SQL Change Guard

Ürün Özeti

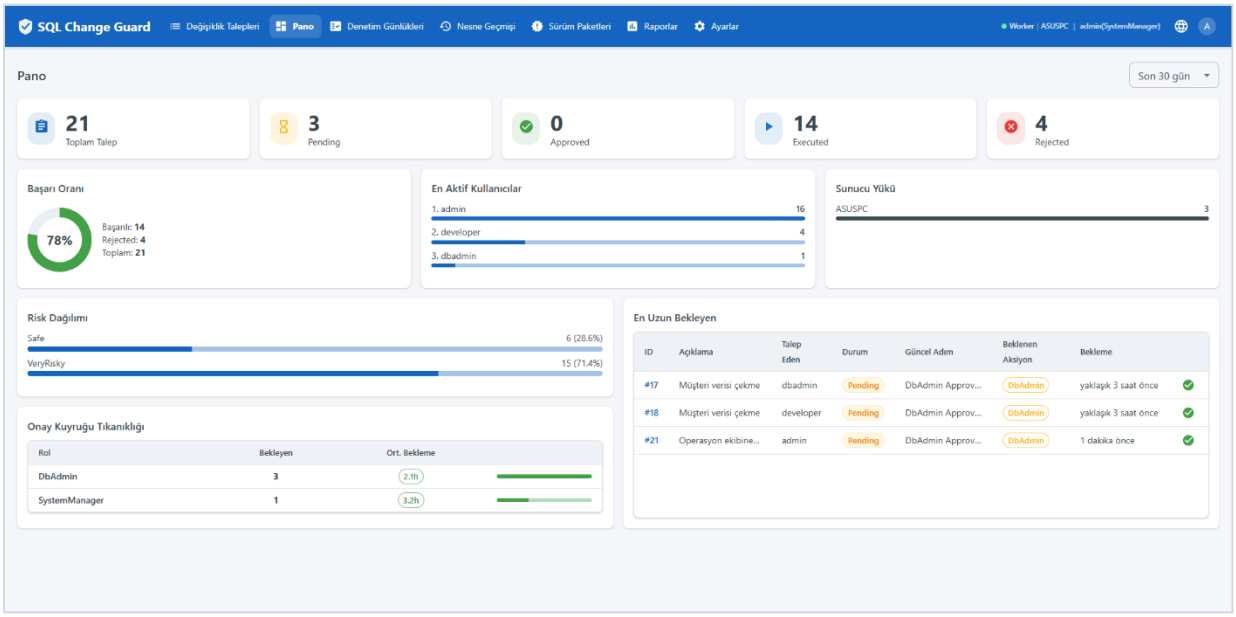
Veritabanı Operasyonları Yönetişim Platformu

SQL Server | PostgreSQL | Oracle

1. Yönetici Özeti

SQL Change Guard, veritabanı değişikliklerini, production veri erişimini ve uyumluluğu tek platformda yöneten bir Database Operations Governance çözümüdür. Sadece schema deployment aracı değildir; değişikliğin talepten dağıtıma, veri erişiminin talepten teslime kadar tüm yaşam döngüsünü policy tabanlı ve denetlenebilir kılar.

SQL Server, PostgreSQL ve Oracle için aynı yönetişim modelini sunar. Tamamen kurum içi (on-premise) çalışır; internet bağlantısı gerektirmez.



Kontrol Paneli

2. Çözülen Problem

Kurumlarda veritabanı operasyonları genellikle üç ayrı ve manuel yerde yürütülür: değişiklik dağıtımı, production veri talepleri ve denetim. Bu dağınıklık şu riskleri doğurur:

- Onaysız veya yanlış değişikliklerin production'a ulaşması
- WHERE koşulsuz UPDATE/DELETE gibi kritik hataların gözden kaçması
- Production'dan çıkan verinin kişisel bilgi içerip içermediğinin ve maskelenip maskelenmediğinin bilinmemesi
- Denetimde kim onayladı, kim çalıştırdı, kim veriyi aldı sorularının ispat edilememesi

3. Üç Yönetişim Katmanı

3.1 Database Change Governance

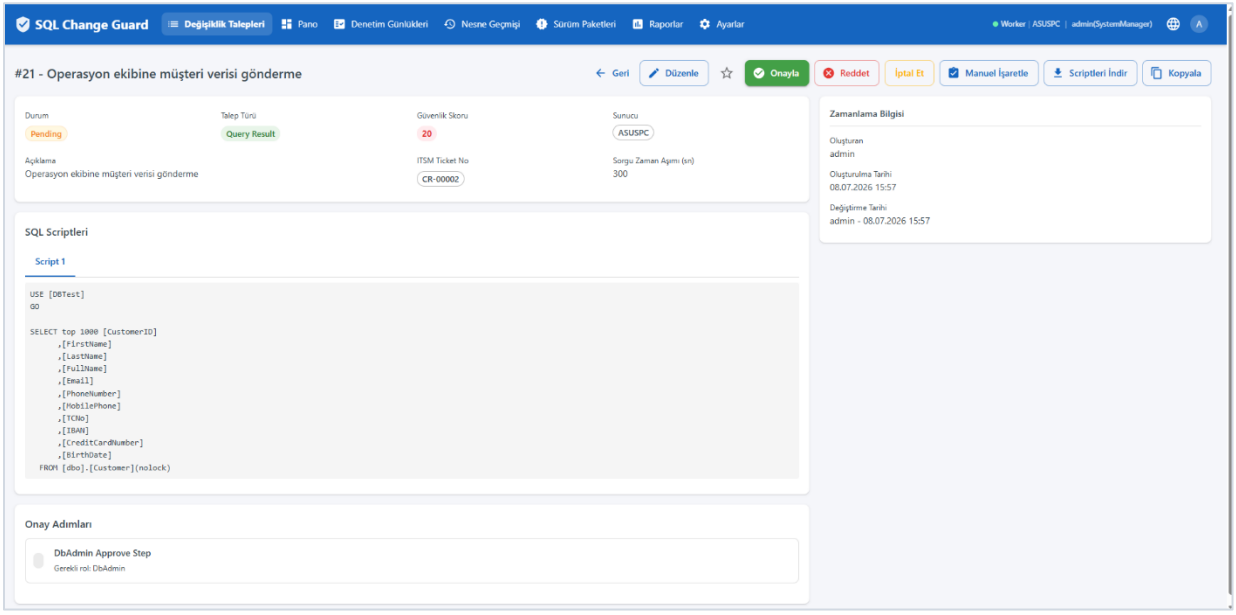
- Change Request: DDL/DML/DCL değişikliklerinin uçtan uca yaşam döngüsü

- Rol bazlı, çok adımlı ve policy tabanlı onay akışı
- Deployment öncesi 84+ SQL standart kuralı ile otomatik validasyon
- Her script için 0-100 arası otomatik risk skoru (Critical / High / Medium / Low)
- Sandbox doğrulama: canlıya geçmeden gerçek ortamda çalıştır ve geri al
- Release paketleri: birden çok değişikliği tek pakette sıralı ve bağımlılıklı dağıtım
- Otomatik rollback üretimi (Oracle örtülü-commit atomiklik güvencesi ile)
- Sürüm geçmişi ve nesne geçmişi (kim, ne zaman, hangi talep, hangi script)

3.2 Production Query Governance

SQL Change Guard'ı migration tabanlı araçlardan ayıran katman budur. Production'dan veri isteme süreci merkezi ve denetlenebilir hâle gelir.

- Sorgu (SELECT) talebi ve policy tabanlı onay akışı
- Kritik tablo ve kolon tespiti
- Hassas veri için otomatik maskeleme (TC, kart, IBAN, telefon doğrulamalı regex tespiti; tam maske veya kısmi maske)
- Maskesiz veri talebi için ayrı güvenlik onayı
- İlk kez kullanılan e-posta adreslerinin doğrulanması
- Sonuçların şifreli ZIP olarak teslimi, indirme gerekçesi ve indirme takibi
- Çoklu sunucuya sorgu ve Excel export

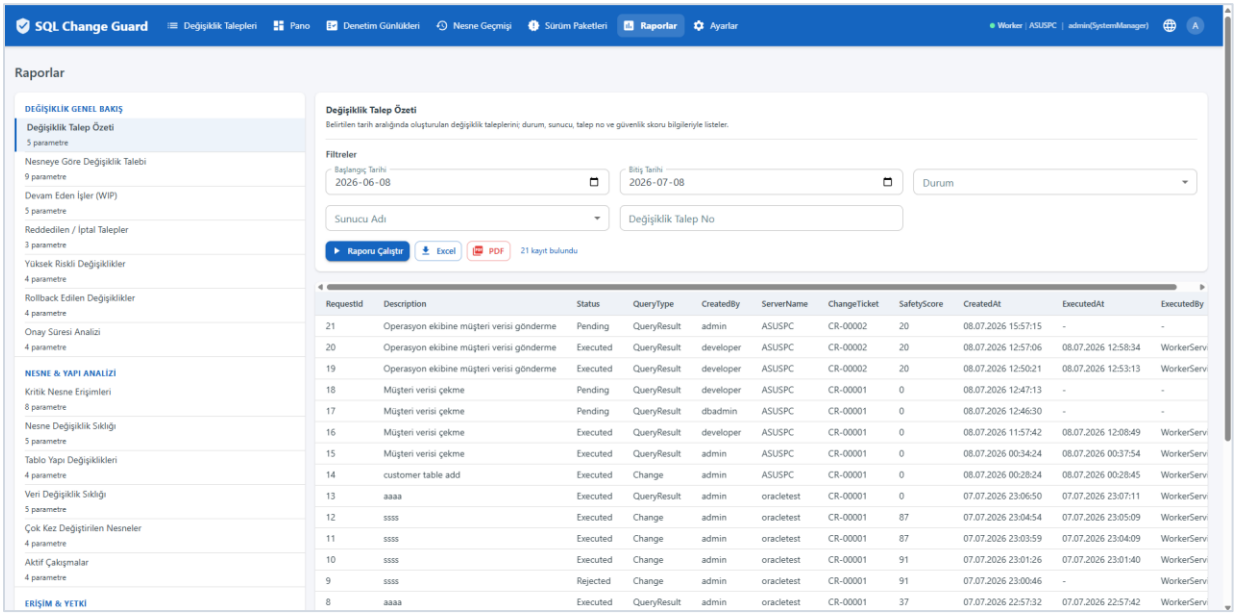


Sorgu Sonucu ve otomatik maskeleme

3.3 Compliance and Audit

- Hash zinciri ile korunan, değiştirilemeyen (immutable) audit kayıtları

- Onay, indirme ve çalıştırma geçmişi
- Denetim için kanıt paketleri
- Talep bazlı denetim dosyası: bir talebin tüm kanıtı (künye, görevler ayrılığı, onaylar, script parmak izi, risk skoru, çalıştırma ve denetim izi) tek tıkla mühürlü tek dosya olarak (PDF ve JSON) indirilir
- Kanıt bütünlüğü doğrulama: audit kayıtlarının kayıt anından beri değişmediği, ayrı bir immutable kopya ile karşılaştırılarak doğrulanır
- 30 hazır rapor: DML/DDL/DCL denetimi, kritik obje erişimi, hassas kolon dokunuşları, yetki hareketleri, ayrıcalıklı hesap işlemleri, QR maskeleme günlüğü ve daha fazlası
- KVKK, ISO 27001, COBIT ve ITIL gereksinimlerine uyum



Raporlar - 30 hazır rapor, Excel/PDF export

4. Policy Engine

Manuel karar yoktur; her şey politika ile yönetilir. Örnek bir production sorgu akışı:

- Production sorgu talebi gelir
- Kritik tablo içeriyorsa DB Admin onayı istenir
- Hassas kolon içeriyorsa veri otomatik maskelenir
- Maskesiz veri talep edilmişse ek güvenlik onayı devreye girer
- Sonuç şifreli teslim edilir ve tüm adımlar audit altına alınır

5. Moduller

Modül	İşlevi
Change Management	**DDL/DML/DCL taleplerinin uçtan uca yaşam döngüsü**
Otomatik Validasyon	**84+ SQL standart kuralı ile deployment öncesi kontrol**
Risk Skorlama	**Her script için 0-100 risk puanı ve sınıflandırma**
Sandbox Test	**Çalıştır ve geri al ile gerçek ortamda güvenli test**
Rollback	**Otomatik rollback üretimi, Oracle örtülü commit farkındalığı**
Release Package	**Bağımlılık yönetimi ve sıralı deployment**
Production Query Governance	**Production SELECT talepleri, policy ve maskeleme**
Hassas Veri Maskeleme	**Regex tabanlı tespit ve kolon bazlı maskeleme**
Policy Engine	**Kritik tablo ve hassas kolona göre çok seviyeli onay**
Raporlama	**30 hazır rapor, Excel/PDF export**

Object History	**Herhangi bir nesnenin tam değişiklik geçmişi**
Sunucu Yönetimi	**Çoklu SS/PG/Oracle sunucusunu tek yerden yönetme**

6. Roller ve Yetkilendirme

Tüm işlemler backend'de yetkilendirilir; UI kontrolü tek başına yeterli değildir. Roller: Viewer, Requester, Request Manager, DB Admin, Change Manager, System Manager. Görevler ayrılığı (separation of duties) desteklenir.

7. Neden SQL Change Guard?

- Tek platformda değişiklik, production veri erişimi ve uyumluluk
- SQL Server, PostgreSQL ve Oracle için aynı yönetişim modeli
- Production veri erişimi ve maskeleme katmanı ile migration araçlarından ayrışır
- Tamamen on-premise; kurum ağı dışına veri çıkmaz
- Bankacılık ve kurumsal denetime hazır audit altyapısı

Bir Platform. Database Change Governance + Production Query Governance + Compliance and Audit = Güvenli Veritabanı Operasyonları.

8. İletişim

- Web: www.sqlchangeguard.com
- E-posta: onur.egilmez@sqlchangeguard.com | info@sqlchangeguard.com
- Telefon: 0505 621 29 02
- LinkedIn: linkedin.com/company/sqlchangeguard

Hassas Veri Maskeleme: Doğrulamalı Tespit ve Sunucu Bazlı Rejim

Maskeleme iki bağımsız mekanizma ile çalışır ve ikisi birbirinin kör noktasını kapatır.

Birincisi sınıflandırma kataloğudur. Kolonun adına bakar, verinin içine hiç bakmaz. Örnek: adında TCKN geçen her kolon maskelenir. Bu mekanizma sayısal kolonları da kapsar; kimlik numarasını sayı olarak tutan sistemlerde tek koruma budur. Her kurala denetçiye gösterilen bir etiket atanır: KVKK-

Kimlik, KVKK-İletişim, KVKK-Sağlık, KVKK-Eğitim, PCI-Kart gibi. Kurulumla birlikte finans, perakende, sağlık ve eğitim alanlarını kapsayan hazır bir başlangıç seti gelir.

İkincisi veri desenleridir. Kolonun adına bakmaz, hücrelerin içeriğine bakar. Önemli olan tarafı şudur: bir desene doğrulama algoritması bağlanabilir. Kimlik numarası için checksum, kart numarası için Luhn, IBAN için mod-97. Böylece 11 haneli bir sipariş numarası boşa maskelenmez, gerçek kimlik numarası ise maskelenir. Bu, gereksiz maskesiz veri taleplerini ortadan kaldırır.

Kolon önizlemesi. Talep kaydedilirken sistem hedef sunucuya bağlanır ve sorgunun hangi kolonları döndüreceğini sorar. Sorgu çalıştırılmaz, tek satır veri okunmaz. Böylece talep sahibi ve onaylayan, teslimden önce hangi kolonun maskeleneceğini görür. Sorguda takma ad kullanılmış olsa bile kaynak kolon tespit edilir ve maskeleme atlanamaz.

Sunucu bazlı rejim. Maskeleme verinin özelliği olduğu için ayar sunucu tanımındadır. İki rejim vardır: tam maskeleme ve yalnız içerik. Yalnız içerik rejimi sentetik veri barındıran ortamlar içindir; kolon adına göre maskeleme yapmaz, ama o sunucuya gerçek veri yüklenirse doğrulamalı desenler devreye girer ve maskeleme kendiliğinden geri gelir. Bu rejim yazılı gerekçe olmadan seçilemez ve değişikliği denetim izine ayrı bir olay olarak yazılır. Aynı talep birden fazla sunucuya gidiyorsa kararlar sunucu bazında verilir: üretim sunucusundan gelen sonuç maskelenirken sentetik veri barındıran sunucudan gelen sonuç açık kalabilir.

Kanıt. Her teslimde hangi kolonun neden maskelendiği kolon bazında kaydedilir: sınıflandırma kataloğu, veri deseni, onaylı maskesiz istek ya da süre bütçesi aşımı. Kayıt sunucu bazındadır ve teslim anındaki rejim ile muafiyet gerekçesi kayda dondurulur; sunucu tanımı sonradan değiştirilse bile kanıt bozulmaz. Maskeleme kurumsal bir anahtarla tamamen kapatılabilir, ancak kapatıldığında da her teslim kayda geçer ve denetim dosyasında kırmızı hükümle işaretlenir.

Öğrenme döngüsü. Desenle yakalanan ama katalogda olmayan kolonlar aday olarak birikir; veritabanı yöneticisi bunları kalıcı kural haline getirir ya da yok sayar. Aday listesinde hiçbir veri değeri tutulmaz, yalnızca kolon, tablo ve desen adları vardır. Böylece sınıflandırma, kimse üretim verisine bakmadan zamanla keskinleşir.

Kanıt: O Gün Hangi Kurallar Geçerliydi

Kurallar zamanla değişir. Bir ayar bugün sıkı, altı ay önce gevşek olabilir. Denetimde sorulan soru şudur: bu talep işlendiği gün hangi kurallara tabiydi? Sistem bu soruyu bugünkü ayarlara bakarak değil, o gün dondurulmuş kayda bakarak cevaplar.

Kural seti anlık görüntüsü. Her talep kaydedildiğinde o anda geçerli olan kural seti tek bir denetim kaydına yazılır: hedef sunucuların künyesi ve kontrol bayrakları (rollback zorunluluğu, otomatik çalıştırma, maskeleme rejimi), onay ve görevler ayrılığı kuralları, hassas veri maskeleme ayarları, sonuç dosyası erişim kuralları, o gün bloklayıcı olan SQL standartlarının listesi ve açık olan lisans modülleri. Kural sonradan değişse bile bu kayıt değişmez.

Teslim anındaki ayarlar. Bir talep bir tarihte kaydedilip başka bir tarihte çalıştırılabilir. Maskeleme çalıştırma anında yapıldığı için, o andaki eşik, örneklem boyutu, örnekleme biçimi ve süre bütçesi de teslim kaydına ayrıca dondurulur. Böylece bir teslimde neden hiçbir kolonun maskelenmediği sorusu kesin olarak cevaplanır.

Kontrol değişiklikleri ayrı olay olarak kaydedilir. Bir ayarın değişmesi ile bir kontrolün gevşetilmesi aynı şey değildir. Maskeleme rejiminin gevşetilmesi, rollback zorunluluğunun kaldırılması, otomatik çalıştırmanın açılması, bir tespit deseninin kapatılması, bir sınıflandırma kuralının silinmesi, alıcı havuzuna adres eklenmesi, bakım görevinin durdurulması ve lisans modüllerinin değişmesi kendi olay adlarıyla yazılır. Gevşetme ve sıkılaştırma farklı adlar alır. Denetim ekranında olay adına göre arama yapılabilir; böylece hangi kontrolün ne zaman ve kim tarafından gevşetildiği tek listede görülür.

İki bağımsız kayıt katmanı. Uygulama denetim izi iş anlamı taşıyan olayları tutar ve ekranda görünür. Veritabanı seviyesindeki ikinci katman ise uygulamadan bağımsız çalışır: yönetim aracıyla doğrudan veritabanına yapılan bir değişiklik de yakalanır. İki katman birbirinin yerine geçmez, biri diğerini tamamlar.

Denetim dosyasında görünür. Talep bazlı denetim dosyası, o talebin işlendiği gün geçerli olan kural setini ayrı bir bölümde okunur biçimde listeler. Denetçi tek bir belgeyle hem ne olduğunu hem hangi kurallara göre olduğunu görür.

Sürüm paketi kapsamı. Sürüm paketleri yalnızca değişiklik taleplerini taşır. Sorgu sonucu talepleri paket içinde yer alamaz; sonuç dosyası ancak hassas veri maskelemesi uygulayan ve denetim kaydı üreten kendi akışında teslim edilir. Bu kural yalnızca ekranda değil, arayüzden bağımsız olarak sunucu tarafında da doğrulanır.

Ayar Değişikliklerinde Dört Göz İlkesi

Bir kontrolü zayıflatan ayar değişikliği tek kişinin kararıyla yapılmamalıdır. Sistem, ayar ekranlarındaki değişiklikleri onaya bağlayabilir: değişiklik hemen uygulanmaz, önce onay bekler ve onaylanana kadar eski değer geçerli kalır.

Nasıl çalışır. Onay bekleyen değişiklik ayrı bir kayıtta durur; gerçek ayar tablosuna onay verilene kadar dokunulmaz. Bu sayede sistemin geri kalanı eski değeri okumaya devam eder ve yarım uygulanmış bir ayar durumu hiç oluşmaz. Onay verildiğinde değişiklik, kullanıcı kaydetmiş gibi aynı yoldan uygulanır; lisans limiti, doğrulama ve eşzamanlılık kontrolleri o anda yeniden çalışır.

Onay yetkisi. Bir ayar değişikliğini, o ekranın yetkisine sahip başka bir kullanıcı onaylar. Ayrı bir onaylayan rolü tanımlanmaz; yetkiler zaten rol tanımında vardır. Kimse kendi talep ettiği değişikliği onaylayamaz veya reddedemez; bu kural isteğe bağlı değildir. Onay listesi kullanıcının yetkisine göre filtrelenir: kişi yalnızca yetkili olduğu ekranların onaylarını görür.

Kapsam. Özellik kurumsal bir parametre ile yönetilir ve üç seçeneği vardır: kapalı, yalnızca kontrol ayarları, tüm ayarlar. Varsayılan kapalıdır. Yalnızca kontrol ayarları seçeneğinde sunucu tanımları, kullanıcı kayıtları, rol yetki matrisi, onay politikaları, SQL standartları, kritik obje listesi, hassas kolon kataloğu, hassas veri desenleri, onaylı e-posta adresleri, bakım işleri ve maskeleme, onay, görevler ayrılığı gibi kontrol parametreleri onaya düşer; işletme verisi niteliğindeki ayarlar akışı yavaşlatmaz. Özelliğin kendisi de bir kontroldür: açmak anında uygulanır, kapatmak onay ister. Parola sıfırlama ve kullanıcı kilidi açma bilinçli olarak kapsam dışıdır; bunlar yardım masası işlemleridir ve denetim kaydına yazılır.

Ekranda görünüm. Onay bekleyen değişikliği olan kayıt, ilgili ayar ekranında işaretlenir ve yeniden düzenlenemez; ekranın üstünde kaç değişikliğin beklediğini gösteren bir uyarı bulunur. Kaydetme

sonrası kullanıcıya değişikliğin uygulanmadığı, onaya gönderildiği açıkça bildirilir. Ayrı bir onay ekranında eski ve yeni değer yan yana gösterilir, değişen alanlar vurgulanır.

Kayıt. Talebin açılması, onaylanması, reddedilmesi ve onaylandığı halde uygulanamaması ayrı denetim olayları olarak yazılır. Onay anında değişikliğin kendi denetim kaydı da oluşur, böylece kimin onayladığı ile değerin ne olduğu ayrı ayrı izlenebilir. Reddetme gerekçe ister.

Kurulum notu. Kimse kendi talebini onaylayamadığı için, kapsamdaki her ekran yetkisine sahip en az iki kullanıcı bulunmalıdır. Uygulamada bu tek şarta iner: en az iki sistem yöneticisi kullanıcı tanımlı olmalıdır.

Denetçi Rolü

Denetim ekiplerinin ihtiyacı çoğu zaman tek bir şeydir: görmek. Kim ne yaptı, hangi onaydan geçti, hangi veri kime gitti. Bunun için sisteme yönetici yetkisi vermek gerekmez. SQL Change Guard bu ihtiyacı ayrı bir rolle karşılar.

Denetçi ne yapar. Tüm talepleri görür, denetim kayıtlarını inceler, raporları ve kontrol panelini kullanır, bir talebin kanıt dosyasını üretip indirir, denetim izinin bütünlüğünü doğrular ve bildirim günlüklerini görür.

Denetçi ne yapamaz. Talep açamaz, onaylayamaz, çalıştıramaz, sandbox kullanamaz, hiçbir ayar ekranını yönetemez ve sorgu sonucu dosyasını indiremez.

Son madde bilinçli bir tasarımdır. Kanıt paketine sorgu sonucu verisi girmez; denetçi kanıta ulaşır, üretim verisine ulaşmaz. Denetim yapabilmek için kişisel veri görmek gerekmediği için bu sınır denetimi zayıflatmaz, aksine kurumun veri yüzeyini daraltır.

Kanıt ekleme ve silme yoktur. Kanıt dosyası talebin kendisinden üretilir; düzenlenebilen bir kanıt deposu bulunmaz. Denetçinin kanıt ekleyip silebilmesi, kanıtın kanıt olma değerini ortadan kaldırırdı.

Görevler ayrılığı. Denetçi onay adımlarında onaylayan olarak seçilemez ve denetçi rolüne onaylama ya da çalıştırma yetkisi verilemez. Denetleyen kişinin onaylayan konumuna geçmesi kontrolün kendisini ortadan kaldırır, bu yüzden kural isteğe bağlı değildir.

Kurulum notu. Ürün tek yönetici hesabıyla gelir; hazır bir denetçi hesabı gönderilmez. Kurum kendi denetçisini kendi tanımlar, böylece parolası bilinen bir denetim hesabı hiçbir kurulumda bulunmaz.