olay yönetim süreci tasarlanır. Üye bünyesinde karşılaşılan tüm bilgi güvenliği olayları kayıt altına alınır.	Kurum içindeki güvenlik olaylarının zamanında tespit edilememesi, karşılaşılan olaylara uygun şekilde müdahale edilememesine ve RM verisine erişimde	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	-	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			kesintilerin meydana gelmesine yol açabilir. Ayrıca, BT süreçlerinde kesintiler veya güvenlik olayları meydana geldiğinde, Risk Merkezi yönetiminin hızla bilgilendirilememesi durumu da ortaya çıkabilir.									
9	57	Girilen müşteri bilgileri (şube adı, kurum bilgisi, üye adı, TCKN/VKN, sektör kodu, hesap kodu) girişi ve değişikliği yapılırken sistemsel/ manuel kontrol	Yetkisiz veya hatalı işlemlerin gerçekleştirilmesine, ilgili işlemlerin zamanında tespit edilememesine,	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Otomatik	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
		mekanizması ile kaydedilmektedir.	Risk Merkezi'ne hatalı veri iletilmesine ve mevzuat ile uyumsuzluğa yol açabilir.									
9	58	Kredi limit/vade girişleri ve güncellemeleri sistemsel/ manuel kontrol mekanizmaları dahilinde yapılmaktadır.	Yetkisiz veya hatalı işlemlerin gerçekleştirilmesine, ilgili işlemlerin zamanında tespit edilememesine, Risk Merkezi'ne hatalı veri iletilmesine ve mevzuat ile uyumsuzluğa yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
9	59	Kredi risk bilgisi girişleri sistemsel/ manuel kontrol mekanizmaları dahilinde yapılmaktadır.	Yetkisiz veya hatalı işlemlerin gerçekleştirilmesine, ilgili işlemlerin zamanında tespit edilememesine, Risk Merkezi'ne hatalı veri iletilmesine ve mevzuat ile uyumsuzluğa yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	BS Destekli Manuel	Recall	1	-	-	Başarılı	0
9	60	Krediye yapılan tahsilatlara ilişkin tutarlar doğru risk vadesi grubundan düşülmektedir.	Risk Merkezi'ne iletilen kredi bilgilerinin doğruluğu konusunda sorunlar oluşturabilir ve mevzuat ile uyumsuzluğa yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
9	61	Kredi türü (TL/YP, nakit/gayrinakit, vb.) sistemde doğru bir şekilde sınıflandırılmaktadır.	Risk Merkezi'ne hatalı kredi risk bilgisi iletilmesine yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0
9	62	Gecikme gün sayısına sistemde manuel müdahale edilememektedir ve rapora doğru olarak yansıtılmaktadır.	Risk Merkezi'ne iletilen kredi bilgilerinin doğruluğu konusunda riskler oluşturabilir ve mevzuata uyumsuzluk sorunlarına yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0
9	63	Limit aşımları olan krediler için limit risk bilgileri doğru şekilde rapora aktarılmaktadır.	Risk Merkezi'ne iletilen kredi ve limit bilgilerinin doğruluğu konusunda	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			riskler oluşturabilir.									
9	64	Risk Merkezi'ne yapılan raporlamalardaki vade kırılımları kredilerin ödeme planlarına göre belirlenmektedir (0-12 ay arası kısa vadeli risk, 12-24 ay arası orta vadeli risk, 24 ay üzeri uzun vadeli risk olarak sınıflandırılmalı).	Risk Merkezi'ne iletilen kredi bilgilerinin doğruluğu konusunda riskler oluşturabilir ve mevzuata uyumsuzluk sorunlarına yol açabilir.	Uygulanabilir Değildir (U/D)	U/D	U/D	U/D	U/D	-	-	U/D	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
9	65	Risk Merkezi tarafından hatalı olduğu bildirilen bilgilere ilişkin düzeltici aksiyon alınmakta, herhangi bir cezai yaptırım bulunması durumunda üst yönetime bilgilendirme yapılmaktadır.	Risk Merkezi üyesinin hatalı bir şekilde raporlama yapmaya devam etmesine ve cezai yaptırımlarla karşılaşmasına yol açabilir.	Onur Eren – Bilgi İşlem Yetkilisi	İşlem Bazlı	Manuel	-	-	-	-	Başarılı	0
9	66	Risk Merkezi verisi bulunan sistemlere yönelik bir iş etki analizi çalışması gerçekleştirilir.	İş etki analizinin yapılmaması, olayların etkilerinin doğru bir şekilde anlaşılamamasına ve çözümlerin gereken süre içinde sağlanamamasına neden olabilir. Bu	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	BS Destekli Manuel	Recall MS SQL Veri Tabanı	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			durumda kritik hizmet olayları tanımlanamaz ve gerektiği şekilde çözülemez.									
9	67	Risk Merkezi üyesi bünyesinde Risk Merkezi tarafından yayımlanan Bilgi Güvenliği dokümanı kapsamında belirlenen standartlar doğrultusunda politika oluşturulmalı ve işletimi gözetilmelidir.	Bilgi Güvenliği Politikası'nın oluşturulmaması, RM verisine erişen tarafların RM verisinin önemini ve gizliliğini yeterince anlamamalarına ve veriyi etkili bir şekilde kullanamamalarına ve veri güvenliğinin sağlanamamasına yol açabilir. Ayrıca, kurumun bilgi güvenliği politikasının	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	-	1	-	-	Başarılı	0

Kontrol Hedefi	Kontrol Numarası	Kontrol Tanımı	Risk Tanımı	Kontrol Sorumlusu	Kontrol Sıklığı	Kontrol Tipi	İlgili Sistem	İncelenen Örneklem Sayısı	Eksiklik/Bulgu Tanımı	Bulgu Sınıflandırması	Sonuç	Risk Puanı
			güncellenmemesi ve yayımlanmaması, güvenlik olaylarının meydana gelmesine neden olabilir.									
9	68	Bilgi Güvenliği Politikası periyodik olarak gözden geçirilerek gerekli görüldüğü durumlarda güncellenerek onaylatılmaktadır.	Politikanın Risk Merkezi üyesinin ve Risk Merkezi'nin beklediği güncel mevzuatlarla uyumsuz olmasına neden olabilir.	Onur Eren – Bilgi İşlem Yetkilisi	Yıllık	Manuel	-	1	-	-	Başarılı	0
											Toplam Risk Puanı	600

VII. BULGU TABLOSU

1 Eylül 2022 - 31 Ağustos 2023 yılı Risk Merkezi Üye kontrol ortamlarının ve aldığı destek hizmetlerinin değerlendirilmesi sonucunda tespit edilen kayda değer kontrol eksiklikleri aşağıdaki tablolarda belirtilmektedir.

Kontrol Hedefi	**3.3**	**Bulgu Kodu**	**2023.ERSM.0001.KD**
Kontrol Hedefi	Risk Merkezi bilgilerinin işlendiği ve tutulduğu sistemlere erişen kullanıcılar tarafından gerçekleştirilen tüm işlemler kişisel kullanıcı hesapları kullanılarak yapılmalı, ortak kullanıcı hesabı kullanılmamalıdır. RM üyesi tarafından kullanılan sistemlerin özellikleri gereği değiştirilemez veya jenerik kullanıcı hesaplarının kullanılması zorunluluğu bulunması durumunda veya RM verilerine bir uygulama kullanıcısı üzerinden erişilebilen altyapılarda, bilgiye erişen gerçek kişi kullanıcıyı belirleyebilecek eşleştirme altyapısı oluşturulmalıdır.		
Kontrol Tanımı	Uygulamaların, veritabanlarının ve işletim sistemlerinin kullanıcı hesapları içerisinde genel kullanıcı hesapları bulunmamaktadır.		
Durum Tespiti	Recall uygulaması canlı ortamında "TEST" isimli bir genel kullanıcı hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür. Aktif dizin kullanıcı listesindeki genel 6 adet test hesabı olduğu ve herhangi bir Kurum içi personele sorumluluğunun atanmadığı görülmüştür.		
Denetim Sonucu	Etkin Değil		
Risk Tanımı	Genel kullanıcı hesaplarının kullanılması ve bu hesaplar üzerinden gerçekleştirilen aktivitelerin izlenmemesi, yetkisiz işlemlerin kim tarafından, ne zaman ve hangi işlemlerle gerçekleştirildiğini belirleme açısından izlenemezlik çerçevesinde sorunlara yol açabilir.		
Üyenin Görüşü/Cevabı	Önceki dönemlerde IT çalışanlarının Recall updatelerini test etmek için açmış olduğu, ancak kapatılması atlanmış olan hesaplardır. İlgili dönem ve test aşaması dışında kullanılmamıştır. 16.08.2023 tarihinde "TEST1" hesabı IT çalışanımız Onur Eren'e sahiplik ataması yapılmış olup, diğer tüm test hesapları kapatılmıştır. Yılda 2 kez İç Kontrol tarafından kontrol noktası konulmasına karar verilmiştir.		
Bağımsız Denetçinin Sonuç Değerlendirmesi	Bulgu denetimimiz sırasında düzeltilmiştir. 16.08.2023 tarihinde Recall uygulaması canlı ortamında "TEST" isimli genel kullanıcı hesabının kapatıldığı görülmüştür. Aktif dizin kullanıcı listesindeki genel 5 adet test hesabının kapatıldığı ve bir hesabın açık bırakılarak Bilgi İşlem Yetkilisinin sorumluluğuna resmi olarak atandığı belirlenmiştir.		

Kontrol Hedefi	**3.9**	**Bulgu Kodu**	**2023.ERSM.0002.KD**
Kontrol Hedefi	RM üyesi, Risk Merkezi bilgilerinin tutulduğu ve işlendiği sistemlerde tanımlanmış olan yetkileri (kullanıcı hesapları ve yetkileri) yılda en az bir kez gözden geçirilmeli, gözden geçirme faaliyetleri kayıt altına alınmalıdır. Tüm kullanıcı ve sistemlere atanmış olan yetkiler ve erişim hakları, başta işletim sistemi, veri tabanı, uygulama ve diğer katmanlar olmak üzere, en az yıllık olarak güncel durumla uyumlulukları açısından değerlendirilmeye tabi tutulmalı ve uyumsuz olan yetki tanımlamaları sistem yetki düzenlemeleri gerçekleştirilerek uyumlu hale getirilmelidir.		
Kontrol Tanımı	Görevler ayrılığı ilkesine uyumu kontrol etmek amacıyla işletim sistemi, veritabanı ve uygulamalara erişim yetkilerinin en az yılda bir defa gözden geçirilmesine ve onaylanmasına yönelik çalışmalar yapılır.		
Durum Tespiti	Haziran 2023 İç kontrol raporunda Recall uygulamasına ait yetkilerin gözden geçirildiği görülmüştür. Ancak Aktif Dizin ve MS SQL veritabanı kullanıcı yetkilerinin gözden geçirilmediği belirlenmiştir.		
Denetim Sonucu	Etkin Değil		
Risk Tanımı	Yetki gözden geçirme çalışmalarının gerçekleştirilmemesi veya yetersiz olması, mevcut yetkilerin kullanıcıların yetkinliklerine ve görev ayrılığına uygun bir şekilde verildiğinden emin olma konusunda güvence sağlayamamaya ve ilişkili durumla ilgili gereken aksiyonların zamanında alınmamasına neden olabilir. Bunun yanı sıra, bilgilerin güvenilirliği, tutarlılığı ve bütünlüğü ile ilgili sorunlar yaşanabilir ve bilgilere yetkisiz kişiler tarafından erişim sağlanabilir.		
Üyenin Görüşü/Cevabı	RM verilerin işlendiği ve saklandığı Recall programı için çeyrek dönemlerde olmak üzere yılda 4 kez İç Kontrol tarafından yetki gözden geçirme raporu yapılmaktadır. AD ve MS SQL için 29.08.2023 tarihinde yetki gözden geçirme raporu yapılmış ve denetime sunulmuştur. İç Kontrol tarafından yılda 1 kez AD ve MS SQL için yetki gözden geçirme çalışması yapılmasına karar verilmiştir.		
Bağımsız Denetçinin Sonuç Değerlendirmesi	Bulgu denetimimiz sırasında düzeltilmiştir. 29.08.2023 Aktif Dizin ve MS SQL veritabanı kullanıcı yetkilerinin gözden geçirilerek raporlandığı görülmüştür.		

VIII. KISALTMALAR

Kısaltma	Tanım
TBB	Türkiye Bankalar Birliği
RM	Risk Merkezi
RMY	Risk Merkezi Yönetimi
BS	Bilgi Sistemleri
BT	Bilgi Teknolojileri
FTP	File Transfer Protocol
IT	Information Technology
OSI	Open Systems Interconnection