Felaket Kurtarma Planı & Yedekleme Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset, Felaket Kurtarma (Disaster Recovery - DR) ve yedekleme stratejisini *"Yedek var ama geri dönmüyor"* belirsizliğinden çıkarıp RPO/RTO hedefleriyle somut olarak ölçülen, offsite (fiziksel/ağ bazında ayrıştırılmış) mimariyle korunan ve düzenli tatbikatlarla doğrulanan bir operasyonel modele dönüştürür. Tier bazlı önceliklendirme yaparak olası bir kriz anında kritik sistemlerin en kısa sürede ayağa kaldırılmasını sağlar. Restore, failover ve rollback testlerini 14 günlük eksiksiz bir uygulama sprint planına bağlar.

Kim Kullanır?: BT/DevOps Ekipleri, Sistem Yöneticileri, Otel Operasyon Liderleri (Kritik PMS/Web sistem sahipleri) ve B2B Portal/CRM Ekipleri.

Nasıl Kullanılır?

1. Kurum bünyesindeki sistemleri kritiklik derecesine göre sınıflandırın (Tier-1: PMS/Web/Rezervasyon, Tier-2: CRM/ERP, Tier-3: Analitik/Arşiv) ve her katman için RPO/RTO hedeflerini tanımlayın.
2. Yedekleme türlerini (Full, Incremental, Snapshot) ve offsite topolojisini (fiziksel ayrık lokasyon, farklı cloud hesabı) belirleyerek erişim ve yetkilendirme politikasını kilitleyin.
3. Restore, failover ve rollback tatbikatlarını 14 günlük uygulama sprint planında çalıştırın, çıkan darboğazları raporlayarak sürekli iyileştirme backlog'una işleyin.

CHECKLIST & SPRINT PLAN — Felaket Kurtarma Planı ve Yedekleme Şablonu

A) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Tier Sınıflandırması Yapıldı:** Otel rezervasyon motoru, PMS, B2B portalı ve CRM gibi servisler Tier-1, Tier-2 ve Tier-3 seviyelerine ayrıldı.
- [ ] **Tier Bazlı RPO / RTO Hedefleri Onaylandı:** Tier-1 sistemler için RPO < 15 dk, RTO < 1 saat şeklinde yönetim onayı alındı.
- [ ] **Yedekleme Kapsamı Netleştirildi:** Veritabanları (DB), uygulama dosyaları, kullanıcı yüklemeleri ve sunucu konfigürasyon dosyaları (Nginx, Docker Compose vb.) kapsama dâhil edildi.
- [ ] **Yedek Türü Kombinasyonu Seçildi:** Veri boyutuna uygun Günlük Full, Saatlik Incremental ve Anlık Snapshot stratejisi kurgulandı.
- [ ] **Offsite Topolojisi Kuruldu:** Yedekler, ana sunuculardan bağımsız, izolasyonu sağlanmış ikincil lokasyon veya farklı bir IAM yetkilendirmeli Cloud hesabına (*Immutable Storage*) aktarıldı.
- [ ] **Erişim, Şifre ve Yetki Politikası Yazıldı:** Kriz anında yedeklere erişecek personel yetkileri, KMS şifreleme anahtarları ve şifre yönetim standartları dökümante edildi.
- [ ] **Restore Testi Takvime Bağlandı:** Ayda en az 1 kez otomatik veya manuel test ortamında *Zero-Data-Loss restore* testi kurala bağlandı.
- [ ] **Failover + Rollback Adımları Runbook'a İşlendi:** Ana sistem çöküşünde yedek sisteme geçiş (Failover) ve ana sistem düzeldiğinde geri dönme (Rollback) adım adım yazıldı.

- [ ] **Tatbikat Raporu ve İyileştirme Backlog'u Oluşturuldu:** Yapılan simülasyonların sonuçları, süre sapmaları ve aksiyon noktaları kayıt altına alındı.
- [ ] **KVKK Saklama ve Erişim Kontrolü Eklendi:** Yedekleme dosyalarının KVKK/GDPR kapsamında şifrelenmesi (AES-256) ve saklama periyotlarının (*Data Retention*) yasal sınırlara çekilmesi sağlandı.

B) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm
Yedek var ama geri dönmüyor	Düzenli restore testinin yapılmaması, bozuk yedek dosyaları.	Düzenli otomatize restore tatbikatı ve başarı/hata raporlama mekanizması.
RTO süresi hedefleri tutmuyor	Geri yükleme zincirinin uzun olması, yanlış yedekleme türü seçimi.	Snapshot/imaj tabanlı yedeklemeye geçiş ve restore adımlarının sadeleştirilmesi.
Offsite yedek krizde işe yaramıyor	Lokasyonun/hesabın tam ayrık olmaması veya yetki/şifre eksikliği.	Fiziksel/ağ bazında ayrık lokasyon + izole IAM hesabı ve kriz erişim runbook'u.
Kriz anında karar karmaşası yaşanıyor	Acil durum sorumlularının ve eskalasyon zincirinin tanımsız olması.	Eskalasyon, rol dağılımı ve acil durum iletişim planının netleştirilmesi.

C) 14 Günlük DR Implementation Sprint Planı

Hafta 1: Mimarinin Tasarımı, Envanter ve Güvenlik

- **Gün 1 (Tier Sınıflandırma):** Tüm sunucu ve servislerin listelenmesi; Web, PMS, B2B Portal ve CRM için Tier-1/2/3 seviyelerinin atanması.
- **Gün 2 (RPO/RTO Hedefleri):** İş birimleri ve yönetimle görüşülerek kabul edilebilir Maksimum Veri Kaybı (RPO) ve Maksimum Kesinti Sürelerinin (RTO) netleştirilip onaylanması.
- **Gün 3 (Kapsam & Envanter):** Veritabanı, medya dosyaları, Nginx/Apache konfigürasyonları, SSL sertifikaları ve env dosyalarının envanter matrisine çıkarılması.
- **Gün 4 (Yedek Türü Tasarımı):** Veri yüküne göre Full, Incremental ve Snapshot periyotlarının kurgulanması; veri sıkıştırma (*deduplication*) standartlarının belirlenmesi.

- **Gün 5 (Offsite Topolojisi):** Ana sunuculardan izolasyonu sağlanmış offsite (ayrık lokasyon veya WORM / Immutable Object Storage) mimarisinin kurulması.
- **Gün 6 (Yetki & Runbook Taslağı):** Kriz anında kullanılacak KMS şifreleme anahtarlarının kilitlenmesi, yetkilerin belirlenmesi ve Failover Runbook taslağının hazırlanması.
- **Gün 7 (İlk Restore Testi - DB):** İkincil bir izole test ortamında veritabanı yedeğinin sıfırdan geri yüklenmesi ve veri bütünlüğünün doğrulanması.

Hafta 2: Tatbikat, Doğrulama ve Yönetim Entegrasyonu

- **Gün 8 (İkinci Restore Testi - Dosya & Config):** Test ortamında medya dosyaları ve konfigürasyon parametrelerinin geri yüklenerek uygulamanın ayağa kaldırılması.
- **Gün 9 (Kısmi Failover Tatbikatı):** Ana sunucuda yapay bir kesinti oluşturularak trafiğin offsite/yedek sunucuya yönlendirilmesi (DNS/Load Balancer anahtarlaması).
- **Gün 10 (Rollback Tatbikatı):** Ana sunucu tekrar aktif edildikten sonra kriz anında biriken verilerin senkronize edilip trafiğin ana sunucuya geri çekilmesi.
- **Gün 11 (RPO/RTO Ölçüm Raporu):** Yapılan tatbikatlardaki gerçek RPO/RTO sürelerinin ölçülmesi ve hedeflenen sürelerle karşılaştırılması.
- **Gün 12 (İyileştirme Aksiyonları):** Yavaş restore veya yetki karmaşası gibi tespit edilen darboğazların (*bottlenecks*) teknik backlog'a işlenmesi.
- **Gün 13 (Tatbikat Dokümantasyonu):** Tüm test sonuçlarının, sistem mimari çizimlerinin ve bakım-destek ekipleri için eskalasyon şemasının dökümante edilmesi.
- **Gün 14 (Yönetim Özeti & Periyodik Takvim):** Yönetim kuruluna DR durum raporunun sunulması ve yıllık periyodik tatbikat takviminin kilitlenmesi.

D) Öncesi / Sonrası Durum KPI Tablosu

KPI Metriği	Yöntem Öncesi (Mevcut Durum)	Yöntem Sonrası (DR Standartı)	Hedef / Notlar
RTO (Recovery Time Objective)	Belirsiz / 12–24 saat	< 1 Saat (Tier-1 için)	Hedefe yakın, kesinti süresi minimuma indirildi.
RPO (Recovery Point Objective)	24 Saat (Günlük yedek)	< 15 Dakika	Veri kaybı riski minimal seviyeye çekildi.
Restore Başarı Oranı	Test edilmiyor ($\%0$)	$\%99.9$	Yapılan düzenli testlerle doğrulanmış başarı.

Tatbikat Sıklığı	Yılda 0 (Sadece kriz anında)	Çeyreklik / Yıllık Takvim	Yıllık plan dahilinde periyodik doğrulama.

Deliverables (Teslim Edilecek Çıktılar)

- **Tier Bazlı RPO/RTO & Sistem Kritiklik Dokümanı (v1.0):** Tüm otel ve B2B web altyapısının toparlanma önceliklerini gösteren stratejik plan.
- **Offsite Topoloji & Güvenli Erişim Politikası:** İzolasyonu sağlanmış yedekleme mimarisi ve kriz anı yetkilendirme prosedürü.
- **Failover & Rollback Runbook (Kriz Anı Operasyon Kitapçığı):** Kriz anında teknik ekibin adım adım uygulayacağı yönlendirme ve geri alma kılavuzu.
- **DR Tatbikat Raporu & İyileştirme Backlog'u:** Gerçekleştirilen simülasyonların süre analizi ve tespit edilen aksaklıkların çözüm listesi.

[Checklist Card]

BT yöneticileri, DevOps mühendisleri ve sistem mimarları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Disaster Recovery (DR) operasyon kontrol kartı. Koyu karbon gri ve siber güvenlik mavisi tonlarındaki teknolojik zemin üzerinde, sunucu koruma kalkanı, yedekleme bulutu ve geri yükleme kronometresi simgelerini barındıran neon yeşili ile

elektrik mavisi ikonlar yer alıyor. Kartın üzerinde; "Tier-1 RPO/RTO Hedefleri", "Offsite & Immutable Storage Kurulumu", "Automated Restore & Failover Tatbikatı" ve "Rollback & Adli Audit Log Kaydı" maddeleri, yanlarında parlak onay işaretleriyle scannable ve kurumsal bir checklist formatında sergileniyor.