

HITGuard GRC

by TogetherSecure

GOVERNANCE, RISK & COMPLIANCE
MANAGEMENT ZUR UNTERNEHMENSSTEUERUNG

Eine Plattform.
Alle GRC-Prozesse im Blick.

Zusammenhänge erkennen. Prozesse vereinfachen.
Entscheidungen fundiert treffen.

Governance, Risk & Compliance entfalten ihren größten Nutzen, wenn Informationen und Prozesse miteinander verknüpft sind. HITGuard GRC vereint unterschiedliche Aufgabenstellungen in einer modularen Plattform – von der Erfüllung regulatorischer Anforderungen über die Bewertung von Risiken bis zur Umsetzung von Kontrollen und Maßnahmen.

So entsteht ein gemeinsamer Überblick über relevante Informationen, Verantwortlichkeiten und Zusammenhänge. Statt isolierter Einzellösungen unterstützt HITGuard GRC eine durchgängige, transparente und nachvollziehbare Unternehmenssteuerung.

Alles im Zusammenhang

Vorgaben · Risiken · Kontrollen · Maßnahmen · Audits · Nachweise



Ihre Vorteile auf einen Blick

Zentrale Informationsbasis
Informationen strukturiert erfassen, gemeinsam nutzen und jederzeit wiederfinden.

Vernetzte Prozesse
Vorgaben, Risiken, Kontrollen und Maßnahmen miteinander in Beziehung setzen.

Transparente Verantwortlichkeiten
Aufgaben, Bearbeitungsstände und Zuständigkeiten übersichtlich verwalten.

Modular und flexibel
Mit einzelnen Anwendungsfällen starten und die Plattform bedarfsgerecht erweitern.

HITGuard GRC – aus einzelnen Informationen wird ein gemeinsames Gesamtbild.

Von der Anforderung zum Nachweis.

So greifen die Funktionen von HITGuard GRC ineinander.

Regulatorische Anforderungen, Risiken, Kontrollen und Audits sind eng miteinander verbunden. HITGuard GRC unterstützt Sie dabei, diese Zusammenhänge abzubilden und die zugehörigen Aufgaben über ihren gesamten Lebenszyklus hinweg nachvollziehbar zu steuern.

Ein durchgängiger GRC-Prozess

01 – Anforderungen erfassen
Relevante Gesetze, Normen und interne Vorgaben identifizieren und dokumentieren.

02 – Risiken bewerten
Mögliche Auswirkungen erkennen, bewerten und betroffene Bereiche zuordnen.

03 – Kontrollen und Maßnahmen festlegen
Geeignete Kontrollen definieren, Maßnahmen planen und Verantwortlichkeiten zuweisen.

04 – Umsetzung nachverfolgen
Aufgaben, Termine und Bearbeitungsstände transparent verwalten.

05 – Wirksamkeit überprüfen
Durch Audits, Assessments und Auswertungen den Umsetzungsstand prüfen und Verbesserungen ableiten.

Ein Beispiel aus der Informationssicherheit

Eine Anforderung der ISO/IEC 27001 wird im ISMS berücksichtigt und mit relevanten Risiken verknüpft. Daraus ergeben sich Kontrollen und gegebenenfalls Maßnahmen, deren Umsetzung dokumentiert und nachverfolgt wird. Im Rahmen eines Audits lässt sich anschließend überprüfen, inwieweit die Anforderung erfüllt ist und wo weiterer Handlungsbedarf besteht.



Das Ergebnis: Transparenz, Nachvollziehbarkeit und kontinuierliche Verbesserung – über einzelne GRC-Disziplinen hinweg.

Risikomanagement

HITGuard gibt Ihnen die Freiheit Chancen und Risiken Ihrer Organisation mit einer individuell konfigurierbaren Risikomatrix zu bewerten. Sie können bei der Identifikation von Risiken nach Bedrohungen und Fragenkatalogen vorgehen oder vorhandene Risikoinventarlisten importieren. Die Behandlungsstrategie hilft Ihnen das Brutto-Risiko zum Netto-Risiko bzw. zu einer Chance zu entwickeln. Die Arbeit in der Plattform entlastet Experten, indem Aufgaben workflowgestützt direkt an die Risikoeigner und andere Umsetzungsverantwortliche delegiert werden. Die Risiko-Kontroll-Matrix ist nur eine von vielen Auswertungsmöglichkeiten.



Exemplarische Anwendungsfälle unserer Kunden

Information Security Risk Management nach ISO 27001 und NIS2/KRITIS

Risikomanagement mit internen Kontrollsystemen

Tax Compliance Management Systeme (TCMS)

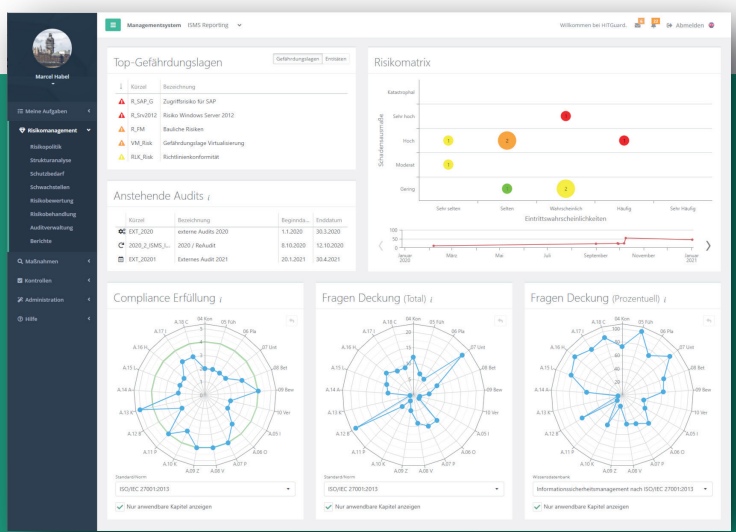
Testimonial

> HITGuard stellt sicher, dass die richtigen risikoreduzierenden Maßnahmen in Unternehmen budgetiert und auch tatsächlich umgesetzt werden. Es zeigt nicht nur Probleme auf, es hilft auch diese nachhaltig zu lösen!

IT-DIENSTLEISTER ÜBER DAS RISIKOMANAGEMENT IN HITGUARD

Highlights

- interaktiver Risikograph
- frei konfigurierbare Risikomatrix
- Risikoidentifikation unter Zuhilfenahme von Wissensdatenbanken
- workflowgestützte Risikobewertung unter Einbindung der Risikoeigner
- Risikoreduktion und -überwachung mittels Maßnahmen und Kontrollen
- historisch nachvollziehbare Entwicklung der Chancen & Risiken



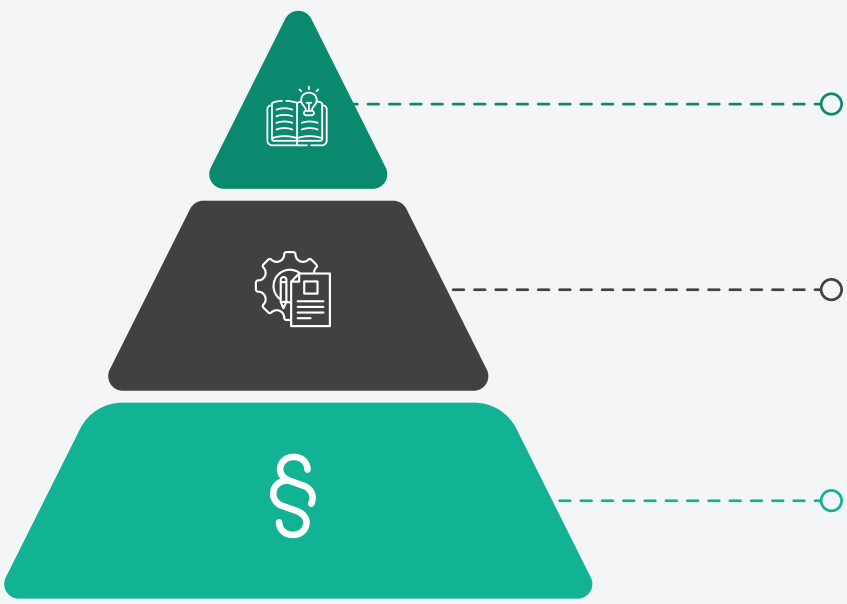
Highlights

- Versionierbare Wissensdatenbanken mit Fragelisten
- Vorschläge für Maßnahmen inkl. Vorlagen zur Behandlung erkannter Potentiale
- Kontrollvorschläge zur Überprüfung der Wirksamkeit umgesetzter Maßnahmen
- Compliance-Auswertung nach diversen Standards & Normen über Norm Mappings

Compliance Management

In HITGuard können Sie eine Vielzahl von Gesetzen, Standards und Normen nutzen. Die Erfüllung dieser Vorgaben durch Kollegen oder Lieferanten kann über eine workflowgestützte Aussendung von Checklisten überprüft werden. Diese Checklisten können mittels HITGuard Wissensdatenbanken selbst erstellt oder abonniert werden. Die Ergebnisse der Prüfungen werden dabei nachweislich dokumentiert und grafisch ansprechend visualisiert. Abweichungen können so zielgerichtet erkannt und behandelt werden.

Hierarchische Struktur der Vorgaben



Wissensdatenbanken

Abbildung der Vorgaben in Fragenkatalogen für Überprüfungen und Analysen

Interne Vorgaben

Code of Conduct, Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen, etc.

Externe Vorgaben

Gesetze, Normen, Branchen-standards, Regulative, etc.

Exemplarische Anwendungsfälle unserer Kunden

- Lieferantenbewertungen, um die Sicherheit der Lieferkette nach NIS2 zu prüfen
- Eigenentwicklung von Checklisten für interne Audits
- Self Assessment nach Standards & Normen, z.B. TISAX, BSI IT-Grundschutz, ISO 27001



Compliance Erfüllung - ISO 27001:2022 (Kap. 8)

Internes Kontrollsystem

Das IKS von HITGuard unterstützt vor allem im Bereich der Risikobehandlung und Risikoüberwachung: Es gewährleistet, dass die Maßnahmen zur Behebung von Schwachstellen systematisch abgearbeitet und dokumentiert werden. Ebenso sorgt es dafür, dass die Umsetzung der Maßnahmen regelmäßig überwacht wird. Mittels Kontrollen wird die Nachhaltigkeit der Risikobehandlung langfristig sichergestellt. Diese Features sind auch im Compliance Management sowie bei den Nacharbeiten zu durchgeführten Audits von höchster Wichtigkeit.

Exemplarische Anwendungsfälle unserer Kunden

- ISAE 3402 Kontrollen
- Implementierung eines Risk Treatment Plans
- Tax Compliance Management Systeme



Highlights

- Workflowgestützte Abarbeitung von Maßnahmen & Kontrollen
- Regelmäßige Erhebung des Fortschritts von Maßnahmen
- Detailliert nachvollziehbare Protokolle zu durchgeführten Kontrollen
- Kennzahlen und aussagekräftiges Reporting, z.B. Risiko-Kontroll-Matrix

Testimonial

Beim Betrieb eines ISMS ist die Königsdisziplin das Maßnahmenmanagement sowie das Funktionieren eines internen Kontrollsystems. Dies trifft vor allem Verantwortliche in Unternehmen, die auf Grund ihrer Größe bzw. geographischen Aufteilung auf die „verteilte Mitarbeit quer durch das Organigramm" angewiesen sind. Auf der anderen Seite muss für die betroffenen Personen die Mitarbeit möglichst einfach und intuitiv erfolgen können, um zeiteffizient das ISMS zu unterstützen.

Das alles wird mit HITGuard ermöglicht, weshalb wir auf den Einsatz dieses Tools setzen!

Geschäftsführerin über das IKS in HITGuard

Informationssicherheitsmanagement



nach ISO/IEC 27001 und BSI IT-Grundschutz

für NIS-2, KRITIS, TISAX und weitere Anforderungen

HITGuard macht Informationssicherheitsmanagement schnell umsetzbar und langfristig beherrschbar. Wissensdatenbanken führen wie Checklisten durch Self Assessments und machen Handlungsbedarf sichtbar. Die Strukturanalyse visualisiert, wo sich erkannte Risiken auf Prozesse, Organisationseinheiten und Ressourcen auswirken. Maßnahmen und Evidenzen werden workflowgestützt gemeinsam mit den zuständigen Kollegen in der gesamten Organisation bearbeitet und nachverfolgt. Gesteuerte Neubewertungsmechanismen und Workflow-Pläne unterstützen die kontinuierliche Weiterentwicklung des ISMS und lenken Überarbeitungen gezielt auf die Bereiche, in denen tatsächlich Handlungsbedarf besteht. So entsteht ein historisch nachvollziehbarer Audittrail – von der Bewertung über die Umsetzung bis zum erforderlichen Nachweis.

Anwendungsfälle unserer Kunden

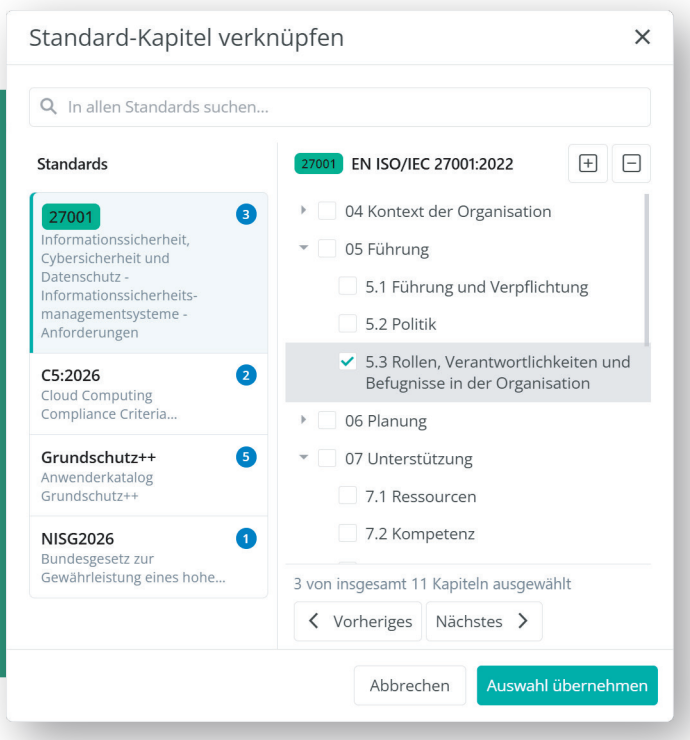
Aufbau & kontinuierliche Weiterentwicklung eines ISMS

Self Assessments nach Normen & Anforderungen

Vorbereitung & Begleitung von Audits und Assessments

Highlights

- Schnell einführbares ISMS durch vorkonfigurierte Inhalte & Wissensdatenbanken
- Bewertung von Anforderungen und gezielte Identifikation von Handlungsbedarfen
- Visualisierung von Risikowirkungen auf Prozesse, Organisationseinheiten & Ressourcen
- Workflowgestützte Zusammenarbeit sowie strukturierte Sammlung von Evidenzen
- Durchgängiger Audit Trail für Bewertungen, Maßnahmen, Änderungen und Nachweise
- Gesteuerte Neubewertungen statt unnötiger Komplettbewertungen
- Kontinuierliche Verbesserung bei reduziertem Zeit- und Abstimmungsaufwand
- Historisch nachvollziehbare Entwicklung des ISMS

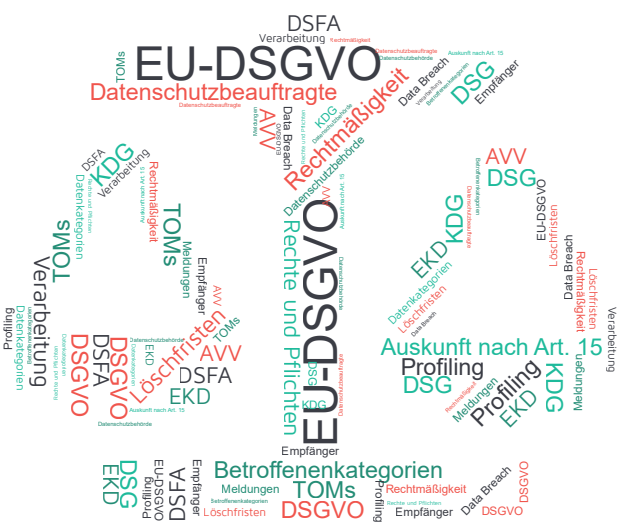


Datenschutz

Mit HITGuard können Sie die Anforderungen des Datenschutzes effizient und nachhaltig erfüllen. Das Tool ermöglicht die Verwaltung von Verarbeitungstätigkeiten (VTs) über Organisationsstrukturen mit mehreren Verantwortlichkeiten hinweg. Die workflowgestützte Zusammenarbeit mit Personen in den Fachbereichen entlastet die Datenschutzbeauftragten. Selbstverständlich bietet das Tool Funktionalitäten wie Datenschutz-Folgenabschätzungen und die Verwaltung von TOMs, Auftragsverarbeitern, Empfängern und Kunden. Hinzu kommt die Einbindung von Wissensdatenbanken für die EU-DSGVO sowie länder-, religions- und branchenspezifische Selbstchecks.

Anwendungsfälle unserer Kunden

- Datenschutz nach der EU-DSGVO
- länderspezifischer Datenschutz für AT, DE und CH
- kirchlicher Datenschutz verschiedener Religionsgemeinschaften





Highlights

- VTs in übersichtlichen, berechtigungstechnisch getrennten Registern
- Funktionalitäten für Auftragsverarbeiter, Verantwortliche und Externe
- Bearbeitung und Review von VTs an Sachbearbeiter delegierbar
- Durchführung von Datenschutz-Folgenabschätzung im Tool
- EU-DSGVO-konforme Vorlagenpakete in Form von Wissensdatenbanken
- Umfassendes Reporting für VT, AV, DSFA, TOMs, Auskunftsbegehren, u.v.m.

Lieferantenrisikomanagement



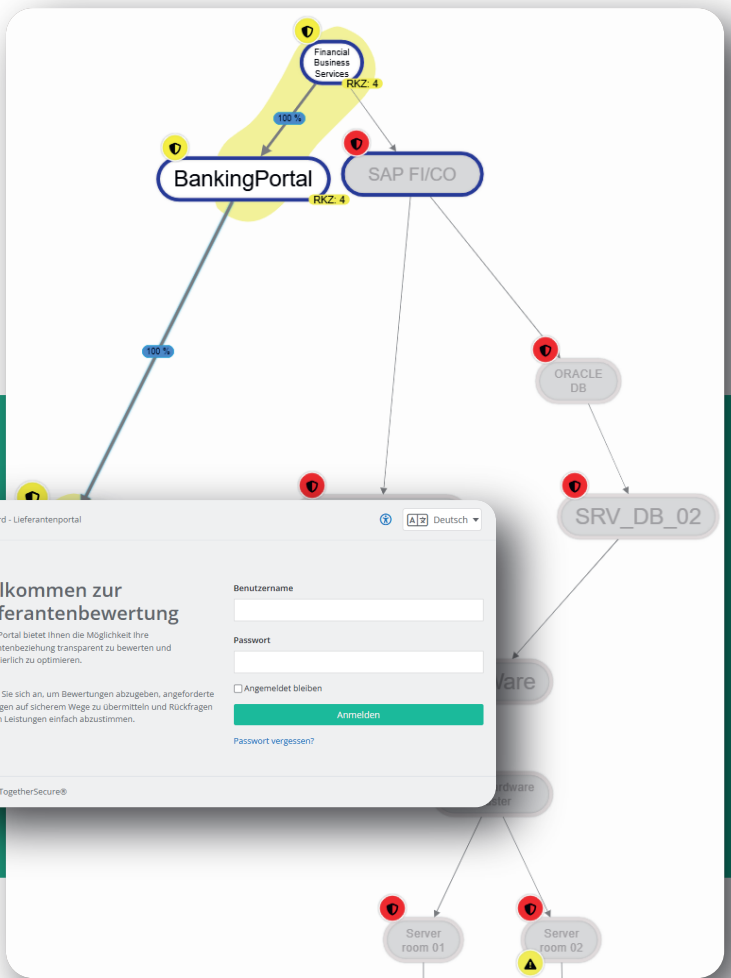
HITGuard gibt Ihnen die Möglichkeit Ihre Lieferanten mittels Checklisten hinsichtlich der Erfüllung Ihrer Anforderungen zu beurteilen. Dabei können Sie Ihre eigene Beurteilung erfassen oder den Lieferanten, über das HITGuard Lieferantenbewertungsportal, zur Beantwortung der Checkliste auffordern. Dafür können Ansprechpartner des Lieferanten eigene Accounts zur sicheren Anmeldung am Portal erhalten und über diesen Weg, auch Unterlagen mit Ihnen austauschen. Aus den Nichterfüllungen von Anforderungen können Sie dann Risiken ableiten. Die Auswirkung des Lieferantenrisikos auf die Organisation wird in der HITGuard Strukturanalyse sofort ersichtlich.

Exemplarische Anwendungsfälle unserer Kunden

- Die Sicherheit der Lieferkette nach NIS2 (Cybersicherheits-Richtlinie)
- Risikoanalyse nach dem LkSG (Liefer-kettensorgfaltspflichtengesetz)
- Compliance nach CSDDD (EU-Lieferketten-richtlinie)

Highlights

- Nachvollziehbar dokumentierte Befragung der Lieferanten
- Ermittlung und Visualisierung kritischer Lieferanten und ihrer Risiken
- versionsgesteuerte Entwicklung von Checklisten
- wiederkehrende Befragungen auf Basis der Vorjahres-Antworten
- ableitbare Behandlungspläne zur Lieferan-tenentwicklung inkl. Fortschrittsverfolgung
- sichere Verwaltung und zeitliche Befris-tungsmöglichkeit für Lieferanten-Accounts





Business Continuity Management

nach BSI 200-4 und ISO 22301

für Anforderungen aus CER/RKE-Richtlinie, RKEG und KRITISDachG

HITGuard unterstützt Sie dabei, die Business Continuity Ihrer Organisation systematisch zu planen, zu steuern und kontinuierlich zu verbessern. Im Business Impact Assessment werden kritische Prozesse und deren Anforderungen an Wiederanlauf und Datenverfügbarkeit ermittelt. Die Strukturanalyse visualisiert die Abhängigkeiten zwischen Prozessen, Organisationseinheiten und Ressourcen und schafft Transparenz über kritische Zusammenhänge. Abweichungen zwischen RTO und RTA sowie RPO und RPA machen Handlungsbedarf sichtbar. Workarounds, Korrektur- und Verbesserungsmaßnahmen sowie Wiederanlaufbeschreibungen unterstützen die gezielte Vorbereitung auf Störungen. Ihre Umsetzung wird ebenso wie Tests und Übungen workflowgestützt geplant und nachvollziehbar verfolgt.

Anwendungsfälle unserer Kunden

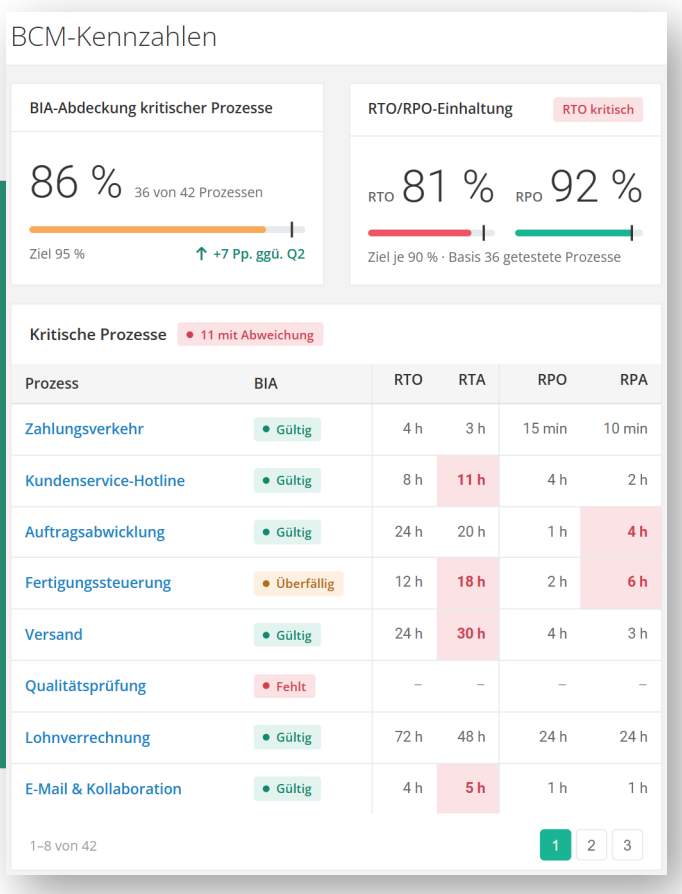
Business Impact Assessment

Notbetriebs- und Wiederanlaufplanung

Resilienzmanagement kritischer Prozesse

Highlights

- Business Impact Assessment zur Ermittlung kritischer Prozesse und Wiederanlaufanforderungen
- Visualisierung von Abhängigkeiten zwischen Prozessen, Organisationseinheiten und Ressourcen
- Ermittlung von Handlungsbedarf aus Abweichungen zwischen RTO und RTA sowie RPO und RPA
- Planung von Workarounds zur Sicherstellung des erforderlichen Notbetriebsniveaus
- Korrektur- und Verbesserungsmaßnahmen zur Optimierung von RTA und RPA
- strukturierte Erfassung von Notbetriebs- und Wiederanlaufbeschreibungen
- workflowgestützte Nachverfolgung der Umsetzung von Maßnahmen und Workarounds
- Planung und Nachverfolgung von Tests und Übungen





Auditmanagement

HITGuard ermöglicht Ihnen die einfache Planung und Organisation von Audits: intern/extern, verschiedene Standorte und Schwerpunkte, über die Jahre verteilt. Mit einem praktischen Kalender behalten Sie den Überblick. Die Durchführung kann mit Interviews oder als Self Assessment erfolgen. Jederzeit können aufschlussreiche Berichte generiert werden und die relevanten KPIs sind auf konfigurierbaren Dashboards ersichtlich. Maßnahmen/Kontrollen können aus Prüfergebnissen heraus erstellt oder mit diesen verknüpft werden. Durchgeführte Prüfungen und Analysen können neu bewertet werden. So sind Entwicklung und Reifegrad Ihrer Auditlandschaft stets ersichtlich.

Exemplarische Anwendungsfälle unserer Kunden

Vorbereitende interne Interviews für die Zertifizierung nach ISO 27001

Standortübergreifende Qualitätsmanagement-audits

Schwerpunktaudits, z.B. Arzneimittelaudits in Apotheken oder TISAX Self Assessments

Planung: Grob- und Feinplanung von Auditterminen

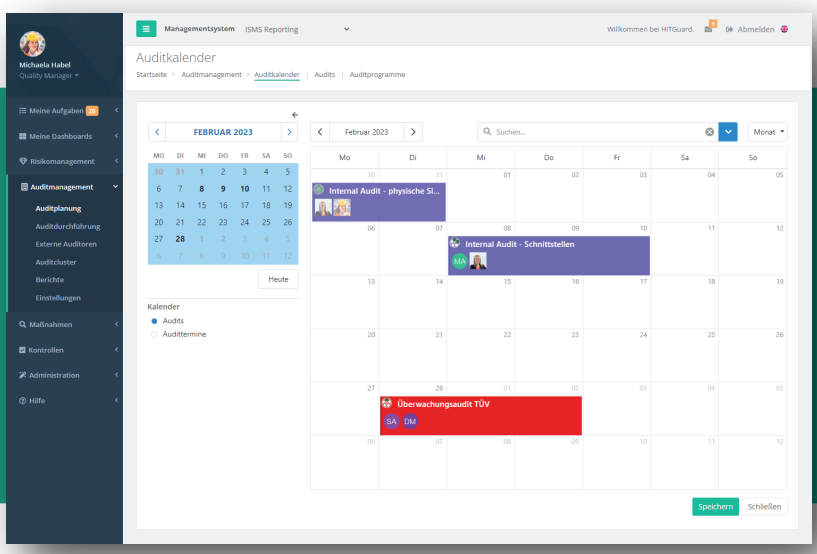
Durchführung: Dokumentation der Interviews bzw. Self Assessments

Reaktion: Ableiten von Maßnahmen samt Nachverfolgung

Auswertung: Visualisierung & Nachbehandlung

Highlights

- Pflege von externen Prüfergebnissen und Fragekatalogen zu internen Audits
- Auditkalender mit Übersichten und Details zu Programmen und Einzelterminen
- Assistenten zur Auditdurchführung mit der Möglichkeit von Self Assessments
- Standards und Normen mit entsprechenden Auswertungsmöglichkeiten auditieren



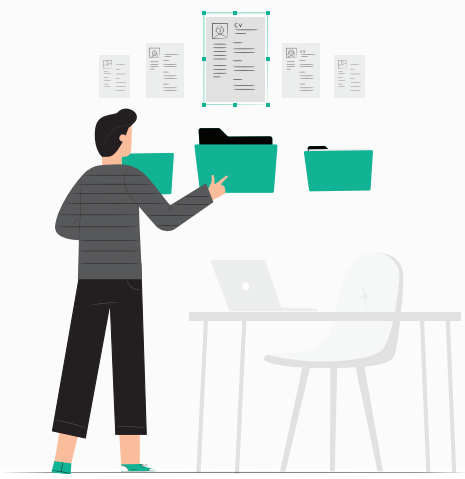
Dokumenten Management

In HITGuard können Sie sowohl Dokumente als auch Links auf andere Datenquellen verwalten. Dabei strukturieren Sie die Ablage nach Ihrem Bedarf und versehen die Einträge mit Metadaten, wie Mappings auf Standards und Normen und dem Dokumentenverantwortlichen. Über wiederkehrende Kontrollläufe können Sie die nachvollziehbare Revisionierung der Dokumente sicherstellen.



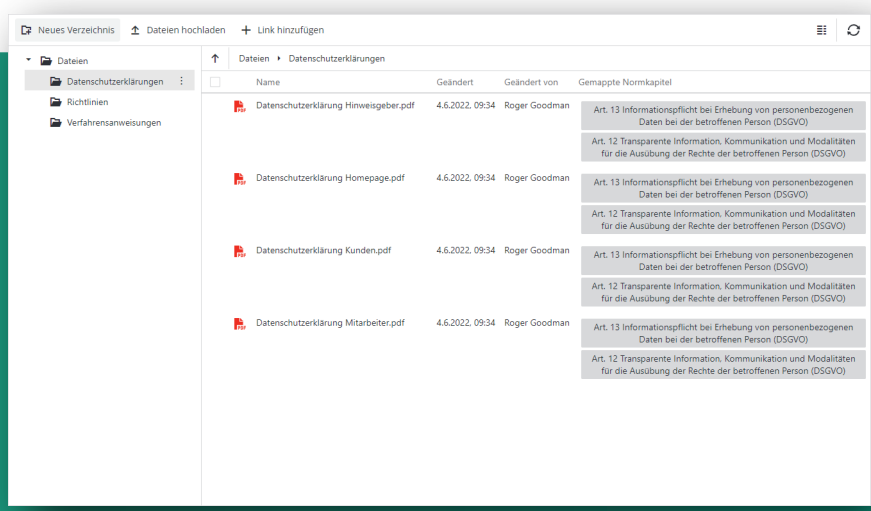
Exemplarische Anwendungsfälle unserer Kunden

- Revisionierung von Policies und Richtlinien
- Strukturierte Ablage von Vertragsdokumenten
- Zentrale Ablage von Berichten



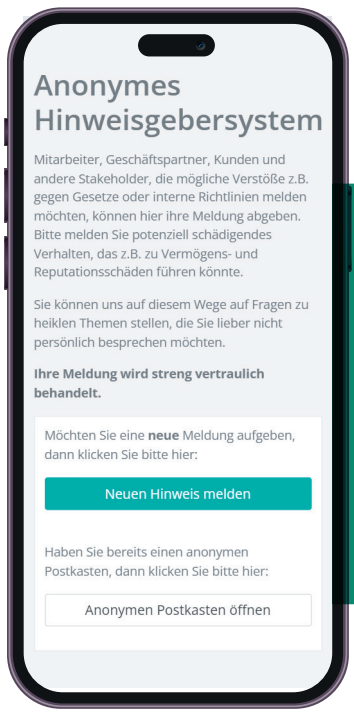
Highlights

- Sammlung von Dokumenten an zentraler Stelle
- Schnelles Auffinden gemappter Dokumente bei Audits
- Nachvollziehbare Revisionshistorie
- Wiederkehrende Kontrollläufe zum Dokumenten Review



Exemplarische Anwendungsfälle unserer Kunden

- Compliance Verstöße
- Datenschutzvorfälle
- Arbeitsschutz



Fallmanagement

Mit HITGuard können Sie ein Vorfalls-Management implementieren, für das auch ein anonymes Meldeportal für Hinweisgeber aktiviert werden kann. Dieses ermöglicht es Mitarbeitern, Geschäftspartnern, Kunden und anderen Stakeholdern, anonym Meldungen abzugeben oder Fragen zu stellen. Verstöße gegen Gesetze oder auch interne Vorgaben können entsprechend nachverfolgt und Vermutungen kann nachgegangen werden. Fristen zur Bearbeitung von Meldungen können verwaltet und ihre Einhaltung überwacht werden. So können alle involvierten Stakeholder gemeinsam daran arbeiten, dass die geltenden Gesetze und internen Regelungen zu Sicherheit und ethischen Standards eingehalten werden.

Highlights

- Anonyme Meldung gemäß EU-Richtlinie 2019/1937 (Whistleblower)
- Sicherer Meldekanal zum Schutz der Identität von Hinweisgebern und Dritten
- Workflows zur effizienten Abwicklung von Meldungen, Fragen und Antworten
- Automatische Erinnerungen zur Einhaltung gesetzlicher Antwortfristen

Wie funktioniert's?

Anonyme Meldung

Am Meldeportal wird ein Hinweis aufgegeben

Behandlung

Die Meldung wird einem Bearbeiter zugewiesen, der sie fristgerecht behandelt

Rückfragen

Über ein anonymes Postfach kann mit dem Melder kommuniziert werden

Ablage

Meldungen werden datenschutzkonform archiviert

ESG / CSRD / ESRS



HITGuard hilft Ihnen die wesentlichen Handlungsfelder im Bereich Environmental, Social & Governance (ESG) für die Nachhaltigkeitsberichtserstattung zu ermitteln. Die Doppelte Wesentlichkeitsanalyse nach CSRD und ESRS kann in HITGuard durchgeführt werden. Dabei werden Risiken und Chancen für die Betrachtung der Innenwirkung und positive sowie negative Auswirkungen für die Betrachtung der Außenwirkung verwaltet. Ihre Behandlung über Maßnahmen und Kontrollen stellt die langfristige Verfolgung der Umsetzungsziele dabei sicher.

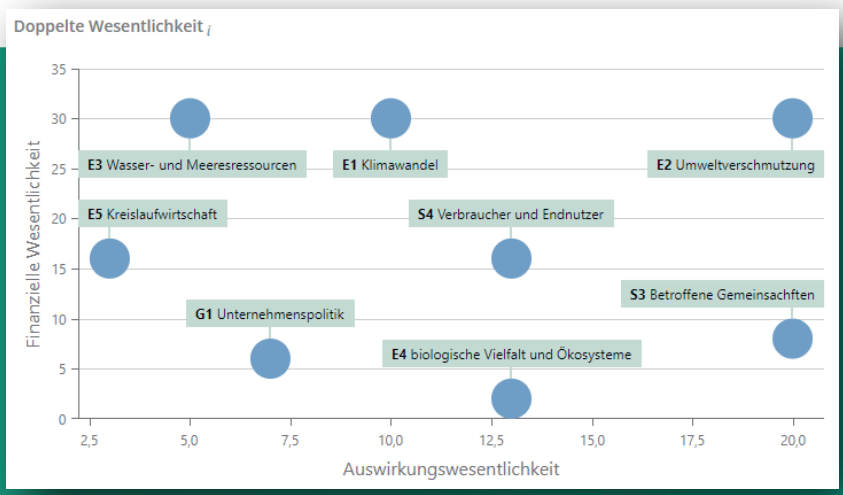
Exemplarische Anwendungsfälle unserer Kunden

- Auswirkungsanalyse
- Chancen und Risikomanagement
- Doppelte Wesentlichkeitsbeurteilung



Highlights

- Nachvollziehbare Behandlung von Risiken, Chancen und Auswirkungen über Maßnahmen und Kontrollen
- Automatische Errechnung der Handlungsfelder, wie ESRS-Themen über das Zusammenwirken von Risiken, Chancen und Auswirkungen
- Visualisierung der Doppelten Wesentlichkeitsanalyse auf gewählter Detailebene



Wissensdatenbanken

In den Bereichen der **Informationssicherheit** und des **Datenschutzes** bieten wir derzeit die folgenden Prüffragenkataloge & Checklisten mit Vorschlagstexten für Maßnahmen und Kontrollen in der Form von jährlichen Abonnements an:

IT-Grundschutz-Kompendium des BSI

IT-Grundschutz | ISO 27001

Autor: Bundesamt für Sicherheit in der Informationstechnik

Cloud Computing Compliance Criteria Catalogue (C5:2026)

C5:2020 | C5:2026

Autor: Bundesamt für Sicherheit in der Informationstechnik

Assessment zur Umsetzung des Informationssicherheitsmanagements nach ISO/IEC 27001:2022

ISO 27001 | NIS 2

Autor: TogetherSecure GmbH

Assessment zur Umsetzung des KI-Managementsystem nach ISO/IEC 42001:2023

ISO 42001

Autor: TogetherSecure GmbH & Advanced Integrity e.U.

Assessment zur Umsetzung des Informationssicherheitsmanagements nach NIS auf Basis von NIS & KRITIS Anforderungen

KRITIS | NIS 2 | ISO 27001

Autor: Deutsche Telekom Cyber Security Austria GmbH

Assessment zur Umsetzung der NIS-2 Risikomanagementmaßnahmen auf Basis NISG 2026 & NIS-2 DVO

NIS 2 DVO | NISG 2026 | ISO 27001

Autor: UNINET it-consulting GmbH

Security Framework Bund 2 (SFB 2)

NIS 2 DVO

Autor: Bundeskanzleramt

Branchenneutrales Vorlagenpaket zum Informationssicherheitsmanagement

ISO 27001 | KRITIS

Autor: TogehterSecure GmbH & Partner

Branchenneutrales Vorlagenpaket zum Datenschutzmanagement

DSGVO

Autor: TogehterSecure GmbH & Partner

Assessment zur Umsetzung der Datenschutz-Grundverordnung

DSGVO

Autor: TogehterSecure GmbH

Vorlagenpaket zum Informationssicherheitsmanagement für den HealthCare Bereich

ISO 27001 | B3S | KRITIS | HealthCare

Autor: TogehterSecure GmbH & Partner

B3S Branchenstandard Gesundheitsversorgung im Krankenhaus

B3S | KRITIS | HealthCare | ISO 27001

Autor: Deutsche Krankenhausgesellschaft e.V. (DKG)

VDA ISA Self Assessment

TISAX | VDA

Autor: Verband der Automobilindustrie

PCI DSS Self Assessment

PCI DSS

Autor: PCI Security Standards Council, LLC

Kontaktieren Sie uns gerne unter support@togethersecure.at falls Sie detaillierte Informationen zu Inhalten, Schwerpunkten und Preisen unserer Wissensdatenbanken erhalten möchten.



Von Praktikern für Praktiker

Das GRC-Tool HITGuard wurde mit Praxiserfahrung ins Leben gerufen und wird unter Miteinbezug der User-Perspektive laufend weiterentwickelt. Es unterstützt Sie daher optimal dabei, in Ihrem Managementsystem mit verschiedenen Personen zielgerichtet zusammenzuarbeiten. Es erlaubt Ihnen, die Entwicklung des Reifegrads Ihres Unternehmens zu steuern und die dadurch erzielten Ergebnisse sowohl mit der Führungsebene wie auch den mitarbeitenden Verantwortlichen selbst zu teilen. Dieses Tool passt sich an Ihre Anforderungen an, nicht umgekehrt!

- mit **konfigurierbaren Dashboards** den Überblick behalten
- mit konfigurierbaren Standard-KPIs **Kennzahlen** Reifegrade messen
- mit **adaptierbaren Berichten** das Management sowie Behörden informieren
- mit **exportierbaren Übersichten** und **Grafiken** das Reporting bereichern
- mit **branchenspezifischen Wissensdatenbanken** das Know-how der Experten ergänzen
- mit **eigenen Wissensdatenbanken** intern erarbeitetes Wissen anwendbar machen

Weitere Vorteile auf einen Blick

- kostengünstiges **Mietmodell**
- **On-premises** oder **SaaS** Betrieb
- **Mehrsprachigkeit** in allen Modulen
- **Online Hilfe** und integrierte Tooltips
- **intuitive Bedienung** und kaum Schulungsaufwand
- personalisierbares **Design**

QR-Code scannen und HITGuard kostenlos testen

Kontaktieren Sie uns

TogetherSecure GmbH
Bauernstraße 11
4600 Wels

Tel: +43 670 200 54 49
Email: office@togethersecure.com
www.togethersecure.com