SQL Change Guard

Uyumluluk ve KVKK

Denetim, Kanıt ve Veri Koruma

KVKK | ISO 27001 | COBIT | ITIL

1. Yaklaşım

SQL Change Guard, veritabanı değişikliklerini ve production veri erişimini denetlenebilir bir sürece dönüştürür. Her işlem bir denetim kanıtına dönüşür; bu da düzenleyici gereksinimleri karşılamayı kolaylaştırır.

2. KVKK ve Kişisel Veri Koruma

- Hassas veri tespiti: TC kimlik, kart numarası, IBAN, telefon gibi desenler regex ve doğrulama algoritmalarıyla (checksum, Luhn, mod-97) yakalanır
- Otomatik maskeleme: hassas kolonlar tam maske veya kısmi maske ile maskelenir
- Maskesiz veri için ek onay: maskesiz talep ayrı güvenlik onayı gerektirir
- Şifreli teslim: sorgu sonuçları şifreli ZIP olarak paylaşılır
- İzlenebilirlik: kim, hangi veriyi, hangi gerekçeyle aldı kaydı tutulur (veri işleme kanıtı)
- On-premise: kişisel veri kurum ağı dışına çıkmaz

3. Denetim İzi (Audit Trail)

- DML denetim izi: INSERT/UPDATE/DELETE işlemlerinin tarih, kullanıcı ve ortam kaydı
- DDL denetim izi: CREATE/ALTER/DROP işlemlerinin nesne geçmişiyle izlenmesi
- DCL/yetki değişiklikleri: GRANT, REVOKE, CREATE/DROP USER işlemlerinin eksiksiz kaydı
- Onay kanıtı: her işlem için onaylayan, tarih ve zaman damgalı kayıt
- Değiştirilemeyen loglar: hash zinciri ile korunan, silinemeyen audit
- Kanıt bütünlüğü doğrulama: audit kayıtları ayrı bir immutable kopya ile karşılaştırılarak, kayıt anından beri değişmediği tek tıkla doğrulanabilir

4. Standart Eşlemesi

Standart / Gereksinim	SQL Change Guard Katkısı
KVKK	**Hassas veri maskeleme, erişim onayı, işleme kaydı, şifreli teslim**
ISO 27001	**Erişim kontrolü, değişiklik yönetimi, denetim kaydı, görevler ayrılığı**
COBIT	**Değişiklik yönetişimi, onay akışları, kanıtlanabilir kontroller**

ITIL	**Change management süreci, release yönetimi, kayıt altına alma**
BDDK / Bankacılık	**Kim neye erişti, kim onayladı, kim çalıştırdı kanıtı**

5. Denetim Kanıt Paketi

Bir değişikliğin veya veri erişiminin tüm yaşam döngüsü tek bir kanıt paketinde toplanabilir: talep, parse sonuçları, risk skoru, onaylar, çalıştırma logu, rollback ve audit kayıtları. 30 hazır rapor Excel ve PDF olarak denetçiye sunulabilir.

Ayrıca herhangi bir talebin tüm yaşam döngüsü, tek tıkla mühürlü tek bir denetim dosyası (PDF ve JSON) olarak indirilebilir. Dosya bir paket mührü (SHA-256) taşır ve üretildikten sonra değişmediği sistem üzerinden doğrulanabilir. Bu dosyayı indirme yetkisi ayrı bir izinle yönetilir ve indirme işleminin kendisi de audit altına alınır.

Görevler ayrılığı sonucu dört durumda raporlanır: sağlandı, zorunlu tutulmadı, ihlal edildi, değerlendirilemez. Hiç onay adımı oluşmamış bir talep için sağlandı denmez. Denetim dosyası ayrıca çalıştırmayı başlatan kişiyi worker servisinden ayrı olarak gösterir ve talebin hangi kural setiyle geçtiğini kontrol ortamı bölümünde listeler. Böylece gevşek yapılandırılmış bir kurumda da belge gerçeği söyler.

Onay akışını atlayabilecek yollar kapatılmıştır: sürüm paketleri yalnızca onaylanmış talep kabul eder ve çalıştırma anında her talep için onay durumu ile görevler ayrılığı yeniden doğrulanır, elle uygulandı işareti talep sahibi kısıtına tabidir, acil durum ilanı asgari rol yetkisi gerektirir. Bu üç yol denetimde en sık sorgulanan atlatma senaryolarıdır.

Risk bandı ve uygulanan politika: Denetim dosyası, talebin risk bandını ve bandı belirleyen kuralı, atlanamaz bir standardın tetiklenip tetiklenmediğini ve talebe uygulanan onay politikasının adını içerir. Eşleşen politika yoksa bu durum da kayda geçer. Böylece bir talebin neden onay istemediği sonradan kanıtlanabilir.

6. Uyumluluk Raporları (Örnekler)

- Kritik obje erişimi ve hassas kolon dokunuşları
- Manuel veri değişiklikleri ve WHERE koşulsuz işlem tespiti
- DB yetki hareketleri, ayrıcalıklı hesap işlemleri, kullanıcı yetki matrisi
- QR maskeleme günlüğü ve sorgu sonucu aktivitesi

7. Sorumluluk Reddi

SQL Change Guard uyumluluk süreçlerini destekleyen bir kontrol ve kanıt altyapısı sağlar. Nihai uyumluluk sorumluluğu kurumun politikaları ve uygulamasıyla birlikte değerlendirilmelidir.

Şifreleme ve Anahtar Yönetimi

SQL Change Guard hassas verileri üç ayrı kategoride, amacına uygun kriptografik yöntemlerle korur. Geri döndürülmesi gerekmeyen sırlar tek yönlü özetlenir (hash); uygulamanın çalışması için geri açılması gereken sırlar ise kimlik doğrulamalı şifreleme ile saklanır. Böylece her veri, ihtiyacına en uygun ve endüstri standardı yöntemle korunur.

1. Kullanıcı parolaları- BCrypt (tek yönlü hash)

Kullanıcı parolaları BCrypt algoritmasıyla (iş faktörü 12 ve kayıt başına rastgele salt) özetlenerek saklanır. Bu tek yönlü bir işlemdir: parolanın açık hali hiçbir yerde tutulmaz ve geri elde edilemez. Kimlik doğrulama, girilen parolanın yeniden özetlenip saklanan özetle karşılaştırılmasıyla yapılır. Veritabanı ele geçirilse dahi parolalar geri döndürülemez.

2. Sunucu veritabanı parolaları- AES-256-GCM (şifreleme)

Hedef veritabanlarına bağlanmak için kullanılan parolalar (Servers.SqlPassword) at-rest olarak AES-256-GCM kimlik doğrulamalı şifreleme ile saklanır. GCM modu hem gizlilik hem de bütünlük sağlar: her kayıt rastgele bir nonce ve doğrulama etiketi (tag) içerir, kurcalanan veri çözülemez. Uygulama, hedef veritabanına bağlanırken parolayı yalnızca bellekte, kısa süreliğine çözer.

3. QR paket zip parolaları- AES-256-GCM (şifreleme)

Sorgu sonucu (QueryResult) paketlerinin parola korumalı zip dosyaları için üretilen parolalar da sunucu parolalarıyla tamamen aynı ilkeyle, AES-256-GCM ile şifrelenerek saklanır. Böylece geri döndürülebilir tüm sırlar tek, doğrulanabilir bir kriptografik yöntem kullanır; bu da hem güvenliği hem de sistemin anlaşılırlığını artırır.

Denetim izi bütünlüğü- HMAC-SHA256

Denetim kayıtları (audit trail) bir hash zinciriyle korunur ve güncel sürüm HMAC-SHA256 kullanır. Anahtar veritabanında tutulmaz, yalnızca uygulama yapılandırmasından gelir; böylece yalnızca veritabanına erişimi olan bir kişi bile denetim zincirini yeniden üretip geçmişi sessizce değiştiremez.

Anahtar yönetimi

Tüm şifreleme anahtarları 256-bit uzunluğundadır (32 bayt, base64) ve uygulama yapılandırmasının Security bölümünde toplanır: Security:ServerPasswordKey (sunucu parolaları), Security:QrZipPasswordKey (QR zip parolaları) ve Audit:HmacKey (denetim izi). Anahtarlar üretim ortamında user-secrets veya ortam değişkeni (environment variable) üzerinden sağlanır; kaynak koda veya veritabanına gömülmez.

Özet: Kullanıcı parolası tek yönlü hash (BCrypt) ile; sunucu ve QR zip parolaları çift yönlü şifreleme (AES-256-GCM) ile; denetim izi ise HMAC-SHA256 ile korunur.

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.

Ayar Onaylarında Kim Ne Yaptı

Dört göz kuralı açıkken bir ayar değişikliğini bir kişi ister, aynı yetkiye sahip başka bir kişi onaylar. Bu iki ismin de kayıt üzerinde görünmesi gerekir; aksi halde denetim sırasında bu ayarı kim değiştirdi sorusunun tek bir cevabı olur ve o cevap eksik kalır.

Son değişiklik sütunu. Dört göz kapsamındaki tüm ayar ekranlarında yeni bir sütun vardır. Üst satırda kaydı değiştiren kişi ve zamanı yazar. Altındaki yeşil rozette onaylayan kişi görünür. Rozet varken üst satır Değiştiren etiketiyle çıkar, rozet yokken tek isim yazar. Hücrenin üzerine gelindiğinde oluşturan, değiştiren ve onaylayan üç satır halinde okunur.

Kayda kimin adı yazılır. Onay verildiğinde değişiklik uygulanır ve kaydın üzerine değişikliği isteyen kişinin adı yazılır. Onaylayan kişinin adı ayar onayı kaydında ve denetim izinde durur. Böylece bir satıra bakan kişi hem değişikliği isteyeni hem onaylayanı görebilir.

Denetim izinde iki ayrı kayıt oluşur. Biri değişikliğin kendisidir ve değişikliği isteyenin adını taşır. Diğeri onay kaydıdır ve onaylayanın adını, saatini ve IP adresini taşır. Onay anındaki IP adresi onaylayana aittir, bu yüzden isteyenin kaydına yazılmaz; yanlış bilgi taşıyan tek bir satır bile denetim izinin değerini düşürür.

Kural kapalıyken ne olur. Dört göz kuralı kapalıyken onaylayan diye biri yoktur. Kaydı değiştiren tek kişi vardır, sütunda tek isim görünür ve onay rozeti çıkmaz. Kural açıkken yapılmış eski bir onay, kayıt sonradan doğrudan değiştirildiyse artık gösterilmez; çünkü o onay kaydın bu halini kapsamaz.

Yenile düğmesi. Onayı başka bir kullanıcı verdiği için ekrandaki liste her an eskiyebilir. Ayarlar sayfasının sağ üst köşesindeki yenile düğmesi açık olan sekmenin verisini tazeler. Onay ekranında bir karar verildiğinde ilgili ekranlar da kendiliğinden tazelenir.

Ayar onayları sekmesi. Bu sekme yalnızca dört göz kapsamındaki bir ekranın yetkisine sahip kullanıcıya görünür. Yalnızca izleme yetkisi olan kullanıcılar için sekme gösterilmez, çünkü onlara filtrelenmiş liste zaten boş dönerdi.

Saatler Nasıl Gösterilir

Sistemdeki her zaman değeri evrensel saatte (UTC) saklanır. Yerel saat bir veri özelliği değil, bir gösterim tercihidir. Bu ayrım sayesinde farklı şehirlerdeki iki kullanıcı aynı olaya baktığında aynı anı görür, yalnızca ekrandaki yazı kendi saatlerine göre değişir.

Ekranda. Tarih ve saatler tarayıcınızın saat dilimine göre gösterilir. Ayrı bir ayar yapmanız gerekmez.

Belgelerde. PDF, Excel ve e-posta sunucuda üretilir; orada tarayıcı olmadığı için gösterim saat dilimi kurulum ayarından okunur ve belgenin üzerine yazılır. Böylece belgeyi okuyan kişi saatin neye göre olduğunu tahmin etmek zorunda kalmaz. Bu seçim bilinçlidir: saat dilimi belgeyi isteyen kişinin tarayıcısına bağlı olsaydı, aynı talebin kanıt dosyası iki denetçide iki farklı belge üretirdi.

Tarih filtrelerinde. Bir tarih aralığı seçtiğinizde gün sizin yerel gününüzdür. Başlangıç günü saat 00.00'dan, bitiş günü ise gün sonuna kadar dahildir.

Denetim izinde. Denetim kayıtları saniye ayrıntısıyla gösterilir; aynı dakika içinde gerçekleşen iki olayın sırası böylece okunabilir.