

Doküman: Airisto Operasyonel Risk Yönetimi Raporu

Belge Adı: Airisto - Operasyonel Risk Analizi ve Yönetim Politikası

Rapor Tarihi: 05.09.2025

Sürüm: 1.0

1. Amaç ve Kapsam

1.1. Raporun Amacı:

Bu raporun amacı, Airisto'nun stratejik hedeflerine ulaşmasını ve operasyonel sürekliliğini tehlikeye atabilecek potansiyel riskleri sistematik bir şekilde tanımlamak, analiz etmek, değerlendirmek ve bu riskleri yönetmek için alınacak aksiyonları ve kontrol mekanizmalarını belirlemektir. Bu proaktif yaklaşım, hizmet kalitemizi güvence altına almayı, paydaşlarımızın güvenini korumayı ve sürdürülebilir bir büyüme sağlamayı hedefler.

1.2. Kapsam:

Bu risk analizi; teknolojik altyapı, bilgi güvenliği, yasal ve düzenleyici uyum, insan kaynakları, finansal sürdürülebilirlik ve itibar yönetimi dahil olmak üzere Airisto'nun tüm temel operasyonel süreçlerini kapsar.

2. Risk Yönetimi Metodolojisi

Airisto, risklerini yönetmek için "Tanımla - Analiz Et - Değerlendir - Müdahale Et - İzle" adımlarından oluşan sistematik bir metodoloji izler:

- **Risk Tanımlama:** Potansiyel riskler beyin fırtınası, iç/dış denetimler ve paydaş geri bildirimleri ile belirlenir.
- **Risk Analizi:** Her bir riskin gerçekleşme **olasılığı** (düşük, orta, yüksek) ve gerçekleşmesi durumunda yaratacağı **etkisi** (düşük, orta, yüksek) analiz edilir.
- **Risk Değerlendirme:** Olasılık ve etki analizine göre riskler önceliklendirilir.
- **Riske Müdahale:** Önceliklendirilen riskler için aşağıdaki stratejilerden biri veya birkaçı uygulanır:
 - **Azaltma (Mitigation):** Riskin olasılığını veya etkisini düşürecek kontroller uygulamak.
 - **Transfer (Transfer):** Riski sigorta gibi üçüncü bir tarafa devretmek.

- **Kaçınma (Avoidance):** Riskli aktiviteden tamamen vazgeçmek.
- **Kabul (Acceptance):** Düşük seviyeli riskler için herhangi bir aksiyon almamak.
- **İzleme ve Gözden Geçirme:** Uygulanan kontrollerin etkinliği ve risk seviyelerindeki değişimler sürekli olarak izlenir.

3. Tanımlanan Ana Operasyonel Riskler ve Yönetim Stratejileri

Aşağıda, Airisto için tanımlanmış ana risk kategorileri, potansiyel riskler ve bunlara yönelik yönetim stratejilerimiz bulunmaktadır:

3.1. Teknolojik ve Altyapı Riskleri:

- **Risk:** Hizmet kesintisi (Downtime) - Sunucu arızaları, DDoS saldırıları veya altyapı sorunları nedeniyle platformun erişilemez hale gelmesi.
- **Etki:** Yüksek | **Olasılık:** Düşük
- **Yönetim Stratejisi (Azaltma):**
 - Yüksek erişilebilirlik (%99.9 Uptime SLA) sunan, coğrafi olarak yedekli bulut altyapısı (örn: AWS, Azure, GCP) kullanımı.
 - Otomatik yük dengeleme (load balancing) ve failover sistemleri.
 - Gelişmiş DDoS koruma hizmetleri.
 - Sistem performansının 7/24 anlık izlenmesi ve anomali tespiti.

3.2. Bilgi Güvenliği Riskleri:

- **Risk:** Veri İhlali - Kullanıcı kişisel verilerinin veya şirket verilerinin yetkisiz kişilerce ele geçirilmesi.
- **Etki:** Yüksek | **Olasılık:** Düşük
- **Yönetim Stratejisi (Azaltma):**
 - "Bilgi Güvenliği Politikası"nda detaylandırılan tüm teknik kontroller (şifreleme, erişim kontrolü, MFA vb.).
 - Düzenli güvenlik denetimleri ve sızma testleri.
 - Kapsamlı bir "Olay Müdahale Planı"nın varlığı.
 - Siber güvenlik sigortası (Transfer).

3.3. Algoritmik ve Performans Riskleri:

- **Risk:** Tespit Doğruluğunun Düşmesi - Yeni nesil yapay zeka modellerinin tespit edilememesi veya "yanlış pozitif" (insan yazımını AI olarak işaretleme) oranının artması.
- **Etki:** Yüksek | **Olasılık:** Orta
- **Yönetim Stratejisi (Azaltma):**
 - Yapay zeka modellerimizin (Türkçe ve İngilizce) yeni AI araçları çıktıkça sürekli olarak güncellenmesi ve yeniden eğitilmesi.
 - Algoritma performansının, geniş ve çeşitli test veri setleri üzerinde sürekli olarak izlenmesi.
 - Kullanıcıların hatalı buldukları sonuçları bildirebilecekleri bir geri bildirim mekanizması.

3.4. Yasal ve Uyumluluk Riskleri:

- **Risk:** KVKK veya diğer veri koruma yasalarına (örn: GDPR) uyumsuzluk.
- **Etki:** Yüksek | **Olasılık:** Düşük
- **Yönetim Stratejisi (Azaltma):**
 - "KVKK Uyum Raporu"nda detaylandırılan tüm politika ve prosedürlerin sıkı bir şekilde uygulanması.
 - Yasal değişikliklerin sürekli takip edilmesi ve politikalara yansıtılması için hukuk danışmanlığı hizmeti alınması.
 - Tüm çalışanlara düzenli KVKK farkındalık eğitimi verilmesi.

3.5. İtibar ve Pazar Riskleri:

- **Risk:** Marka itibarının zedelenmesi - Olumsuz medya haberleri, sosyal medya krizleri veya rakip faaliyetleri nedeniyle marka güveninin sarsılması.
- **Etki:** Yüksek | **Olasılık:** Orta
- **Yönetim Stratejisi (Azaltma):**
 - "Şeffaflık ve Hesap Verebilirlik Politikası"na tam bağlılık.
 - Proaktif halkla ilişkiler ve iletişim stratejisi.

- Müşteri memnuniyetinin sürekli ölçülmesi ve şikayet yönetimi süreçlerinin etkin işletilmesi.
- Pazar ve rakip faaliyetlerinin sürekli analizi.

4. Raporlama ve Gözden Geçirme

Bu Risk Yönetimi Raporu, yılda en az bir kez veya şirketin stratejik yönünü etkileyebilecek önemli bir değişiklik olduğunda üst yönetim tarafından gözden geçirilir ve güncellenir. Risk matrisi ve kontrol etkinlikleri, düzenli olarak "Yönetimin Gözden Geçirme" toplantılarının bir parçası olarak değerlendirilir.