OMERDOGU.COM GERİ BİLDİRİM PLATFORMU

Ramak Kala, Tehlikeli Durum ve DÖF Yönetimi İçin Literatür Taramalı Algoritmik Model

Algoritmik tasarım, başarı ölçümü ve uygulama başarımı yüksek dijital İSG geri bildirim sistemi için makale

Hazırlanma tarihi: 05.07.2026 | Kapsam: PHP + SQLite + SMTP tabanlı kurumsal geri bildirim platformu | Hedef çıktı: uygulanabilir akademik/teknik makale

Bu makale, yakın olay ve tehlikeli durum bildirimlerini yalnızca kayıt altına alan bir yazılım yaklaşımı yerine; ISO 45001 odaklı sürekli iyileştirme, ISO/IEC 27001 odaklı bilgi güvenliği, ISO 10002 odaklı şikayet/geri bildirim yönetimi ve DÖF/CAPA kapatma disipliniyle bütünleşen bir algoritmik sistem modeli olarak ele alır.

Çalışmanın temel iddiası şudur: yüksek başarımlı bir geri bildirim platformu, yalnızca form ve e-posta gönderen bir araç değildir; çalışan katılımını artıran, anonim bildirim güvenini koruyan, fotoğraf kanıtını güvenli ve taşınabilir hale getiren, kritik bildirimleri otomatik DÖF dokümanına dönüştüren, e-posta ve panel üzerinden takip edilebilir aksiyon döngüsü kuran bir organizasyonel öğrenme altyapısıdır.

Bu nedenle makale, literatür taraması ile yazılım algoritmasını birlikte okur: yakın olay bildirimi, güvenlik iklimi, raporlama kültürü, hiyerarşik kontrol yaklaşımı, dijital olay yönetimi, bilgi güvenliği ve teknoloji kabul modelleri aynı çerçevede değerlendirilmiştir.

Özet

İş sağlığı ve güvenliği alanında ramak kala olayları ve tehlikeli durum bildirimleri, kazaya dönüşmeden önce riskin görünür hale getirilmesini sağlayan kritik öncü göstergelerdir. Ancak literatür, yalnızca bir raporlama aracı kurmanın güvenlik performansını kendiliğinden iyileştirmediğini; raporların sınıflandırılması, kök neden analizi, düzeltici/önleyici faaliyet takibi, çalışan katılımı, güvenli veri işleme ve yönetim sahipliği ile birlikte tasarlanması gerektiğini göstermektedir.

Bu makale, omerdogu.com geri bildirim platformu bağlamında geliştirilen algoritmik modeli geniş literatür çerçevesinde incelemektedir. Model; firma kayıt/onay süreci, token tabanlı karekod erişimi, anonim bildirim, güvenli dosya yükleme, fotoğrafı hafif JPG formatına dönüştürme, kritik türlerde otomatik DÖF Word üretimi, SMTP e-posta ekiyle bildirim, firma panelinde sorumlu-hedef tarih-aksiyon-kapanış takibi ve denetim kaydı bileşenlerinden oluşur.

Çalışma, ISO 45001'in önleyici ve sistematik İSG yaklaşımı, OSHA/NIOSH kaynaklarında vurgulanan öncü göstergeler ve hiyerarşik kontrol mantığı, ISO/IEC 27001'in risk temelli bilgi güvenliği, ISO 10002'nin geri bildirim/şikayet süreçleri ve teknoloji kabul modellerinin uygulama başarısı değişkenleri ile uyumlu bir tasarım önermektedir.

Abstract

Near-miss and unsafe-condition reporting are leading mechanisms for making latent occupational risks visible before they become accidents. Nevertheless, literature shows that reporting systems produce value only when reports are classified, investigated, linked to corrective/preventive actions, protected by trust and privacy safeguards, and integrated into management review. This article develops a literature-grounded algorithmic model for a PHP/SQLite/SMTP-based feedback platform that converts high-risk reports into Word-based CAPA/DÖF records, compresses photographic evidence into portable JPEG files, sends structured notifications, and enables traceable closure in the firm panel.

Anahtar kelimeler

Ramak kala, tehlikeli durum, DÖF, CAPA, ISO 45001, ISO/IEC 27001, ISO 10002, yakın olay yönetimi, dijital olay bildirimi, güvenli dosya yükleme, teknoloji kabulü, İSG performansı.

1. Giriş

Modern İSG yönetimi, kaza olduktan sonra kayıt tutan reaktif yaklaşımın ötesine geçerek, kaza olmadan önce zayıf sinyalleri yakalamaya yönelmiştir. Ramak kala olayları, tehlikeli durumlar ve güvensiz davranış bildirimleri bu zayıf sinyallerin en pratik kaynaklarıdır. ISO 45001 açıklamalarında da işyerinde yaralanma ve hastalıkların önlenmesi, risklerin yönetilmesi ve İSG performansının sürekli iyileştirilmesi merkezî amaçlar olarak tanımlanır (ISO, 2026a).

Saha gerçekliğinde ise üç temel sorun görülür. Birincisi, çalışanlar çoğu zaman bildirim yapmanın sonucundan emin değildir; bildirim ceza, suçlama veya gereksiz bürokrasi olarak algılanabilir. İkincisi, formlar dijital olsa bile fotoğraf, açıklama, tarih, konum ve aksiyon bilgisi aynı takip döngüsüne bağlanmazsa kayıt "veri mezarlığına" dönüşebilir. Üçüncüsü, firma yönetimi bildirimi aldıktan sonra aksiyonun kime atandığını, hedef tarihin ne olduğunu ve kapanışın nasıl doğrulandığını izleyemezse sistem öğrenme üretmez.

Bu makalenin amacı, yakın olay ve tehlikeli durum bildirimlerini uçtan uca işleyen; yüksek gizlilik, yüksek taşınabilirlik, yüksek uygulanabilirlik ve yüksek yönetim görünürlüğü sağlayan bir algoritmik model önermektir. Model, geliştirilen PHP platformunun somut akışına dayanmakla birlikte, farklı küçük ve orta ölçekli işletmelere uyarlanabilir genel bir tasarım mantığı sunar.

Araştırma sorusu şu şekilde ifade edilebilir: Ramak kala ve tehlikeli durum bildirimlerini, güvenli dosya işleme ve DÖF takibiyle bütünleştiren bir dijital platform hangi algoritmik adımlarla tasarlanır ve başarımı hangi ölçütlerle değerlendirilir? Bu tasarlanan platformlarını gizliliğinin sağlanması ve kullanıcıya özgü yapıların özelleştirimesi, gerçek ve tüzel kişilikli resmi işletmelerin işlemlerinin kolaylaştırılması ve raporlanmasını hızlandırması süreçlerini içermektedir.

İlerleyen süreçte bu yapıların bu yapıların ilerletilmesi ve toplanması yasal izinler çerçevesinde işlenmesi ve daha geliştirilerek sistemlerin bütünleştirilmesi amaçlanmıştır.

2. Yöntem

Çalışma iki katmanlı bir yöntem izler. İlk katman, literatür ve standart taramasıdır. Bu kapsamda yakın olay yönetimi, güvenlik iklimi, öncü göstergeler, hiyerarşik kontrol, olay bildirim sistemleri, CAPA/DÖF yaklaşımı, bilgi güvenliği, güvenli dosya yükleme ve teknoloji kabul modelleri incelenmiştir. İkinci katman, tasarım bilimi mantığıdır: literatürden çıkarılan gereksinimler, uygulanabilir bir yazılım algoritmasına dönüştürülmüştür.

Kaynak seçiminde resmi standart ve rehberlere öncelik verilmiştir. ISO 45001, ISO 10002 ve ISO/IEC 27001/27700 sayfaları yönetim sistemi çerçevesi için; OSHA ve NIOSH kaynakları öncü göstergeler, yakın olay bildirimi ve hiyerarşik kontrol için; OWASP ve NIST kaynakları güvenli dosya yükleme ve siber risk yönetimi için; KVKK ve EDPB kaynakları kişisel veri ve tasarımdan itibaren mahremiyet ilkeleri için kullanılmıştır.

Akademik tarafta Gnoni ve arkadaşlarının yakın olay yönetim sistemlerine ilişkin literatür taraması, Demich ve arkadaşlarının NIOSH destekli yakın olay raporları çalışması, Zohar'ın güvenlik iklimi çalışması, teknoloji kabul literatüründe Davis'in TAM modeli, Venkatesh ve arkadaşlarının UTAUT modeli ve DeLone-McLean bilgi sistemleri başarı modeli dikkate alınmıştır.

> Yöntemsel sınır: Bu makale bir saha deneyinin sonuçlarını raporlamaz; uygulama başarımını ölçmek için kullanılacak metrikleri ve pilot uygulama planını önerir. Dolayısıyla performans iddiaları "ölçülmüş sonuç" değil, literatür destekli tasarım ve değerlendirme hipotezidir.

3. ISO 45001 ve önleyici İSG yönetimi

ISO 45001:2018, iş sağlığı ve güvenliği yönetim sistemi için uluslararası bir çerçeve sunar. ISO'nun açıklamasına göre standart, kuruluşların güvenli ve sağlıklı çalışma ortamları sağlamasına, iş kaynaklı yaralanma ve hastalıkları önlemesine, riskleri yönetmesine ve İSG performansını sürekli iyileştirmesine yardımcı olur (ISO, 2026a). Bu bakış, olay bildirim platformunun yalnızca kayıt modülü değil, yönetim sistemi bileşeni olarak tasarlanması gerektiğini gösterir.

ISO 45001'in uygulama mantığında liderlik, çalışan katılımı, tehlikelerin belirlenmesi, risklerin değerlendirilmesi, operasyonel kontrol, eğitim, performans izleme ve sürekli iyileştirme birlikte değerlendirilir. OSHA'nın güvenlik ve sağlık programı yaklaşımı da yönetim liderliği, çalışan katılımı, tehlike tanımlama, önleme-kontrol, eğitim, değerlendirme ve iletişim gibi çekirdek unsurlar etrafında şekillenir (OSHA, 2026a).

Bu çerçeve, dijital bildirim algoritmasına şu gereksinimleri yükler: bildirim kolay olmalı, çalışan anonim kalabilmeli, kayıtlar sınıflandırılmalı, kritik bildirimler aksiyona dönmeli, aksiyon sahipliği görünür olmalı, kapanış doğrulanmalı ve yönetime ölçülebilir veri üretmelidir. Aksi halde yazılım, ISO 45001'in sürekli iyileştirme amacına değil, yalnızca arşivleme amacına hizmet eder.

Bu makalede önerilen model, PDCA döngüsünü şu şekilde yorumlar: Plan aşamasında firma, alıcıları, karekodları, veri alanlarını ve sorumlulukları belirler; Do(yapmak) aşamasında sahadan bildirim alınır ve DÖF üretilir; Check(kontrol) aşamasında durum, hedef tarih, kapanış ve göstergeler izlenir; düzeleme aşamasında aksiyonların etkinliği değerlendirilir ve kontroller güncellenir.

4. Yakın olay yönetimi

Yakın olay, zarar doğurmamış ancak zarar doğurma potansiyeli taşıyan olay olarak ele alınır. Gnoni ve arkadaşları, yakın olayların iş kazalarını önlemede değerli bilgi kaynağı olduğunu; buna karşın yapılandırılmış yakın olay yönetim sistemlerinin sanayide sınırlı yaygınlıkta kaldığını belirtir (Gnoni et al., 2022). Bu bulgu, yazılım tasarımında yalnızca "bildir" düğmesinin değil, sınıflandırma, analiz, geri bildirim ve öğrenme yayılımının da yer alması gerektiğini gösterir.

Hepimiz biliyoruz ki iş kazaların %88 yakını kişilerden kaynaklı iken %10 yakını işletmelerden kaynaklı iken %1 veya %2 yakını ise bilinmeyen veya tahmin edilemeyen sebeplerden kaynaklanmaktadır. Biz burada işletmeden kastımız işletme yöneticisi değil işletmenin sahadaki iş akışları ile ilgilendiren konuları vurgulamaktayız. Kişilerden kastımız ise işyerinde çalışan bütün yönetici, patron, işveren, stajer dahil bütün insanların anlatılmak istenmiştir.

NIOSH destekli Demich, Haas ve McGuire çalışması, işçilerin yakın olay raporlarının potansiyel yaralanma nedenlerini görünür kıldığını ve güvenlik yönetimi girişimlerini tetikleyebileceğini gösterir. Çalışmada bir çeyrek içinde 249 yakın olay raporu analiz edilmiştir; raporların risk iletişimi ve yönetim programlarını iyileştirme potansiyeli vurgulanmıştır (Demich et al., 2020).

Heinrich güvenlik üçgeni literatürde yakın olaylara uzun süre güçlü bir teorik gerekçe sağlamıştır. Bununla birlikte modern çalışmalar, üçgenin sayısal oranlarının bağlama bağlı olduğunu ve dikkatli kullanılmasını gerektiğini gösterir. NIOSH/CDC tarafından özetlenen 25.000'den fazla işletmeye dayalı çalışma, düşük şiddetli olaylar ile fatalite olasılığı arasında ilişki bulunduğunu; ancak üçgen biçiminin olay şiddetinin nasıl sınıflandırıldığına bağlı olduğunu belirtir (CDC/NIOSH, 2018).

Bu nedenle önerilen platform, yakın olayları tek başına "kaza öncülü" olarak değil, tehlike kaynakları, kontrol zayıflıkları, davranış örüntüleri, eğitim ihtiyacı ve yönetim kör noktaları için veri kaynağı olarak ele alır.

Tehlike ile risk analiz ederek sahayı canlı tutmalıyız ve bunların daha hızlı bir bildirmi sağlanmasını amaçlamalıyız. Her ne kadar Türkiye Cumhuriyeti Devletimizde iş hukuk ve/veya iş güvenliği ve iş sağlığı hukuku süreklilik ifade etse de bazı konular saha da soyut ve uygulanması imkansızlaştırılmakta veya imkansızlaştırılmış olarak görülmektedir. Özellikle " Tehlike: İşyerinde var olan ya da dışarıdan gelebilecek, çalışanı veya işyerini etkileyebilecek zarar veya hasar verme potansiyelini," ve "Risk: Tehlikeden kaynaklanacak kayıp, yaralanma ya da başka zararlı sonuç meydana gelme ihtimalini," tanımlanmaktadır.

5. Raporlama kültürü ve güvenlik iklimi

Zohar'ın güvenlik iklimi çalışması, çalışanların güvenli davranışa verilen örgütsel önceliği nasıl algıladığını anlamak açısından klasik bir başlangıç noktasıdır (Zohar, 1980). Dijital bildirim sistemi, güvenlik iklimini doğrudan değiştirmez; ancak yönetimin raporları nasıl karşıladığı, ne kadar hızlı aksiyona dönüştürdüğü ve bildirim yapanı ne ölçüde koruduğu güvenlik iklimini güçlendirebilir veya zayıflatabilir.

OSHA'nın yakın olay raporlama politikası şablonu, yakın olayların raporlanması, kayıt altına alınması ve araştırılması gerektiğini; raporlama bilgisinin "ne oldu ve neden oldu" sorularına cevap vererek tekrarın önlenmesine yardımcı olduğunu belirtir (OSHA, 2021). Şablon ayrıca anonim bildirim ve disiplin tehdidi üretmeyen raporlama yaklaşımını vurgular. Bu, platformda anonim seçenek, açık aydınlatma metni ve sınırlı veri toplama ilkelerinin neden zorunlu olduğunu açıklar.

Literatürü, raporlama sistemlerinin tek başına kültür dönüşümü yaratmadığını gösterir. Milbank Quarterly'de yayımlanan sistematik derleme, olay bildirim sistemlerinin öğrenme için bilgi toplama yöntemi olduğunu ancak etkinliğin net olay tanımı, klinik/operasyonel sahiplik ve daha geniş güvenlik programına entegrasyonla arttığını belirtir (Howell et al., 2017). Bu bulgu İSG bağlamına uyarlandığında, yazılımın mutlaka yönetim sahipliği, aksiyon takibi ve performans göstergeleriyle desteklenmesi gerekir.

Dolayısıyla önerilen model, "bildirim sayısını artırmayı" tek başarı ölçütü yapmaz. Bildirimlerin kapanma süresi, aksiyon kalitesi, tekrar eden risk kümelerinin azalması, çalışan güveni ve geri bildirim döngüsünün görünürlüğü birlikte değerlendirilir.

6. Öncü göstergeler ve hiyerarşik kontrol

OSHA'ya göre öncü göstergeler, güvenlik ve sağlık faaliyetlerinin etkinliğini gösteren proaktif ve önleyici ölçütlerdir; buna karşılık gecikmeli göstergeler geçmişte gerçekleşmiş yaralanma, hastalık veya fatalite gibi olayları ölçer (OSHA, 2026b). Ramak kala ve tehlikeli durum bildirimleri, doğru bağlamda ele alındığında öncü gösterge olarak kullanılabilir. Ancak yalnızca saymak yeterli değildir; nitelik, risk şiddeti, aksiyona dönüşme ve kapatma kalitesi de ölçülmelidir.

NIOSH hiyerarşik kontrol yaklaşımı, tehlikeleri kontrol etmek için tercih edilen sırayı eliminasyon, ikame, mühendislik kontrolleri, idari kontroller ve kişisel koruyucu donanım olarak tanımlar (CDC/NIOSH, 2024). Bu yaklaşım DÖF algoritmasında doğrudan kullanılabilir: her aksiyon notu, yalnızca "uyarı verildi" gibi zayıf idari kontrole indirgenmemeli; mümkün olduğunda tehlikeyi ortadan kaldıran veya mühendislik kontrolüne taşıyan önlemleri teşvik etmelidir.

Önerilen platformda DÖF Word çıktısı ve firma takip formu bu nedenle yalnızca durum güncellemesi değil, kontrol etkinliği sorgulaması da içermelidir. Kritik risklerde "fotoğraf + açıklama + yer + tür + öneri" verisi, aksiyon sorumlusunun hiyerarşik kontrol mantığıyla daha güçlü çözüm seçmesini kolaylaştırır.

Gösterge türü	Örnek ölçüt	Yazılım karşılığı
Öncü	Ramak kala bildirim oranı	Karekod formundan gelen tür bazlı kayıt sayısı
Öncü	DÖF kapanma süresi	hedef_tarih, durum, kapanis_tarihi alanları
Öncü	Aksiyon kalitesi	aksiyon_notu ve hiyerarşik kontrol sınıflaması
Gecikmeli	Kaza/yaralanma oranı	Harici İSG kayıtlarıyla entegrasyon ihtiyacı

7. DÖF/CAPA ve geri bildirim yönetimi

DÖF, düzeltici ve önleyici faaliyetin Türkçe uygulama karşılığı olarak düşünülebilir. CAPA literatüründe düzeltici faaliyet mevcut uygunsuzluğun kök nedenini gidermeye, önleyici faaliyet ise benzer uygunsuzlukların ortaya çıkmasını engellemeye yönelir. Bu nedenle ramak kala ve tehlikeli durum kayıtları, henüz zarar doğmamışken önleyici faaliyet üretmek için kritik fırsat sunar.

ISO 10002:2018, kuruluşlarda ürün ve hizmetlerle ilgili şikayetlerin planlanması, tasarımı, geliştirilmesi, işletilmesi, sürdürülmesi ve iyileştirilmesi için rehberlik sağlar; şikayet işleme sürecinin genel kalite yönetim sisteminin bir parçası olabileceğini belirtir (ISO, 2026b). Platformun “Şikayet / Sorun Bildirimi” türünü de içermesi, İSG dışındaki geri bildirimlerin kalite iyileştirme döngüsüne bağlanmasını sağlar.

Bununla birlikte her geri bildirim DÖF olmak zorunda değildir. Önerilen algoritma, DÖF üretimini Ramak Kala Olayı ve Tehlikeli Durum / Davranış türleriyle sınırlar. Böylece sistem hem risk bazlı önceliklendirme yapar hem de gereksiz belge üretimiyle kullanıcıyı yormaz. Bu ayrım, uygulama başarımı açısından önemlidir: yüksek riskli bildirimler otomatik Word DÖF ile resmileştirilirken, öneri veya teşekkür türleri normal bildirim ve panel takibiyle yönetilebilir.

Bu yaklaşım, kalite yönetimi, İSG yönetimi ve müşteri/çalışan geri bildirimi arasında pratik bir köprü kurar. Makalenin önerdiği değer, DÖF’ü statik bir Word şablonu olmaktan çıkarıp olay anında fotoğraf, açıklama ve takip numarasıyla otomatik üretilen bir yönetim nesnesine dönüştürmesidir.

8. Dijital olay bildirimi

Dijital olay bildirim sistemleri, kağıt formların veya dağınık e-posta zincirlerinin ürettiği görünürlük sorunlarını azaltır. Badea ve arkadaşları laboratuvarlarda İSG amaçlı dijital olay raporlama için yapılandırılmış veri girişi, olay sınıflandırma, uyarı/alert, raporlara erişim ve takip izleme olmak üzere beş temel fonksiyon tanımlar (Badea et al., 2025). Bu beş fonksiyon, önerilen platformun çekirdek algoritmasıyla büyük ölçüde örtüşür.

Dijitalleşmenin başarısı, yalnızca teknik doğrulukla ölçülmez. Davis'in Teknoloji Kabul Modeli, algılanan fayda ve algılanan kullanım kolaylığının kullanıcı kabulünde belirleyici olduğunu ortaya koyar (Davis, 1989). Venkatesh ve arkadaşlarının UTAUT modeli ise performans beklentisi, çaba beklentisi, sosyal etki ve kolaylaştırıcı koşulların kullanım niyeti ve davranış üzerindeki rolünü vurgular (Venkatesh et al., 2003).

Bu nedenle önerilen sistem, çalışan tarafında mümkün olduğunca kısa ve mobil uyumlu form, anonim seçenek, fotoğraf yükleme kolaylığı ve KVKK aydınlatma metni sunmalıdır. Firma tarafında ise DÖF dosyasının otomatik oluşması, e-posta eki olarak gelmesi, takip alanlarının panelde görünmesi ve alıcı test ekranının bulunması algılanan faydayı artırır.

Bilgi sistemleri başarısı açısından DeLone-McLean modeli; sistem kalitesi, bilgi kalitesi, hizmet kalitesi, kullanım, kullanıcı memnuniyeti ve net fayda boyutlarıyla değerlendirme yapmayı önerir (DeLone & McLean, 2003). Platform başarımı için önerilen metrikler bu çerçeveye bağlanmıştır.

9. Bilgi güvenliği ve mahremiyet

ISO/IEC 27001:2022, bilgi güvenliği yönetim sistemleri için en bilinen standartlardan biridir ve kuruluşlara bilgi güvenliği yönetim sistemi kurma, uygulama, sürdürme ve sürekli iyileştirme konusunda rehberlik eder (ISO, 2026c). Geri bildirim platformu kişisel veri, olay fotoğrafı, firma bilgisi ve e-posta adresi işlediği için bilgi güvenliği tasarımın ayrılmaz parçasıdır.

KVKK aydınlatma yükümlülüğü rehberi, 6698 sayılı Kanun'un 10. maddesiyle veri sorumlularına kişisel verisi işlenen kişileri aydınlatma yükümlülüğü getirildiğini belirtir (KVKK, 2024). Bu nedenle formda KVKK teyidi, veri minimizasyonu, anonim seçenek ve özel nitelikli veri yazılmaması uyarıları uygulama başarısının yalnızca hukuki değil, güven ilişkisi boyutudur.

EDPB'nin Article 25 rehberi, veri korumayı tasarımdan itibaren ve varsayılan olarak ele alır (EDPB, 2020). Platform açısından bu, SMTP şifresinin public_html dışında tutulması, veri klasörüne doğrudan web erişiminin kapatılması, dosya adlarının random üretilmesi, yalnızca yetkili firmanın kendi DÖF ve eklerini indirebilmesi, gereksiz kişisel verinin alınmaması gibi teknik kararlara dönüşür.

OWASP File Upload Cheat Sheet, dosya yükleme fonksiyonlarının kötü niyetli dosyalara karşı korunması gerektiğini vurgular (OWASP, 2026). Önerilen platformda uzantı, MIME, görsel okunabilirliği, PDF imzası, boyut sınırı, güvenli klasör ve rastgele dosya adı kontrolleri bu nedenle kritik algoritmik savunmalardır.

10. Kavramsal model

Önerilen model dört aktör üzerine kuruludur: yönetici, firma yetkilisi, bildirim yapan kişi ve sistem servisleri. Yönetici firma başvurularını onaylar, firma pasifleştirme ve genel kontrol süreçlerini yürütür. Firma yetkilisi karekod üretir, alıcı e-postalarını tanımlar, gelen bildirimleri inceler ve aksiyonları kapatır. Bildirim yapan kişi sahadan anonim veya isimli kayıt oluşturur. Sistem servisleri ise dosya doğrulama, fotoğraf dönüştürme, DÖF üretme, e-posta gönderme ve denetim kaydı işlevlerini yürütür.

Şekil 1. Önerilen sistemin kavramsal akışı

```
Firma Kaydı -> E-posta Doğrulama -> Admin Onayı -> Firma Paneli
Firma Paneli -> Alıcı Tanımı -> Karekod Tokeni -> Saha Bildirimi
Saha Bildirimi -> Dosya Doğrulama -> Bildirim Kaydı -> Takip No
Tür = Ramak Kala / Tehlikeli Durum ise -> DÖF Word + JPG Ekleri
E-posta Gönderimi -> Panel Takibi -> Aksiyon -> Kapanış -> Denetim Kaydı
```

Mimarinin temel tasarım ilkesi, kritik iş mantığını sunumdan ayırmak ve ortak fonksiyonları çekirdek kütüphanede toplamaktır. Veritabanı bağlantısı, şema migrasyonu, güvenlik başlıkları, CSRF kontrolü, e-posta gönderimi, dosya yükleme ve DÖF üretimi lib.php içinde merkezileştirilmiştir. Böylece farklı ekranlar aynı doğrulama ve güvenlik politikasını kullanır.

Bu mimari küçük işletme ortamlarına uygundur çünkü SQLite, saf PHP ve SMTP ile çalışabilir. Composer, Node veya özel sunucu servisi gerektirmemesi dağıtım başarımını artırır. Bunun karşılığında ölçek çok büyüdüğünde raporlama, indeksleme ve arşivleme için daha gelişmiş veritabanı ve arka plan iş kuyruğu gerekebilir.

11. Veri modeli

Veri modeli, izlenebilirlik ve veri minimizasyonu arasında denge kurar. Firma bilgileri firmalar tablosunda; bildirimler, dosya adları, DÖF dosyası ve takip alanları bildirimler tablosunda; anlık e-posta alıcıları alicilar tablosunda; sistem olayları denetim tablosunda tutulur. Bu yapı, her bildirimin firma_id ile sahiplenilmesini sağlar ve yetkisiz erişim riskini azaltır.

Varlık	Ana alanlar	İşlev
firmalar	firma_adi, ticari_unvan, yetkili_ad, email, vergi_no, firma_email, onaylandi, aktif, feedback_token	Firma kimliği, hesap durumu, ana e-posta ve karekod bağlantısı.
bildirimler	takip_no, turler, baslik, aciklama, dosya, dof_dosya, durum, sorumlu, hedef_tarih, aksiyon_notu, kapanis_notu	Saha bildirimi, DÖF dosyası, ekler ve aksiyon/kapanış takibi.
alicilar	firma_id, email	Firma bazlı anlık bildirim alıcıları.
denetim	kim, islem, detay, ip, zaman	Kayıt, hata, e-posta ve yönetim işlemleri için hesap verebilirlik izi.

Takip numarası GB-YIL-SIRA formatındadır. Bu biçim, hem e-postada hem panelde hem DÖF dosya adında kullanılabilir. Kullanıcılar açısından hatırlanabilir; yönetim açısından arşivlenebilir; teknik açıdan bildirimin id alanına bağlanabilir.

DÖF dosyası ve ekler web kökünde doğrudan erişilebilir URL olarak sunulmaz. Kullanıcı dosyaya dof.php veya dosya.php üzerinden ulaşır; bu uçlar önce oturumu ve firma sahipliğini doğrular, sonra dosyayı indirir. Bu yaklaşım ISO/IEC 27001 ve veri koruma ilkeleriyle uyumlu yetki kontrolü sağlar.

12. Algoritma 1: Firma yaşam döngüsü

Firma yaşam döngüsü, sahadan bildirim alınmadan önce güvenli bir organizasyon kimliği kurulmasını sağlar. Bu aşamada firma adı ve ticari ünvanın alınması, DÖF belgesinin kurumsal bağlamla üretilmesini sağlar. Yetkili e-postası doğrulanmadan ve yönetici onayı verilmeden firma karekod üretemez.

```
Girdi: firma_adi, ticari_unvan, yetkili_ad, email, vergi_no, firma_email, telefon,
adres
1. Alanları temizle ve zorunlu alanları doğrula.
2. email ve firma_email için format kontrolü yap.
3. vergi_no değerini 10-11 haneli rakam olarak doğrula.
4. Aynı email veya vergi_no ile doğrulanmış kayıt var mı kontrol et.
5. Yoksa doğrulama_token ve doğrulama_biter üret.
6. Kayıt veritabanına transaction içinde yaz.
7. Doğrulama e-postası gönder.
8. E-posta başarısızsa rollback yap; başarılıysa commit yap.
9. Kullanıcı doğrulama linkini açınca geçici parola üret.
10. Admin onay verirse firma aktif ve onaylı hale gelir.
```

Bu algoritmada e-posta gönderimi transaction kararını etkiler. Kayıt doğrulama e-postası gönderilemezse başlatılmış sayılmaz. Bu tercih, sistemin “kayıt var ama kullanıcı doğrulayamıyor” gibi yarı-bozuk durumlar üretmesini önler.

Güvenlik açısından kurulum anahtarı ve SMTP şifresi config.php içinde değil, public_html dışındaki fb-secrets.php içinde tutulur. Bu karar, yanlışlıkla webden okunabilir dosya içinde gizli değer bırakma riskini azaltır.

13. Algoritma 2: Token tabanlı saha erişimi

Karekod algoritmasının amacı, her firmaya tahmin edilemeyen ve iptal edilebilir bir saha bağlantısı vermektir. Bağlantı firma kimliğini açıkça taşımak yerine random token taşır. Böylece URL tahmin edilerek başka firmaların formlarına erişim riski düşer.

```
Girdi: firma oturumu
1. Firma giriş yapmış mı kontrol et.
2. Firma aktif ve onaylı mı kontrol et.
3. feedback_token yoksa veya yenileme istenirse random 64 hex token üret.
4. Tokeni firmalar.feedback_token alanına yaz.
5. URL = SITE_URL + /geribildirim.php?token=TOKEN olarak oluştur.
6. Karekod bu URL üzerinden üretilir.
7. Admin firmayı pasife alırsa feedback_token NULL yapılır.
```

Form açılışında token_gecerli kontrolü önce formatı doğrular. Ardından veritabanında tokene karşılık gelen aktif ve onaylı firma aranır. Bu iki aşamalı doğrulama hem kaba hatalı URL girişlerini hem de pasifleştirilmiş firmalara ait eski karekodları engeller.

Uygulama başarımı açısından tokenin iptal edilebilir olması önemlidir. Firma kapanmış, sözleşme bitmiş veya kötüye kullanım yaşanmışsa eski saha afişlerinin çalışmaya devam etmemesi gerekir. Bu, operasyonel kontrolün yazılım algoritmasına taşınmış halidir.

14. Algoritma 3: Bildirim alma

Bildirim alma algoritması, çalışan veya ziyaretçinin sahadan minimum sürtünmeyle veri girmesini hedefler. Form; anonim seçenek, ad/iletişim/departman, bildirim türü, başlık, olay tarihi, olay yeri, açıklama, öneri ve ekler alanlarından oluşur. Bildirim türleri arasında Ramak Kala Olayı ve Tehlikeli Durum / Davranış kritik DÖF tetikleyicileridir.

```
Girdi: token, form alanları, fotolar[]
1. Token formatını kontrol et.
2. Firma aktif/onaylı mı doğrula.
3. CSRF ve KVKK teyidini kontrol et.
4. Bildirim türü, başlık ve açıklama zorunlu mu kontrol et.
5. Anonim seçildiyse kimlik alanlarını boşalt.
6. Dosyaları ek_dosyalarini_kaydet algoritmasına gönder.
7. Hata yoksa bildirimler tablosuna kayıt yaz.
8. bid değerinden takip_no üret: GB-YIL-000001.
9. DÖF karar algoritmasını çağır.
10. Alıcılara e-posta gönder.
11. Bildiren e-posta yazmışsa alındı teyidi gönder.
```

Sınıflandırma algoritmasının başarısı, tür listesinin pratik ve anlaşılır olmasına bağlıdır. Çok fazla kategori çalışanı yorar; çok az kategori ise analiz değerini düşürür. Önerilen liste, İSG riskleri ile genel geri bildirimleri ayırır: Ramak Kala, Tehlikeli Durum/Davranış, Şikayet/Sorun, Öneri/İyileştirme, Teşekkür/Memnuniyet ve Diğer.

Bu aşamada sistemin en önemli etik kararı anonimliktir. Anonim seçildiğinde ad, iletişim ve departman sistemde saklanmaz. Bu özellik, raporlama kültürünü güçlendirmek ve misilleme korkusunu azaltmak için tasarlanmıştır.

15. Algoritma 4: Fotoğraf ve ek işleme

Fotoğraf kanıtı, olayın anlaşılmasını hızlandırır; ancak yüksek çözünürlüklü fotoğraflar e-posta teslimatını bozabilir, depolama maliyetini artırabilir ve gereksiz veri işleme riski doğurabilir. Bu nedenle algoritma, JPG/JPEG/PNG görselleri taşınabilir ve hafif JPG formatına dönüştürür. PDF dosyaları ise imza kontrolü sonrası saklanır fakat görsele çevrilmez.

```
Girdi: fotolar[]
1. Dosya sayısı MAKS_FOTO sınırını aşıyor mu kontrol et.
2. Her dosya için upload hata kodunu kontrol et.
3. Boyut <= MAX_DOSYA_MB mi kontrol et.
4. Uzantı yalnızca jpg, jpeg, png, pdf olabilir.
5. MIME türü uzantıyla uyumlu mu kontrol et.
6. Görsel ise getimagesize ile okunabilirliği doğrula.
7. PDF ise ilk 4 byte %PDF mi kontrol et.
8. Görsel ise random_ad.jpg oluştur.
9. GD varsa EXIF orientation düzelt, genişliği FOTO_MAX_GENISLIK değerine indir,
FOTO_JPEG_KALITE ile kaydet.
10. Hata çıkarsa bu denemede kaydedilen dosyaları sil.
```

OWASP'ın dosya yükleme rehberi, dosya yükleme fonksiyonlarının kötü niyetli dosyalara karşı açık hedef olduğunu vurgular (OWASP, 2026). Bu nedenle yalnızca uzantıya güvenmek yeterli değildir. MIME kontrolü, görsel okunabilirlik kontrolü, PDF imza kontrolü, random dosya adı ve webden doğrudan erişilemeyen güvenli saklama dizini birlikte uygulanmalıdır.

Bu algoritma aynı zamanda e-posta başarımını artırır. MAIL_EK_MAX_MB sınırı, DÖF Word dosyası ve fotoğrafların toplam boyutunun SMTP sunucularında reddedilmesini önlemek için kullanılır. Fotoğrafların "WhatsApp benzeri hafif" formata dönüştürülmesi bu nedenle hem kullanıcı deneyimi hem teslimat başarısı açısından gereklidir.

16. Algoritma 5: DÖF üretimi

DÖF üretim algoritması risk bazlıdır. Her bildirim Word belgesine dönüştürülmez. Yalnızca Ramak Kala Olayı veya Tehlikeli Durum / Davranış türü seçildiğinde DÖF kapsamı başlar. Böylece sistem kritik riskleri resmileştirirken öneri, teşekkür veya genel şikayet gibi kayıtları gereksiz belge yüküyle ağırlaştırmaz.

```
Girdi: firma, bildirim, dosyalar[]
1. turler içinde Ramak Kala veya Tehlikeli Durum var mı kontrol et.
2. Yoksa dof_dosya boş kalır; normal bildirim akışı devam eder.
3. Varsa DATA_DIR/dof altında takip_no-DOF.docx hedefi oluştur.
4. Word içeriğine firma adı, ticari ünvan, yetkili, takip no, tür, olay yeri, olay
tarihi, bildiren, açıklama ve öneri yaz.
5. JPG fotoğrafları Word dosyasına göm.
6. ZipArchive varsa docx üret; yoksa Word uyumlu doc yedeği üret.
7. Başarılıysa bildirimler.dof_dosya alanını güncelle.
8. Başarısızsa denetim kaydı yaz; bildirim kaydını silme.
```

Bu karar, DÖF'ü operasyonel olarak sürdürülebilir hale getirir. Literatürde yakın olay yönetim sistemlerinin toplama, analiz ve bilginin yayılımı süreçlerinden oluştuğu belirtilir (Gnoni et al., 2022). Word DÖF çıktısı bu zincirin "analiz ve yayılım" aşamasına hizmet eder: e-posta eki olarak karar vericilere gider ve panelde indirilebilir kayıt olarak kalır.

DÖF dosyasının içinde ilk değerlendirme metni bulunur: sorumlu atanmalı, kök neden analizi yapılmalı ve faaliyet kapatma notu ile sonuçlandırılmalıdır. Bu ifade, belgenin yalnızca olay anlatımı değil, aksiyon çağrısı olduğunu açıkça gösterir.

17. Algoritma 6: E-posta gönderimi

E-posta algoritmasının amacı, bildirimin doğru kişilere zamanında ve güvenilir biçimde ulaşmasını sağlamaktır. Sistemde üç mod vardır: smtp canlı gönderim, mail sunucu mail() fonksiyonu ve file test modu. Canlı kullanımda SMTP tercih edilir; çünkü kimlik doğrulama, gönderici tutarlılığı ve hata mesajı okunabilirliği daha yüksektir.

```
Girdi: alıcılar, konu, gövde, ekler[]
1. MAIL_GONDEREN adresini ayıkla ve doğrula.
2. Alıcı e-postasını doğrula.
3. Eklerin okunabilirliğini ve toplam boyutunu kontrol et.
4. MAIL_MODE = smtp ise SMTP_HOST, PORT, SECURE, KULLANICI, SIFRE değerlerini kontrol
et.
5. SSL/TLS kuralına göre bağlantı aç.
6. AUTH LOGIN ile kimlik doğrula.
7. MIME multipart mesajı oluştur.
8. DÖF varsa Word ve JPG fotoğrafları ekle.
9. Başarısız gönderimi denetim tablosuna yaz.
```

Alıcı listesi iki kaynaktan oluşur: firma kaydındaki firma_email ve alicilar tablosundaki anlık bildirim adresleri. Liste tekilleştirilir. Bu, hem ana firma e-postasına hem de İSG sorumlusu, saha yöneticisi veya kalite birimi gibi ilgili taraflara bildirim gitmesini sağlar.

SMTP şifresi config.php içinde tutulmaz. public_html dışındaki fb-secrets.php veya ortam değişkeni kullanılır. Bu tercih, ISO/IEC 27001'in risk temelli bilgi güvenliği yaklaşımı ve NIST CSF'nin yönetişim-koruma mantığıyla uyumlu bir kontrol olarak değerlendirilebilir (ISO, 2026c; NIST, 2024).

18. Algoritma 7: Takip ve kapatma

Raporlama sistemlerinin etkisi, kayıt alındıktan sonra başlar. Firma panelinde her bildirim takip numarası, tür, durum, bildiren bilgisi, olay yeri, ekler, DÖF Word bağlantısı ve aksiyon alanlarıyla listelenir. Firma yalnızca kendi firma_id değerine bağlı kayıtları görür.

```
Girdi: bildirim_id, durum, sorumlu, hedef_tarih, aksiyon_notu, kapanis_notu
1. Firma oturumunu doğrula.
2. Bildirim firma_id ile eşleşiyor mu kontrol et.
3. durum ∈ {Açık, İşlemde, Kapalı} mı kontrol et.
4. hedef_tarih YYYY-AA-GG formatında mı kontrol et.
5. Durum Kapalı ve kapanis_tarihi boşsa kapanis_tarihi = şimdi.
6. Durum Kapalı değilse kapanis_tarihi temizlenir.
7. Sorumlu, hedef tarih, aksiyon ve kapanış notu kaydedilir.
8. Denetim kaydı oluşturulur.
```

Bu algoritma, DÖF'ü yaşayan bir takip nesnesine dönüştürür. Klasik uygulamalarda Word DÖF dosyası e-postada kalır ve süreç dağılır. Önerilen modelde Word dosyası belge niteliğini sağlar; panel alanları ise canlı takip ve kapanış disiplinini sağlar.

Kapanış tarihi yalnızca Kapalı durumunda atanır. Kayıt yeniden Açık veya İşlemde yapılırsa kapanış tarihi temizlenir. Bu karar, sahada yanlışlıkla kapatılan kayıtların tekrar sürece alınabilmesini sağlar ve metriklerin gerçeğe daha yakın kalmasına yardım eder.

19. Başarım modeli

Başarım modeli üç düzeyde kurulmalıdır: sistem başarımı, süreç başarımı ve İSG öğrenme başarımı. Sistem başarımı, yazılımın çalışabilirliği ve kullanıcı deneyimiyle ilgilidir. Süreç başarımı, kayıtların aksiyona dönüşmesi ve kapanmasıyla ilgilidir. İSG öğrenme başarımı ise tekrar eden risklerin azalması, yönetim görünürlüğünün artması ve çalışan katılımının güçlenmesiyle ilgilidir.

Boyut	Ölçüt	Hedef yorum
Sistem kalitesi	Form gönderim başarı oranı, e-posta teslim hata oranı, ek boyutu reddi	Teknik sürtünme düştükçe kullanım artar.
Bilgi kalitesi	Eksiksiz başlık/açıklama oranı, fotoğraf ekli kritik bildirim oranı	Daha iyi veri daha iyi aksiyon üretir.
Süreç kalitesi	DÖF üretim oranı, ortalama kapanış süresi, hedef tarihi aşan kayıt oranı	Yönetim sahipliği görünür hale gelir.
Kültür etkisi	Anonim/isimli bildirim dengesi, tekrar bildirim yapan kullanıcı oranı	Güven ve katılım hakkında sinyal verir.
Net fayda	Tekrarlayan tehlike kümelerinde azalma, kontrol iyileştirme sayısı	İSG öğrenme değerini temsil eder.

DeLone-McLean modelindeki sistem kalitesi, bilgi kalitesi, hizmet kalitesi, kullanım, kullanıcı memnuniyeti ve net fayda boyutları, platformun başarı ölçümünde kullanılabilir (DeLone & McLean, 2003). Ancak İSG bağlamında net fayda yalnızca kullanım sayısı değildir; risk azaltma ve öğrenme etkisiyle birlikte değerlendirilmelidir.

OSHA'nın öncü göstergeler yaklaşımı da bu ayrımı destekler: iyi bir program, değişimi sürmek için öncü göstergeleri, etkinliği ölçmek için gecikmeli göstergeleri birlikte kullanır (OSHA, 2026b).

20. Uygulama başarımı

Yazılım teknik olarak doğru olsa bile çalışanlar kullanmazsa etkisiz kalır. TAM ve UTAUT literatürü bu noktada yararlıdır. Algılanan fayda, çalışan ve firma açısından net olmalıdır: bildirim kolay yapılacak, kimlik gizlenebilecek, fotoğraf kanıtı eklenebilecek, yönetim bildirimi görecek ve aksiyon kapanışı izlenebilecektir. Algılanan kullanım kolaylığı ise formun kısa, mobil uyumlu ve anlaşılır olmasıyla sağlanır.

Uygulama planı aşamalı olmalıdır. İlk aşamada admin kurulumu, SMTP testi, firma kaydı ve alıcı testleri yapılır. İkinci aşamada sınırlı bir pilot alanda karekod afişi kullanılır. Üçüncü aşamada gelen ilk kayıtlar birlikte incelenir ve DÖF çıktıları kontrol edilir. Dördüncü aşamada sorumlu-hedef tarih-kapanış disiplini yöneticilerle netleştirilir. Beşinci aşamada KPI panosu ve aylık yönetim değerlendirmesi devreye alınır.

Aşama	Faaliyet	Başarı işareti
Hazırlık	SMTP, gizli dosya, GD/ZipArchive, admin kurulumu	E-posta testi ve DÖF üretim testi başarılı.
Pilot	Tek saha veya tek departmanda karekod kullanımı	İlk 10 kayıt sorunsuz alınır.
Eğitim	Anonimlik, KVKK, bildirim türleri ve fotoğraf örnekleri anlatılır	Çalışanlar neyi bildireceğini bilir.
Yönetim	DÖF atama ve kapanış sorumluları belirlenir	Hedef tarihi geçen kayıtlar takip edilir.
İyileştirme	Aylık tekrar eden risk analizi yapılır	Aksiyonlar hiyerarşik kontrol mantığına taşınır.

21. Test ve doğrulama

Uygulama başarımı yüksek bir sistem için test, yalnızca “sayfa açılıyor mu” kontrolü değildir. Test senaryoları iş akışını, güvenliği, dosya işleme mantığını, e-posta eklerini, DÖF üretimini, yetkilendirmeyi ve kapanış metriklerini kapsamalıdır.

Test alanı	Senaryo	Beklenen sonuç
Kayıt	Firma adı ve ticari ünvanla kayıt oluşturulur	Doğrulama e-postası gelir; doğrulanmadan giriş olmaz.
SMTP	E-posta test ekranı çalıştırılır	SMTP_SIFRE tanımlı, gönderim başarılı.
Token	Pasif firmanın karekodu açılır	Geçersiz bağlantı mesajı döner.
Fotoğraf	PNG fotoğraf eklenir	JPG olarak sıkıştırılmış dosya saklanır.
DÖF	Ramak Kala seçilerek bildirim gönderilir	Word DÖF üretilir, e-postaya eklenir.
Yetki	Başka firma bildirimi indirmeye çalışılır	404 veya erişim reddi davranışı oluşur.
Kapanış	Durum Kapalı yapılır	kapanis_tarihi otomatik atanır.

Testlerin gerçek veriyle yapılması sırasında kişisel veri içermeyen örnek fotoğraflar kullanılmalıdır. Canlı sistemde test bildirimi atılırken konu başlığına TEST yazılması, daha sonra raporlamada ayrıştırma kolaylığı sağlar. Veri koruma açısından test dosyalarının düzenli silinmesi de bakım planına dahil edilmelidir.

DÖF Word çıktısı ayrıca elle açılarak kontrol edilmelidir: Türkçe karakterler, fotoğraf görünümü, takip numarası, firma adı, ticari ünvan ve olay açıklaması doğru olmalıdır. ZipArchive kapalı sunucularda .doc yedeği oluşacağı için canlı hostingte PHP zip eklentisinin açık olması tavsiye edilir.

22. Risk analizi

Dijital İSG bildirim sistemi hem operasyonel hem teknik riskler taşır. Operasyonel riskler; bildirim yapmama, yanlış sınıflandırma, aksiyonların kapanmaması, yönetim sahipliğinin zayıf kalması ve çalışan güveninin oluşmaması gibi konulardır. Teknik riskler ise SMTP hataları, dosya yükleme açıkları, kişisel veri sızıntısı, yanlış yetkilendirme, yedekleme eksikliği ve sunucu eklenti uyumsuzluklarıdır.

Risk	Etkisi	Kontrol
Bildirim yapılmaması	Sistem görünür risk üretmez	Anonimlik, eğitim, yönetim geri bildirimi, kolay karekod erişimi.
DÖF kapanmaması	Öğrenme döngüsü tamamlanmaz	Sorumlu, hedef tarih, geciken kayıt raporu.
SMTP başarısızlığı	Bildirim zamanında ulaşmaz	E-posta test ekranı, Track Delivery kontrolü, SPF/DKIM doğrulama.
Zararlı dosya yükleme	Web güvenliği riski	Uzantı/MIME/imza kontrolü, random ad, web dışı saklama.
Gizli değer sızıntısı	Hesap ele geçirme riski	SMTP_SIFRE ve kurulum anahtarı public_html dışında.
Veri kaybı	Kayıt ve DÖF arşivi kaybolur	SQLite ve data klasörü yedekleme planı.

NIST CSF 2.0; Govern, Identify, Protect, Detect, Respond ve Recover fonksiyonlarıyla siber risk yönetimi sonuçlarını düzenler (NIST, 2024). Platform kontrol planı bu mantığa bağlanabilir: yönetişim için yetki ve politika, tanımlama için veri varlıkları, koruma için dosya ve gizli değer kontrolleri, tespit için denetim kaydı, yanıt için hata yönetimi, kurtarma için yedekleme.

22.1 Mevzuat ve hukuk uyum katmanı

Dijital İSG geri bildirim platformunun başarısı yalnızca teknik çalışabilirliğe değil; iş güvenliği hukukunun öngördüğü önleme, belgelendirme, çalışan katılımı, risk değerlendirmesi ve takip yükümlülüklerini desteklemesine bağlıdır. Bu nedenle ramak kala ve tehlikeli durum kayıtları, hukuki izlenebilirliği olan önleyici faaliyet girdisi olarak işlenmelidir.

Türkiye bakımından çekirdek çerçeve 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği, 6698 -KVKK ve 7545 sayılı Siber Güvenlik Kanunu ile birlikte okunmalıdır. Uluslararası bağlamda EU OSH Framework Directive 89/391/EEC, ILO C155/C187, GDPR ve NIS2 Direktifi karşılaştırmalı ölçüt sağlar.

Hukuki tasarım ilkesi

Uyum, forma birkaç onay kutusu eklemek değildir. Uyum; verinin neden toplandığını, kimin görebileceğini, ne kadar saklanacağını, hangi bildirimin DÖF oluşturacağını, hangi olayda yöneticiye bildirim gideceğini ve kapanış kanıtının nasıl tutulacağını baştan tasarlayan algoritmik bir disiplindir.

Bu nedenle yazılım, işverenin veya İSG profesyonelinin hukuki sorumluluğunu devralmaz; fakat sorumluluğun yerine getirilip getirilmediğini gösterebilen düzenli kayıt, aksiyon ve denetim izi üretir.

22.1.1 Mevzuat uyum matrisi

Çerçeve	Temel gereklilik	Platform karşılığı
6331 sayılı Kanun	Önleme, bilgilendirme, katılım ve güvenli çalışma düzeni.	Kolay bildirim, DÖF, sorumlu, hedef tarih, kapanış notu.
Risk Değerlendirmesi Yönetmeliği	Tehlike belirleme, risk analizi, kontrol tedbiri, dokümantasyon.	Tür, risk sınıfı, fotoğraf kanıtı, aksiyon ve doğrulama.
KVKK / GDPR	Amaçla sınırlılık, veri minimizasyonu, güvenli saklama.	Anonim seçenek, yetki ayrımı, web dışı ek saklama.
7545 / NIS2	Siber risk yönetimi, olay etkisini azaltma, süreklilik.	TLS, gizli dosya, log, yedek, giriş deneme sınırı.
EU 89/391 / ILO C155-C187	Önleme, çalışan katılımı, eğitim ve sürekli iyileştirme.	Cezasız bildirim dili, geri dönüş, metrik ve yönetim gözden geçirmesi.

Matrisin amacı, mevzuatı yazılıma birebir çevirmek değil; yazılımın üretmesi gereken karar izini görünür kılmaktır. Canlı uygulamada her firma kendi sektörüne, tehlike sınıfına ve İSG profesyoneli değerlendirmesine göre ek alanlar tanımlayabilir.

22.2 Risk değerlendirmesi yönetmeliği ile algoritmik bağı

İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği, 29.12.2012 tarihli ve 28512 sayılı Resmi Gazete'de yayımlanmış; işyerlerinde İSG yönünden yapılacak risk değerlendirmesinin usul ve esaslarını düzenlemiştir. Yönetmeliğin 6331 sayılı Kanun kapsamındaki işyerlerini esas alması, platformun firma temelli veri modelini doğrudan anlamlı kılar.

Algoritmanın "bildirim al, e-posta gönder, arşivle" düzeyinde kalması yeterli değildir. Kritik bildirim; tehlike tanımı, mevcut durum, kanıt, önerilen kontrol tedbiri, sorumlu kişi, hedef tarih, gerçekleşen aksiyon ve kapanış doğrulaması alanlarıyla risk değerlendirmesi döngüsüne bağlanmalıdır.

Algoritma 8: Mevzuata bağlı risk değerlendirme güncellemesi

```
Girdi: bildirim_turu, aciklama, dosyalar, firma_id, risk_skoru, dof_id
1. Tür Ramak Kala veya Tehlikeli Durum ise kayıt kritik sınıfa alınır.
2. Fotoğraf JPEG/JPG formatına dönüştürülür ve dosya bütünlüğü doğrulanır.
3. Olay; tehlike kaynağı, etkilenebilecek kişiler ve mevcut kontrol bilgisiyle
etiketlenir.
4. Risk seviyesi yoksa firma panelinde tamamlanması zorunlu alan açılır.
5. DÖF kaydı; sorumlu, hedef tarih ve önerilen tedbir olmadan kapatılamaz.
6. Kapanışta alınan tedbir ve doğrulama notu kaydedilir.
7. Risk değerlendirme envanterine güncelleme gereksinimi işaretlenir.
8. Tüm değişiklikler denetim kaydına yazılır.
```

Bu algoritma, resmi risk değerlendirmesi belgesinin yerine geçmez; fakat risk değerlendirmesinin canlı tutulmasını destekleyen kanıt, aksiyon ve izlenebilirlik altyapısını oluşturur.

22.3 İş güvenliği hukuku, kişisel veri ve siber güvenlik bağı

6331 sayılı İş Sağlığı ve Güvenliği Kanunu, işyerlerinde İSG'nin sağlanması ve mevcut şartların iyileştirilmesi için işveren ve çalışanların görev, yetki, sorumluluk, hak ve yükümlülüklerini düzenler. Platform bu bağlamda işverenin önleyici organizasyon kurma, riskleri izleme ve çalışan bildirimlerini aksiyona dönüştürme kapasitesini artıran yardımcı bir yönetim aracıdır.

7545 sayılı Siber Güvenlik Kanunu, 19.03.2025 tarihli ve 32846 sayılı Resmi Gazete'de yayımlanmış; siber tehditlerin tespiti ve bertarafı, siber olayların etkilerinin azaltılması ve kurum/kişilerin siber saldırılara karşı korunması için çerçeve oluşturmuştur. Platform kişisel veri, fotoğraf, e-posta ve firma bilgisi işlediği için siber güvenlik mantığıyla tasarlanmalıdır.

KVKK ve GDPR bakımından fotoğraflar kişisel veri içerebilir; yüz, plaka, kimlik kartı, çalışma alanı veya konum bilgisi olay kanıtına istemeden girebilir. Bu nedenle veri minimizasyonu, yetki ayrımı, saklama süresi, anonim bildirim ve gerektiğinde maskeleme/erişim kısıtlama süreçleri desteklenmelidir.

Teknik karşılık açıktır: SMTP şifreleri public_html altında tutulmamalı, dosya yükleme uçları MIME/uzantı/boyut kontrolü yapmalı, ekler doğrudan URL ile indirilememeli, oturumlar zaman aşımına uğramalı, giriş denemeleri sınırlandırılmalı ve TLS doğrulaması açık kalmalıdır.

22.3.1 Hukuki/teknik kontrol matrisi

Risk	Anlamı	Önerilen kontrol
Aşırı veri toplama	Amaçla sınırlılık ve minimizasyon riski.	Zorunlu alanları azalt; kimliği opsiyonel tut; fotoğraf sınırı uygula.
Yetkisiz dosya erişimi	Fotoğraf ve DÖF kayıtları kişisel/ticari bilgi içerebilir.	Ekleri web kökü dışında tut; indirmeyi yetkili PHP uçlarıyla yap.
SMTP sırrı sızıntısı	E-posta hesabı ve alan adı itibarı zarar görebilir.	Şifreyi fb-secrets.php içinde sakla; uygulama şifresi ve TLS kullan.
Kapanmayan aksiyon	Önleyici faaliyet tamamlanmadan kayıt kapanmış görünür.	Sorumlu, hedef tarih ve kapanış notu olmadan kapatma yaptırma.
Kayıt bütünlüğü	Denetimde işlem geçmişi açıklanamaz hale gelir.	Denetim kaydı, zaman damgası, firma-id ve kullanıcı-id tut.

Bu kontrol matrisi, yazılımın hukuk metinlerini otomatik uyguladığı anlamına gelmez. Ama canlı sistemin, hukuki değerlendirme yapan kişiye güvenilir veri, kanıt ve işlem geçmişi sunmasını sağlar.

22.4 Uluslararası mevzuat ve karşılaştırmalı çerçeve

Uluslararası çerçeve Türkiye mevzuatının yerine geçmez; fakat platformun daha olgun, denetlenebilir ve çok paydaşlı çalışma düzenine uygun tasarlanması için karşılaştırma zemini sağlar. EU OSH Framework Directive 89/391/EEC, işveren yükümlülüğünü önleme, bilgilendirme, danışma, çalışan katılımı ve eğitim ilkeleriyle kurar. ILO C155 ve C187 ise güvenli çalışma ortamı hakkını ve sürekli iyileştirme yaklaşımını güçlendirir.

Siber güvenlik ve veri koruma tarafında GDPR, kişisel verilerin korunması için genel çerçeveyi kurarken; NIS2 Direktifi Avrupa Birliği genelinde yüksek ortak siber güvenlik seviyesi hedefler. Avrupa ile çalışan veya tedarik zincirinde yer alan firmalar için bu iki düzenleme, olay yönetimi ve veri güvenliği açısından karşılaştırmalı tasarım ölçütleri sunar.

Uygulama önerisi olarak canlı sistemde “Mevzuat Uyum Notu” alanı eklenmeli; firma yöneticisi her DÖF için uygulanacak kontrol tedbirini, kapanış kanıtını ve gerekiyorsa risk değerlendirme dokümanının güncellenip güncellenmediğini işaretlemelidir.

22.4.1 Karşılaştırmalı uygulama matrisi

Kaynak	Makaledeki karşılığı	Uygulama etkisi
EU 89/391/EEC	Önleme, bilgilendirme, danışma, katılım.	Cezasız bildirim dili ve yönetim geri dönüşü benimsemeyi artırır.
ILO C155	İş kazası ve sağlığa zarar veren durumları önleme.	Ramak kala verisi önleyici risk girdisine dönüşür.
ILO C187	Ulusal sistem, program ve sürekli iyileştirme.	Panel metrikleri ve kapatma oranları yönetim gözden geçirmesine veri sağlar.
GDPR	Veri minimizasyonu, güvenlik, hesap verebilirlik.	Anonim bildirim, sınırlı erişim ve saklama politikası güven üretir.
NIS2	Siber risk yönetimi, olay bildirimi, süreklilik.	Loglama, yedekleme, SMTP güvenliği ve olay müdahalesi güçlenir.

Sonuç olarak uluslararası mevzuat, platformun yalnızca yerel kuruluma değil; daha yüksek güvenlik, veri koruma ve yönetim sistemi beklentilerine de hazırlanmasını sağlar.

23. Tartışma

Önerilen modelin temel katkısı, yakın olay bildirimini yazılım, belge ve yönetim aksiyonu düzeyinde birleştirmesidir. Çoğu küçük işletmede bildirimler WhatsApp mesajı, e-posta veya kağıt form olarak dağınık ilerler. Bu model, aynı veriyi tek takip numarası altında toplar; kritik türleri otomatik DÖF dosyasına dönüştürür; fotoğrafı hafif ve taşınabilir hale getirir; e-postayla hızlı dağıtım sağlar; panelde kapanış disiplinini korur.

İkinci katkı, uygulanabilirliktir. Saf PHP ve SQLite mimarisi, küçük ve orta ölçekli hosting ortamlarında hızlı devreye alınabilir. Bu, teknoloji kabulü açısından kolaylaştırıcı koşulları güçlendirir. Ancak aynı tercih çok yüksek hacimli kurumsal yapılarda sınırlılık doğurabilir. Büyük ölçekli kullanımda PostgreSQL/MySQL, kuyruk tabanlı e-posta, rol bazlı yetki matrisi, gelişmiş raporlama ve arşivleme gerekebilir.

Üçüncü katkı, güvenlik ve mahremiyetin iş akışına gömülmesidir. Anonim bildirim, KVKK aydınlatması, gizli dosya ayrımı, güvenli ek saklama ve yetkili indirme uçları yalnızca teknik ayrıntı değil, raporlama kültürünün ön şartlarıdır.

Sınırlılıklar da açıktır. Bu çalışma saha pilot verisi içermez; dolayısıyla gerçek kaza oranı azaltımı iddia etmez. Yakın olay sayısındaki artış her zaman risk artışı anlamına gelmeyebilir; güven artışı ve raporlama kültürünün güçlenmesi de sayıyı artırabilir. Bu nedenle metrikler yorumlanırken nitel değerlendirme ve yönetim görüşmesiyle birlikte kullanılmalıdır.

24. Sonuç

Ramak kala ve tehlikeli durum bildirimleri, İSG yönetiminde erken uyarı ve öğrenme fırsatı sunar; ancak bu fırsatın kurumsal değere dönüşmesi için 6331 sayılı Kanun, Risk Değerlendirmesi Yönetmeliği, KVKK, 7545 sayılı Siber Güvenlik Kanunu ve uluslararası İSG/siber güvenlik çerçeveleriyle uyumlu bir kayıt ve aksiyon düzenine bağlanması gerekir. Ancak bu fırsatın değere dönüşmesi için bildirimlerin kolay yapılması, güvenle paylaşılması, doğru sınıflandırılması, kanıtla desteklenmesi, kritik türlerde DÖF'e dönüşmesi, ilgili .

Bu makale, omerdogu.com geri bildirim platformu için literatür temelli ve uygulanabilir bir algoritmik model önermiştir. Model; ISO 45001'in önleyici yönetim mantığına, ISO 10002'nin geri bildirim süreçlerine, ISO/IEC 27001'in bilgi güvenliği yaklaşımına, OSHA/NIOSH'un öncü gösterge ve hiyerarşik kontrol çerçevesine, OWASP'ın güvenli dosya yükleme kontrollerine ve teknoloji kabul literatürünün uygulama başarısı değişkenlerine bağlanmıştır.

Uygulama için en kritik öneriler şunlardır: canlı sistemde SMTP ayarları düzenli test edilmeli; GD ve ZipArchive eklentileri açık olmalı; firma alıcıları tanımlanmalı; çalışanlara anonimlik ve bildirim türleri anlatılmalı; DÖF kayıtları hedef tarih ve sorumlu ile kapatılmalı; aylık yönetim değerlendirmesinde açık kayıtlar, geciken DÖF'ler, tekrar eden tehlike kümeleri ve kontrol türleri incelenmelidir.

Sonuç olarak yüksek başarımlı bir İSG geri bildirim platformu, yalnızca yazılım kurulumu değil; raporlama kültürü, veri güvenliği, DÖF disiplini ve yönetim öğrenmesiyle birlikte uygulandığında anlamlıdır. Yazılım algoritması bu kültürü tek başına yaratmaz; fakat doğru tasarlandığında güvenilir, ölçülebilir ve sürdürülebilir bir iyileştirme zemini sağlar.

Kaynakça

Avrupa Birliği. (1989). Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. Official Journal L 183, 29.06.1989. https://eur-lex.europa.eu/eli/dir/1989/391/oj/eng

Avrupa Birliği. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal L 119, 04.05.2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Avrupa Birliği. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal L 333, 27.12.2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Çalışma ve Sosyal Güvenlik Bakanlığı. (2012). 6331 sayılı İş Sağlığı ve Güvenliği Kanunu. Resmi Gazete Tarihi: 30.06.2012, Sayı: 28339. https://www.csgb.gov.tr/Media/fldk2co0/6331_isgkanunu_tr.pdf

ILO. (1981). C155 - Occupational Safety and Health Convention, 1981 (No. 155). International Labour Organization. https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C155

ILO. (2006). C187 - Promotional Framework for Occupational Safety and Health Convention, 2006 (No. 187). International Labour Organization. https://www.ilo.org/resource/other/promotional-framework-occupational-safety-health-convention-2006-no-187

Mevzuat Bilgi Sistemi. (2012). İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği. Resmi Gazete Tarihi: 29.12.2012, Sayı: 28512, Mevzuat No: 16925. Ziyaret tarihi: 05.07.2026. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=16925&MevzuatTur=7&MevzuatTertip=5

Türkiye Cumhuriyeti Resmi Gazete. (2025). 7545 sayılı Siber Güvenlik Kanunu. Kabul Tarihi: 12.03.2025; Resmi Gazete Tarihi: 19.03.2025, Sayı: 32846. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7545&MevzuatTur=1&MevzuatTertip=5

Badea, D. O., Darabont, D. C., Trifu, A., Ivan, I., & Ciocirlea, V. (2025). A Digital Model for Incident Reporting to Support Occupational Safety and Health in Laboratories. Laboratories, 2(2), 13. https://doi.org/10.3390/laboratories2020013

CDC/NIOSH. (2018). Examining Factors That Influence the Existence of Heinrich's Safety Triangle Using Site-Specific H&S Data from More than 25,000 Establishments. CDC Stacks. https://stacks.cdc.gov/view/cdc/210656

CDC/NIOSH. (2024). Hierarchy of Controls. https://www.cdc.gov/niosh/hierarchy-of-controls/about/index.html

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13, 319-340. https://doi.org/10.2307/249008

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9-30.

Demich, B., Haas, E. J., & McGuire, J. (2020). The Use of Workers' Near-Miss Reports to Improve Organizational Management. Mining Publications, 72(8), 40-42. https://stacks.cdc.gov/view/cdc/215344

EDPB. (2020). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. European Data Protection Board. https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en

Gnoni, M. G., Tornese, F., Guglielmi, A., Pellicci, M., Campo, G., & De Merich, D. (2022). Near miss management systems in the industrial sector: A literature review. Safety Science, 150, 105704. https://doi.org/10.1016/j.ssci.2022.105704

Howell, A. M., Burns, E. M., Hull, L., Mayer, E., Sevdalis, N., & Darzi, A. (2017). How Effective Are Incident-Reporting Systems for Improving Patient Safety? A Systematic Literature Review. The Milbank Quarterly. https://www.milbank.org/quarterly/articles/how-effective-are-incident-reporting-systems-for-improving-patient-safety-a-systematic-literature-review/

ISO. (2026a). ISO 45001 explained: What it is and why it matters. https://www.iso.org/home/insights-news/resources/iso-45001-explained-what-it-is.html

ISO. (2026b). ISO 10002:2018 Quality management — Customer satisfaction — Guidelines for complaints handling in organizations. https://www.iso.org/standard/71580.html

ISO. (2026c). ISO/IEC 27001:2022 Information security management systems. https://www.iso.org/standard/27001

KVKK. (2024). Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi. Kişisel Verileri Koruma Kurumu. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

OSHA. (2021). Near Miss Reporting Policy Template. Occupational Safety and Health Administration. https://www.osha.gov/sites/default/files/2021-07/Template%20for%20Near%20Miss%20Reporting%20Policy.pdf

OSHA. (2026a). Safety Management: A safe workplace is sound business. https://www.osha.gov/safety-management

OSHA. (2026b). Leading Indicators. https://www.osha.gov/leading-indicators

OWASP. (2026). File Upload Cheat Sheet. OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

Reason, J. (1990). Human Error. Cambridge University Press.

Reason, J. (2000). Human error: models and management. BMJ, 320(7237), 768-770.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27, 425-478. https://doi.org/10.2307/30036540

Zohar, D. (1980). Safety climate in industrial organizations: theoretical and applied implications. Journal of Applied Psychology, 65(1), 96-102. PMID: 7364709.