Yıllık KVKK Teknik Sağlık Kontrolü & Internal Audit Checklist Şablonu — Yazılım / Internal Audit (v1.0)

Asset Amaç: Bu asset; KVKK teknik tedbirlerini bir defalık kurulum olmaktan çıkarıp "sürekli işletilen bir süreç" haline getirmek amacıyla yıllık ve 6 aylık iç denetim (*internal audit*) döngüleri ve kontrol listeleri sunar. Otomatik sistem taramalarını (zafiyet, konfigürasyon, log izleme) manuel kontrollerle (rol ve kullanıcı listeleri, script envanteri, yedekleme testleri) aynı operasyonel rutinde birleştirir. Denetimlerde tespit edilen bulguların açıkta kalmasını engelleyerek takip (*follow-up*) planıyla kapatılmasını ve yasal kanıt üretimini standartlaştırır. Otel ve B2B altyapılarında teknik uyumu sürekli canlı tutmayı hedefler.

Kim Kullanır?: IT / BT Yöneticileri, KVKK / Uyum Sorumluları ve Sistem Owner'ları (Otel ve B2B).

Nasıl Kullanılır?

1. Denetim kapsamındaki sistemleri belirleyip denetim frekansını (Yıllık, 6 Aylık, Aylık) ve kontrol alanlarını seçin.
2. Her bir kontrol maddesi için kurum içinden bir sorumlusu (*owner*) ve kabul edilebilir kanıt formatını (ekran görüntüsü, log kaydı, değişiklik kaydı) atayın.
3. Denetim bulgularını önceliklendirip (*P1/P2/P3*) biletleme (*ticket*) sistemine aktarın; kapanış kanıtı doğrulaması ile yönetim raporunu üretin.

CHECKLIST & SPRINT PLAN — Yıllık KVKK Teknik Sağlık Kontrolü & Internal Audit

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Yıllık Audit Tarihi Belirlendi:** Ana KVKK teknik denetiminin yapılacağı tarih takvime işlendi.
- [ ] **6 Aylık Ara Audit Planlandı:** Sistem değişikliklerini ve yeni entegrasyonları kapsayan ara kontrol tarihi netleştirildi.
- [ ] **Otomatik Taramalar (Vuln/Config) Planlı:** Zafiyet taraması (*vulnerability scan*) ve konfigürasyon denetim araçları otomatize edildi.
- [ ] **Rol / Kullanıcı Listesi Review Süreci Var:** Aktif, pasif ve yetkisi değiştirilmiş kullanıcı/personel hesapları gözden geçirildi.
- [ ] **Admin MFA ve Erişim Kısıtları Kontrol Ediliyor:** Yönetici panellerinde Çok Faktörlü Doğrulama (MFA) ve IP kısıtlamaları doğrulandı.
- [ ] **Log Heartbeat Testi Var:** Kritik veritabanı ve sunuculardan merkezi log sistemine veri akışının kesintisiz sürdüğü doğrulandı.
- [ ] **Export İşlemleri ve Audit Log Kontrolü Var:** Veri dışa aktarma (Excel/CSV) hareketleri ve yetkisiz aktarım logları incelendi.
- [ ] **Script / Tag Envanteri Kontrol Ediliyor:** Web sitelerindeki ve uygulamalardaki üçüncü taraf script'ler ve Rıza/Consent tetikleyicileri test edildi.
- [ ] **Backup / Snapshot Şifreli ve Retention'a Uygun:** Tüm yedeklerin AES-256 ile şifrelendiği ve veri saklama politikasına uygun olduğu teyit edildi.

- [ ] **Restore Testi Periyodik Yapılıyor:** Şifrelenmiş yedeklerin geri yükleme (restore) provaları gerçekleştirildi ve raporlandı.
- [ ] **Vendor Erişimleri Yılda 1 Gözden Geçiriliyor:** Dış tedarikçilere verilen API, VPN ve panel erişimlerinin güncelliği kontrol edildi.
- [ ] **Bulgular İçin Triage (P1/P2/P3) Var:** Tespit edilen zafiyet ve eksiklikler risk derecesine göre sınıflandırıldı.
- [ ] **Her Bulgu İçin Owner + Due Date Var:** Her bir bulgu için bir sorumlu atandı ve kapatma süresi tanımlandı.
- [ ] **Kapanış Kanıtı Zorunlu:** Bulguların kapatılmış sayılması için log kaydı, ekran görüntüsü veya değişiklik kaydı (*change record*) şart koşuldu.

2) Problem → Kök Neden→ Çözüm Tablosu

Problem	**Kök Neden**	**Çözüm (Internal Audit Standardı)**
Audit Yapılıyor Ama Bulgular Kapanmıyor	Takip (*Follow-up*) planının ve sorumluluk atamasının olmaması	**Owner + Due Date + Kapanış Kanıtı Zorunluluğu**
Backup Var Ama Restore Hiç Test Edilmemiş	Düzenli restore test takviminin ve prova prosedürünün bulunmaması	**Çeyreklik Restore Provası + Restore Raporu**
Script/Tag'ler Kontrolsüz Çoğalıyor	Web/Uygulama script envanterinin ve temizlik rutininin olmaması	**Yıllık Script Audit + Consent Tetikleme Testleri**

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14) — "Audit Kurulum Sprint'i"

[Gün 1–4: Kapsam, Owner & Otomasyon] ——> [Gün 5–8: Log, Backup & Script Kontrolleri] ——> [Gün 9–11: Vendor & Triage Kurgusu] ——> [Gün 12–14: Dry Run & Takvimleme]

- **Gün 1:** Denetim kapsamının ve kapsama girecek sistem/sunucu listesinin netleştirilmesi.
- **Gün 2:** Kontrol alanlarının belirlenmesi ve her alan için kurum içi sorumlu (*owner*) atamalarının yapılması.
- **Gün 3:** Otomatik tarama (zafiyet ve konfigürasyon) araçlarının yapılandırılması ve tarama takviminin oluşturulması.
- **Gün 4:** Kullanıcı rolleri, pasif hesaplar ve Admin MFA durumlarını içeren ilk kontrol raporunun çıkarılması.

- **Gün 5:** Kritik sistemlerin merkezi log sunucusuna kesintisiz akışını doğrulayan Log Heartbeat test kurgusunun kurulması.
- **Gün 6:** Veritabanı ve dosya sunucusu yedeklerinin şifreleme (At-Rest) ve saklama (*retention*) kurallarına uygunluğunun denetlenmesi.
- **Gün 7:** Şifreli yedekler üzerinden uygulamalı geri yükleme (*restore*) test planının hazırlanması ve yürütülmesi.
- **Gün 8:** Web ve mobil platformlardaki script/tag envanterinin çıkarılması ve Rıza (Consent) mekanizması tetikleme testlerinin yapılması.
- **Gün 9:** Üçüncü taraf tedarikçi (*vendor*) erişim listelerinin, API token'larının ve yetkilerinin gözden geçirilmesi.
- **Gün 10:** Denetim bulguları için risk önceliklendirme kural setinin (*P1 / P2 / P3 Triage*) tanımlanması.
- **Gün 11:** Biletleme (*ticket*) sisteminde denetim bulgusu şablonunun ve kapanış kanıt standartlarının oluşturulması.
- **Gün 12:** İlk Mini-Audit (*Dry Run*) simülasyonunun gerçekleştirilmesi ve süreç aksaklıklarının tespiti.
- **Gün 13:** Dry Run sırasında tespit edilen operasyonel eksikliklerin giderilmesi.
- **Gün 14:** Audit döngüsünün resmi olarak yayımlanması, yönetim sunumu ve 365 günlük denetim takviminin devreye alınması.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
Açık Kritik Bulgu Sayısı (P1)	Belirsiz / Yüksek	0 (Tüm P1'ler KAPALI)	**Hedef ↓ (Düşüş)**
Ortalama Bulgu Kapanış Süresi	60+ Gün / Takipsiz	< 14 Gün (P1 için < 48 Saat)	**Hedef ↓ (Hızlanma)**
Log Heartbeat Başarı Oranı (%)	%60 (Sık kesinti)	%99.9 (Kesintisiz akış)	**Hedef ↑ (Yükselme)**
Backup Restore Başarı Oranı (%)	Test Edilmedi	%100 (Doğrulanmış restore)	**Hedef ↑ (Yükselme)**

Atıl / Yetkisi Fazla Admin Sayısı	Yüksek	Minimum Yetki (*Least Privilege*)	**Hedef ↓ (Düşüş)**

Deliverables (Teslim Edilecek Çıktılar)

- **Yıllık / 6 Aylık Internal Audit Timeline:** Periyodik kontrol ve tarama tarihlerini gösteren denetim takvimi.
- **Internal Audit Checklist (v1.0):** Teknik tedbirlerin tamamını kapsayan uygulamalı kontrol listesi.
- **Ticket Şablonu & Kanıt Standardı Rehberi:** Bulguların takibi, önceliklendirilmesi ve doğrulama kanıtı gereksinimleri dokümanı.
- **İlk Audit Raporu & Follow-Up Backlog:** Yürütülen ilk denetimin sonuçları ve açık bulguların kapanış takip listesi.
- **365 Günlük Refresh Planı:** Yıllık teknik sağlık kontrolü sürecinin periyodik yenileme ve iyileştirme prosedürü.

[Checklist / Framework Card]

IT yöneticileri, KVKK uyum liderleri ve sistem owner'ları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Internal Audit Checklist Kartı. Koyu karbon gri zemin üzerine yerleştirilmiş; denetim büyüteci, kilitli onay rozeti, otomasyon çarkı ve zamanlayıcı takvim simgesi. Kartın üzerinde; "Periodic Internal Audit Schedule: Annual & Semi-Annual Runs", "Automated Scans: Vulnerability, Config & Log Heartbeat Checks", "Access & Role Review: Admin MFA & Least Privilege Verification", ve "Closed-Loop Follow-Up: Owner Assignment, Triage & Evidence Standards" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.

[Diagram / Flow]

365 günlük bir iç denetim yaşam döngüsünü kapsayan, 16:9 formatında yüksek çözünürlüklü bir Audit Timeline & Workflow Diyagramı. Koyu şık zemin üzerinde; Yıllık Ana Audit, 6 Aylık Ara Kontrol, Çeyreklik Restore Provaları ve Aylık Log/MFA Taramalarını gösteren dairesel ve çizimsel zaman akışı. Bulguların tespitinden P1/P2/P3 Triage aşamasına, biletleme sistemine aktarılmasına, kanıt doğrulamasına ve kapanış onayına kadar uzanan adım adım takip mimarisi profesyonel bir şema olarak sergileniyor.