RİSK YÖNETİMİ

Hazırlayan: İzzet Esener **210229048** - Salih Can Turan **210229040**

Grup No: 12

Gurup Yöneticisi

İzzet Esener **210229048**

Gurup Üyeleri

Salih Can Turan **210229040**

Kerem Kartal **210229019**

Furkan Öztürk **230229083**

Ders: Yazılım Proje Yönetimi

Proje Tanımı

Bu proje, diyetisyenler ile danışanları bir araya getiren, sağlıklı yaşam ve beslenme süreçlerini daha erişilebilir ve etkili hale getirmeyi amaçlayan yenilikçi bir platformdur. Kullanıcı dostu bir yapıya sahip olan bu sistem, bireylerin ihtiyaçlarına uygun uzmanlarla kolayca iletişime geçmesini ve profesyonel destek almasını sağlar. Aynı zamanda, platform içerisindeki etkileşim mekanizmaları sayesinde danışanlar, deneyimlerini paylaşarak diğer kullanıcılara rehberlik edebilir. Güvenilir, şeffaf ve etkileşimli bir hizmet anlayışıyla geliştirilen bu proje, sağlıklı beslenme alanında dijital dönüşüme katkıda bulunmayı hedeflemektedir.

Rapor Tanımı

Bu rapor Diet App projesinin olası risklerini belirlemek, riskleri sınıflandırmak ve risklerin çözümü için bir şema sunmak için hazırlanmıştır. Risk yönetimi raporu, **Projenin Sürekliliği**, **Müşteri Güveni, Yasal Uyum** gibi konularda projenin doğru amaçla ve eksiksiz ilerlemesi için kritiktir. Bu raporda değinilen başlıklar aşağıdaki gibidir:

Risklerin Tanımlanması:

Projeyi etkileyebilecek 17 temel risk (veri sızıntısı, yasal uyumsuzluk, sistem kesintileri vb.) detaylı şekilde listelendi.

Risk Analizi:

Her risk için şiddet, olasılık ve risk puanı hesaplandı.

Örnek: *"Platform dışı ödeme dolandırıcılığı"* riski 20 puan (Kritik) olarak derecelendirildi.

Önlem Planları:

Her risk için pratik çözümler sunuldu (örn: çok faktörlü kimlik doğrulama, düzenli yedekleme, sertifika doğrulama sistemleri).

Proje Riskleri

1. Finansal ve İşlem Riskleri

- **Platform Dışı Ödeme Dolandırıcılığı:** Diyetisyen ve danışanın platform dışında anlaşarak ödeme yapması, sistemin gelir kaybına uğraması ve güvenlik denetiminin bypass edilmesi.
- **Ödeme Sistemindeki Sorunlar:** Danışanların ödeme yapamaması veya tekrar tekrar ücret alınması.
- **Abonelik İptallerinin Yüksek Olması:** Memnuniyetsiz danışanların platformu terk etmesi.

2. Veri ve Mahremiyet Riskleri

- **Hassas Sağlık Verilerinin İzinsiz Paylaşımı:** Danışanların kilo, hastalık geçmişi gibi özel verilerinin sızması.
- **Zayıf Şifreleme ve Güvenlik Açıkları:** Kullanıcı hesaplarının kolayca ele geçirilmesi.
- **Üçüncü Taraf Uygulamalarla Güvensiz Entegrasyon:** Ödeme sistemleri veya harici API'lerden kaynaklı veri ihlalleri.

3. Kullanıcı Deneyimi ve Sistem Riskleri

- **Yanlış Diyet Programı Oluşturma:** Sistemin hatalı veri işlemesi nedeniyle danışana uygun olmayan diyet listesi sunması.
- **Yorum ve Değerlendirme Manipülasyonu:** Sahte hesaplarla diyetisyenlere haksız puanlama yapılması.
- **Chat Sisteminin Güvenlik Açıkları:** Danışan-diyetisyen arasındaki yazışmaların üçüncü şahıslarca okunması.

4. İş Sürekliliği ve Altyapı Riskleri

- **Sunucu Kesintileri:** Yüksek trafikte sistemin çökmesi ve randevu/diyet planlarının kaybolması.
- **Veri Yedekleme Eksikliği:** Kullanıcı verilerinin ani bir arızada silinmesi.

5. Yasal ve Uyum Riskleri

- **Sağlık Verilerinin Yasalara Uygunsuz Saklanması:** GDPR/HIPAA gibi düzenlemelere aykırı veri işleme.
- **Diyetisyenlerin Sertifikasız Çalışması:** Platformda yetkisiz kişilerin danışmanlık vermesi.
- **Yanlış Tıbbi Tavsiye Riski:** Diyetisyenlerin yanlış bilgi vermesi nedeniyle hukuki sorunlar.

6. Kullanıcı ve Eğitim Eksiklikleri

- **Danışanların Sistemi Yanlış Kullanımı:** Hedef kiloyu veya alerjileri yanlış girmesi.
- **Diyetisyenlerin Platform Kurallarını İhlali:** Spam mesaj atma veya uygunsuz içerik paylaşma.
- **Güvenlik Farkındalığının Düşük Olması:** Kullanıcıların basit şifreler seçmesi veya phishing saldırılarına açık olması.

Risk Değerlendirme Matrisi

Risk değerlendirme matrisi ile Risklerin olasılığı ve şiddeti ile seviyesi belirlenmiştir. Daha sonra riskler bu matris kullanılarak riskler derecelendirilecektir

Olasılık / Şiddet	**1-Çok Hafif**	**2-Hafif**	**3-Orta**	**4-Ciddi**	**5-Çok Ciddi**
1-Çok Düşük	1 (Önemsiz)	2(Önemsiz)	3(Düşük)	4(Düşük)	5(Düşük)
2-Düşük	2(Önemsiz)	4(Düşük)	6(Düşük)	8(Orta)	10(Orta)
3-Orta	3(Orta)	6 (Düşük)	9 (Orta)	12(Yüksek)	15(Yüksek)
4-Yüksek	4(Düşük)	8 (Orta)	12 (Yüksek)	16 (Yüksek)	20 (Çok Yüksek)
5-Çok Yüksek	5 (Düşük)	10 (Orta)	15 (Yüksek)	20 (Çok Yüksek)	25 (Kritik)

Risk Matrisi Seviye Tanımları

Risk değerlendirme matrisindeki seviyelerin tanımı ve aksiyon planı aşağıdaki tabloda yapılmıştır.

Risk Puanı	**Seviye**	**Tanımı**	**Aksiyon Planı**
20-25	**Kritik**	Kabul edilemez. Sistemin/iş modelinin çökmesine veya ciddi yasal sonuçlara yol açar.	**Acil müdahale.** Faaliyet durdurulur, risk azaltılmadan devam edilmez
15-19	**Çok Yüksek**	Büyük zarar olasılığı. Finansal/itibar kaybı veya uzun süreli kesintiler.	**Hemen harekete geç.** Önlemler 48 saat içinde planlanır ve uygulanır.
12-14	**Yüksek**	Önemli operasyonel /finansal etki. Kullanıcı güvenini sarsabilir.	**Kısa vadeli çözüm.** 1 hafta içinde aksiyon alınır, süreç iyileştirilir.
8-11	**Orta**	Kontrol edilebilir ama göz ardı edilmemeli. Hafif verimlilik kaybı.	**Orta vadeli plan.** 1 ay içinde önlemler devreye alınır.
3-7	**Düşük**	Minimal etki. Sistem performansını veya kullanıcı deneyimini hafif etkiler.	**Rutin takip.** Mevcut önlemler yeterli, düzenli denetim yapılır.
1-3	**Önemsiz**	Neredeyse hiç etkisi yok. Kayda değer bir tehdit oluşturmaz.	**Pasif izleme.** Ek kaynak ayrılmaz, raporlama yapılır.

Risklerin Analizi ve Değerlendirmesi

Raporun bu kısmında ilgili projenin risklerinin **Nedenleri**, **Potansiyel Sonuçları**, **Risk Seviyesi** ve bu risk için **Yapılacaklar** incelenmiştir.

Risk	Nedenler	Potansiyel Sonuçlar	Risk Seviyesi	Yapılacaklar
Platform Dışı Ödeme Dolandırıcılığı	-Kullanıcıların komisyon ödememek için platform dışı ödeme yapması. - Sistemsel denetim eksikliği	-Gelir kaybı, güvenlik bypass'ı -Platform itibarının zedelenmesi	**Şiddet: 5** **Olasılık: 4** **Risk Puanı: 20**	1. Otomatik chat filtreleme sistemi 2. Sözleşme yaptırımları ekleme 3. İhlal durumunda hesap askıya alma.
Ödeme Sistemindeki Sorunlar	- Teknik altyapı hataları - Ödeme sağlayıcı entegrasyon sorunları - Fraud (sahtecilik) girişimleri	- Müşteri memnuniyetsizliği - Gelir kaybı - İtibar zedelenmesi - Yasal uyum sorunları	**Şiddet:4** **Olasılık:3** **Risk Puanı:12**	1. Yedek ödeme kanalları oluşturma 2. Fraud önleme sistemi* kurma 3. Ödeme işlem loglarının düzenli denetlenmesi
Abonelik İptallerinin Yüksek Olması	- Hizmet kalitesinde düşüş - Rekabetçi fiyatlandırma eksikliği - Kullanıcı deneyimi sorunları - Memnuniyet ölçümlerinin yetersizliği	- Gelir kaybı - Müşteri tabanında azalma - Pazar payı kaybı - Marka itibarında zedelenme	**Şiddet:3** **Olasılık:3** **Risk Puanı:9**	1. İptal öncesi anketler uygulama 2. Geri kazanım kampanyaları düzenleme 3. Kullanıcı deneyimi iyileştirmeleri yapma
Hassas Sağlık Veri Sızıntısı	- Zayıf veri şifreleme protokolleri - Yetkisiz erişim açıkları - Çalışan hataları veya kötü niyetli davranışlar - Üçüncü taraf entegrasyon güvenlik açıkları	- Ağır yasal yaptırımlar (GDPR/HIPAA ihlalleri) - Marka itibarında ciddi kayıp - Müşteri güveninin sarsılması - Tazminat talepleri ve davalar	**Şiddet:5** **Olasılık:4** **Risk Puanı:20**	1. End-to-end veri şifreleme* uygulama 2. Sıkı erişim kontrolleri ve izin yönetimi 3. Düzenli güvenlik denetimleri ve penetrasyon testleri 4. Çalışan eğitimleri ve bilinçlendirme programları

Zayıf Şifreleme	- Eski şifreleme algoritmaları kullanımı - Yetersiz şifre karmaşıklık kuralları - Düzenli şifre güncelleme politikası eksikliği - Çok faktörlü kimlik doğrulamanın olmaması	- Kullanıcı hesaplarının ele geçirilmesi - Hassas verilere yetkisiz erişim - Veri ihlali ve mahremiyet sorunları - Yasal uyum problemleri	**Şiddet:4** **Olasılık:3** **Risk Puanı:12**	1. Güçlü şifre politikaları uygulama (min. 12 karakter, özel karakter zorunluluğu) 2. Çok faktörlü kimlik doğrulama (MFA) zorunlu hale getirme 3. Düzenli şifre değişim zorunluluğu (90 günde bir)

Üçüncü Taraf Entegrasyon Riskleri	- Güvenlik açıkları - Zayıf API kontrolleri - Yetkisiz erişim	- Veri sızıntıları - Sistem istismarı - Hizmet kesintileri	**Şiddet:4** **Olasılık:4** **Risk Puanı:16**	1. API güvenlik denetimi 2. Sıkı erişim kontrolleri 3. Düzenli güvenlik testleri
Yanlış Diyet Programı	-Sahte hesap oluşturma kolaylığı. -Yeterli doğrulama ve filtreleme sisteminin olmaması	-Güvenilirlik kaybı -Haksız rekabet -Kaliteli diyetisyenlerin platformdan ayrılması	**Şiddet:5** **Olasılık:3** **Risk Puanı:15**	1.Hesap doğrulama sistemleri, yorum filtreleme algoritmaları 2.Şüpheli puanlama davranışları için denetim mekanizması kurulması
Yorum Manipülasyonu **Bot Saldırıları (Spam Kayıtlar veya Yorumlar)**	-Sahte hesapların kolay oluşturulması, yorum yapma erişiminin kontrolsüz olması. -CAPTCHA gibi doğrulama sistemlerinin olmaması.	-Güven kaybı, haksız rekabet, kaliteli uzmanların platformdan ayrılması. -Gerçek kullanıcı deneyiminin düşmesi, sistem kaynaklarının boşa kullanılması.	**Şiddet:4** **Olasılık:4** **Risk Puanı:12**	Google reCAPTCHA IP sınırlama Kullanıcı aktivite izleme.

Chat Güvenlik Açıkları	-Yetersiz şifreleme -Açık bağlantılar -Güvenli oturum yönetiminin olmaması	-Özel sağlık bilgilerinin sızması -Hukuki yaptırımlar -Kullanıcı güveninin sarsılması	**Şiddet:4** **Olasılık:3** **Risk Puanı:12**	1.Uçtan uca şifreleme uygulanmalı. 2.Oturum kimlik doğrulama mekanizmaları (JWT, token süresi vb.) güçlendirilmeli.

Sunucu Kesintileri	-Yetersiz sunucu kapasitesi -Ölçeklenebilir altyapı eksikliği -Ani trafik artışlarına hazırlıksız sistem yapısı	-Randevu ve diyet planlarının kaybolması -Kullanıcı memnuniyetsizliği -Platforma olan güvenin azalması	**Şiddet:5** **Olasılık:3** **Risk Puanı:15**	1.Sunucu altyapısı bulut ortamında ölçeklenebilir hale getirilmeli 2.Trafik yoğunluğuna karşı otomatik kaynak artırımı ve düzenli performans testleri uygulanmalı .
Veri Yedekleme Eksikliği	-Düzenli yedekleme yapılmaması -Yedekleme sistemlerinin eksikliği - Felaket kurtarma planı olmaması	-Veri kaybı yaşanır -Hizmet kesintileri oluşur -Müşteri güveni sarsılır	**Şiddet:5** **Olasılık:2** **Risk Puanı:10**	1. Otomatik yedekleme sistemleri kurulur 2. Çapraz bölge veri replikasyonu yapılır 3. Düzenli kurtarma testleri uygulanır
Sağlık Verilerinin Yasalara Uygunsuz Saklanması	-Veri saklama politikalarının eksikliği - Çalışanların yasal gereklilikler konusunda bilgisizliği -Uyumsuz üçüncü taraf entegrasyonları	-Ağır yasal yaptırımlar uygulanır -Kurum itibarı zedelenir -Müşteri güveni kaybolur	**Şiddet:5** **Olasılık:3** **Risk Puanı:15**	1. Veri saklama ve imha politikaları oluşturulur 2. Düzenli yasal uyum denetimleri yapılır 3. Çalışan eğitim programları uygulanır

Sertifikasız Diyetisyen Riski	-Sertifika doğrulama sürecinin olmaması -Sahte belgelerin tespit edilememesi -Denetim mekanizmalarının yetersizliği	-Yanlış tıbbi tavsiye riski artar - Hukuki sorumluluk doğar -Platform güvenilirliği zedelenir	**Şiddet:4** **Olasılık:4** **Risk Puanı:16**	1. Sertifika doğrulama sistemi kurulur 2. Resmi kurumlarla entegre doğrulama yapılır 3. Düzenli denetimler uygulanır
Yanlış Tıbbi Tavsiye Riski	-Diyetisyenin alanında yeterli bilgiye sahip olmaması. -Danışanın ne istediğini bilmesi.	- Danışan sağlığı riske girer - Tazminat davaları açılabilir - Platformun itibarı zarar görür	**Şiddet:5** **Olasılık:4** **Risk Puanı:20**	1 Diyetisyen sertifikaları düzenli kontrol edilir 2 Sürekli eğitim programları uygulanır 3 Tavsiyeler için ikinci görüş mekanizması kurulur
Danışanların Sistemi Yanlış Kullanımı	-Danışanın kendi sağlık durumu hakkında yeterli bilgiye sahip olmaması.	-Danışanların doğru diyetisyen hizmetini alamaması ve şikayette bulunması	**Şiddet:3** **Olasılık:2** **Risk Puanı:6**	Sistem tanıtımının doğru v-bir şekilde yapılması ve danışanların sistem tanımına rahatça ulaşmasının sağlanması (Görünürlük açısından).
Diyetisyenlerin Platform Kurallarının İhlali	-Kuralların net belirtilmemesi -Denetim mekanizmalarının yetersizliği - Yaptırımların caydırıcı olmaması	- Kullanıcılar rahatsız olur - Platform itibarı zedelenir - Yasal sorunlar yaşanabilir	**Şiddet:5** **Olasılık:4** **Risk Puanı:20**	1. Net kullanım kuralları oluşturulur 2. Otomatik içerik filtreleme sistemi kurulur 3. İhlal durumunda yaptırımlar uygulanır
Güvenlik Farkındalığının Düşük Olması	- Düzenli güvenlik eğitimi eksikliği -Şifre politikalarının zayıf olması - Phishing testlerinin* yapılmaması	-Hesap güvenliği ihlal edilir -Veri sızıntıları yaşanır -Platform güvenilirliği azalır	**Şiddet:5** **Olasılık:5** **Risk Puanı:25**	1. Zorunlu güvenlik eğitimleri verilir 2.Güçlü şifre politikaları uygulanır 3. Düzenli phishing simülasyonları yapılır

SEO ve İtibar Zedelenmesi	Kötü içeriklerin yayılması, Google tarafından cezalandırma	Kullanıcı trafiğinde azalma, güven kaybı	**Şiddet:5 Olasılık:4 Risk Puanı:20**	Marka yönetim stratejisi, SEO danışmanlığı, Search Console kullanımı
Sosyal Mühendislik Saldırıları	Kullanıcı eğitimsizliği, sahte e-posta/mesajlar	Hesap ele geçirme, veri sızdırma, kullanıcı kaybı	**Şiddet:4 Olasılık:4 Risk Puanı:16**	Kullanıcı farkındalık eğitimi, güvenli iletişim yönergeleri
Lisans İhlalleri	Üçüncü parti yazılım lisanslarının ihlali	Yasal cezalar, ürünün durdurulması	**Şiddet:4 Olasılık:2 Risk Puanı:8**	Lisans kontrol araçları kullanmak, açık kaynak lisans bilinci eğitimi
Vergi / Fatura Uyumsuzluğu	Otomasyon eksikliği, muhasebe takibi zayıf	Mali ceza, güven kaybı	**Şiddet:4 Olasılık:3 Risk Puanı:8**	Otomatik faturalama sistemi, muhasebe danışmanlığı

Fraud Önleme Sistemi Nedir?

Fraud önleme sistemi, bir platformda kullanıcıların yaptığı işlemleri analiz ederek, şüpheli ya da olağandışı davranışları otomatik olarak tespit eden yazılım ve algoritmalardan oluşur. Genellikle yapay zekâ, makine öğrenimi, davranışsal analiz ve istatistiksel modellerle desteklenir.

End-to-end veri şifreleme (Uçtan Uca Şifreleme - E2EE) Nedir?

Bir verinin gönderen ile alıcı arasında tamamen şifrelenmiş şekilde iletilmesini sağlayan bir güvenlik yöntemidir.

Phishing testleri (oltalama testleri) Nedir?

Bir kurumun çalışanlarının veya kullanıcılarının sahte e-posta, mesaj veya bağlantılar yoluyla kandırılma eğilimini ölçmek için yapılan kontrollü ve simüle edilmiş siber güvenlik testleridir.