TogetherSecure

für lebendige und schlagkräftige Managementsysteme

Steckbrief | Ing. Mag. Christina Haas, MBA

Job: Geschäftsführerin TogetherSecure Gmbh

verantwortlich für Consulting & Vertrieb

Ausbildung:

HTL für IT & Organisation,
Wirtschaftsinformatik Studium,
General Management MBA,
CISA, CISM und ITIL V3 Expert

Berufserfahrung:

Mehr als 10 Jahre im Information Risk & Security Management sowie im strategischen IT-Management

Hobbies: Marathonlaufen, Westernreiten, Konzerte besuchen und um die Welt reisen

TogetherSecure

NIS-2

NIS-2 | Worum es geht?

- Die Cybersicherheits-Richtlinie soll zur Erhöhung der Netzwerk- und Informationssicherheit beitragen und die Reaktion auf Sicherheitsvorfälle in der EU verbessern. Das gilt für den öffentlichen und den privaten Sektor.

- Die NIS-Richtlinie trat dazu 2016 in Kraft und wurde mit der NIS-2 Richtlinie 2023 erweitert. NIS-2 wird allerspätestens ab 18. Oktober 2024 gültig sein.

- NIS verfolgte das Ziel,
  - Betreiber kritischer Infrastruktur durch Risikomanagementmaßnahmen für die Sicherheit ihrer Netz- und Informationssysteme sorgen zu lassen,
  - Meldepflichten bei Vorfällen einzuführen,
  - nationale Behörden dafür zu schaffen
  - und die Zusammenarbeit zwischen den Mietgliedstaaten im Bereich CyberSecurity zu entwickeln.

  Durch abschreckend hohen Sanktionen wurde das Thema in der Öffentlichkeit ernst genommen.

- NIS-2 weitet nun den Anwendungsbereich nach Sektoren und Unternehmens-größen deutlich aus und versucht das Sicherheitsniveau zwischen den Mitgliedsstaaten besser aneinander anzugleichen.

NIS-2 | Wer ist davon betroffen?

CENTRE FOR CYBER SECURITY BELGIUM

NIS-2 Scope – Final version

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees **or** more than 50 million revenue)	Medium (more than 50 employees **or** more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions (**attention: DORA lex specialis**)					
4. **Financial Market Infrastructure**	Trading venues, central counterparties (**attention: DORA lex specialis**)					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers					
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment		Essential		
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
	Internet Exchange Point providers					
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations (**excluding education institutions**)	Member State(s) where established				
Entities providing domain name registration services		**One stop**: Only the MS where they have Main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

TogetherSecure

Quelle: https://ccb.belgium.be/de/die-nis2-richtlinie-was-bedeutet-sie-f%C3%BCr-mein-unternehmen, abgerufen am 07.04.2024

NIS-2 | Was ist zu tun?

Folgende 10 Risikomanagementmaßnahmen sind umzusetzen:

1. Konzepte zur Risikoanalyse und Informationssicherheit
2. Vorgehen zur Bewältigung von Sicherheitsvorfällen
3. Business Continuity- und Krisenmanagement-Konzepte
4. Sicherstellung der Sicherheit der **Lieferkette**
5. Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
7. Cyberhygiene und Schulungen zur Cybersicherheit
8. Kryptografie und ggf. Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle
10. Multi-Faktor-Authentifizierung

Es sind Berichtspflichten zu erfüllen (nach 24h, 72h, nach 1 Monat)

und die Verantwortlichkeit des **Top-Management** wiegt schwerer; das Top-Management ist explizit zu schulen!

NIS-2 | Was sin die Folgen?

Wichtige Einrichtungen	Wesentliche Einrichtungen
Aufsicht	**Aufsicht**
nur bei begründetem Verdacht	Regelmäßige gezielte Sicherheitsüberprüfungen
Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen	Vor-Ort-Kontrollen, externe Aufsichtsmaßnahmen, Stichprobenkontrollen
Strafe	**Strafe**
EUR 7 Millionen oder 1,4 % des weltweiten Umsatzes	EUR 10 Millionen oder 2 % des weltweiten Umsatzes


DER WEG ZUR INFORMATIONSSICHERHEIT
... eine Heldenreise zur NIS2
Es war einmal, vor nicht allzu langer Zeit, ...
Bild KI generiert

Die ISMS Burg

Bild KI generiert

PROZESSE UND FUNKTIONEN EINER GUT GERÜSTETEN ISMS BURG

- Governance mit Richtlinien
- Risikomanagement
- Asset Management
- Lieferantenmanagement
- IT-BCM
- IS-Vorfall Management
- IT Compliance
- Sichere Softwareauswahl & Softwareentwicklung
- Awareness
- Aktionspläne & Kontrollen
- Dokumentation
- wichtige ITSM-Prozesse
  - Change Management (Patchmanagement)
  - Incident Management
  - Problem Management
  - Capacity Management
  - Availability Management
- Kryptographie & sicherer Datenaustausch
- Interne / externe Audits
- KPIs & Berichte, regelmäßige Messungen
- Physische Sicherheit
- Rechtemanagement (PAM)
- Personalsicherheit
- Zugriffskontrolle - Netzwerk, Monitoring

IT-On und Off-Boarding

Ein Beispiel aus dem Zugriffschutz

tenfold

Bild KI generiert

Held / Heldin

Skills & Superkräfte

- Analytisches Denkvermögen
- Beharrlichkeit
- Belastbarkeit
- Zielorientierung
- Durchsetzungsstärke
- Glaubwürdigkeit
- Kommunikationsstärke
- Teamfähigkeit

sowie

- die Identifikation mit den Zielsetzungen der Institution,
- die Einsicht in die Notwendigkeit von Informationssicherheit,
- Erfahrungen im Projektmanagement.

Bild KI generiert

Helden-Inventar

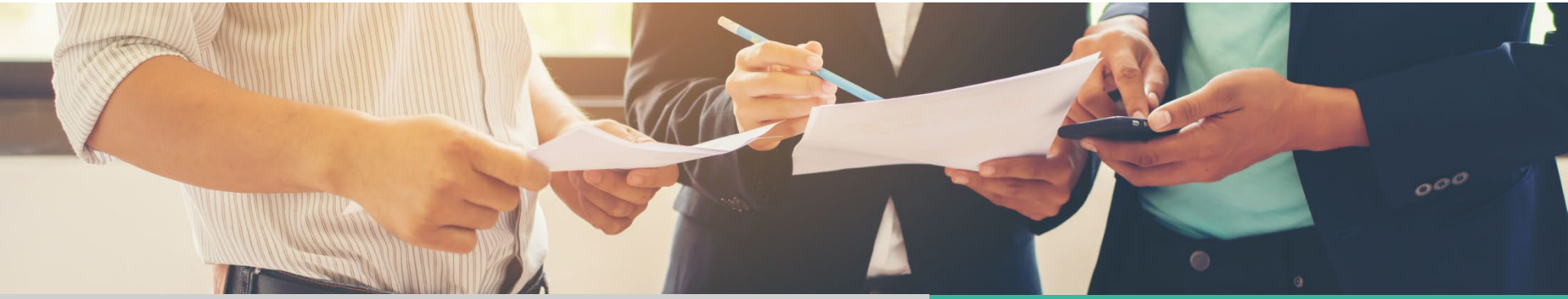
tenfold

HITGuard

TogetherSecure
& HITGuard

Unsere Mission

Ressourcenschonendes Governance, Risk & Compliance Management zur effizienten Unternehmenssteuerung



Interaktiv,
kollaborativ
und partnerschaftlich

Gemeinsam für ein sicheres Unternehmen

Dafür steht TogetherSecure!

WIR WISSEN …

Interaktion im GRC erhöht die Effizienz ihrer Managementsysteme!

Mit HITGuard kann keine Aufgabe vergessen werden.

TogetherSecure

Unser Leistungsangebot | HITGuard

Wir bieten Ihnen Software Unterstützung und begleitende Beratung für Ihre spezifischen Bedürfnisse!

- abonnierbare Wissensdatenbanken
- Vorschläge für einmalige Maßnahmen
- Vorschläge für regelmäßige Kontrollen
- Auswertung interner und externer Vorgaben

- Anonyme Meldung gemäß (EU) 2019/1937
- Sicherer und anonymer Meldekanal
- Abwicklung von Meldungen und Anfragen
- Erinnerungen an definierbare Antwortfristen

- interaktiver Risikograph
- frei konfigurierbare Risikomatrix
- Behandlung und Überwachung von Risiken
- historisch nachvollziehbare Entwicklung

- interne und externe Audits
- praktischer Auditkalender
- Interviews oder Self Assessments
- flexible Auswertungsmöglichkeiten

- übersichtliche VT-Register
- Auskunftsbegehren nachkommen
- Quick-Checks zur Anforderungsermittlung
- Reporting für VT, DSFA, TOMs, u.v.m.

- Maßnahmen & Kontrollen
- Regelmäßige Fortschrittserhebung
- detaillierte Kontrollprotokolle
- Risiko-Kontroll-Matrix

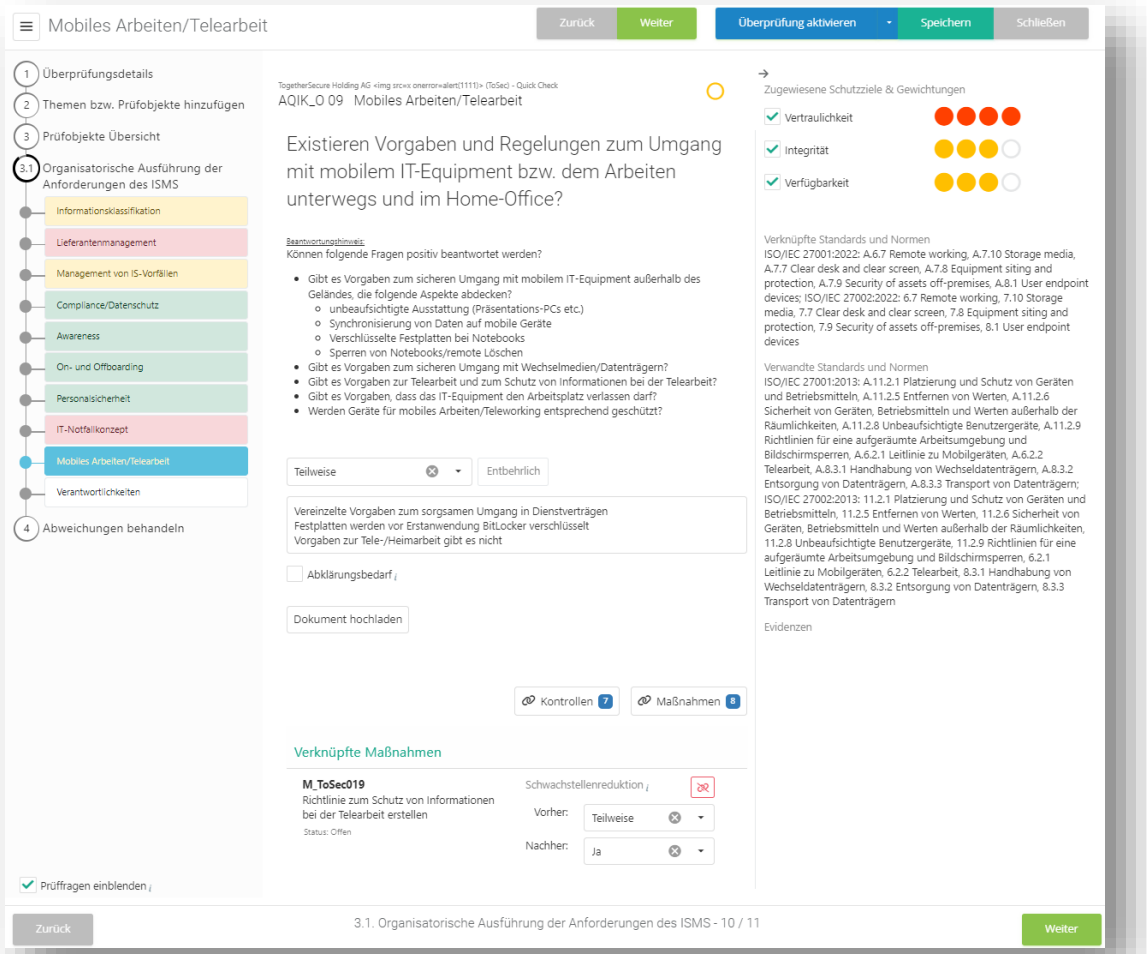
TogetherSecure

HITGuard

Impressionen

HITGuard Impressionen

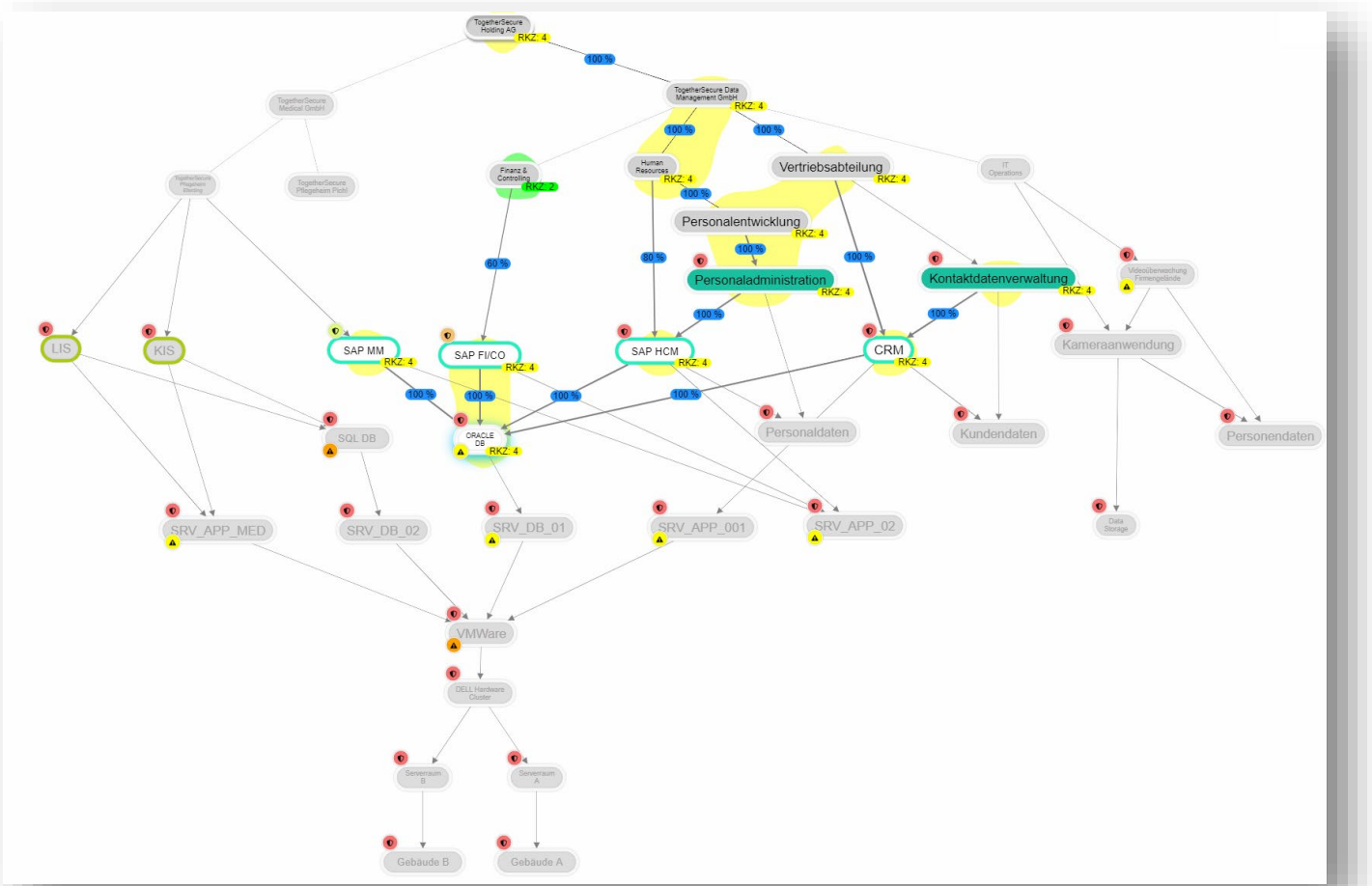
Gap Analysen anhand themenspezifischer Wissensdatenbanken



TogetherSecure

HITGuard Impressionen

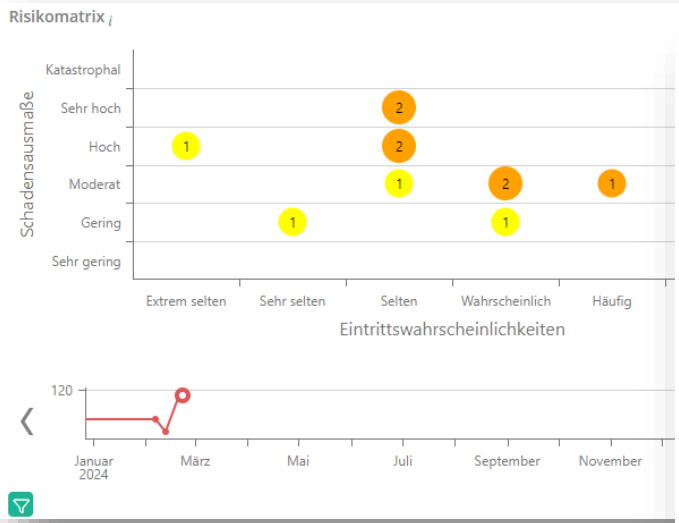
Strukturanalysen zur Darstellung der Auswirkung von Risiken auf schutzbedürftige Assets

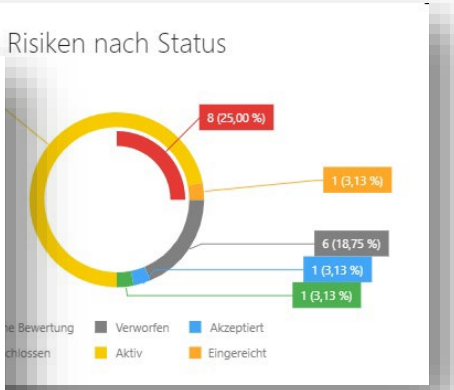


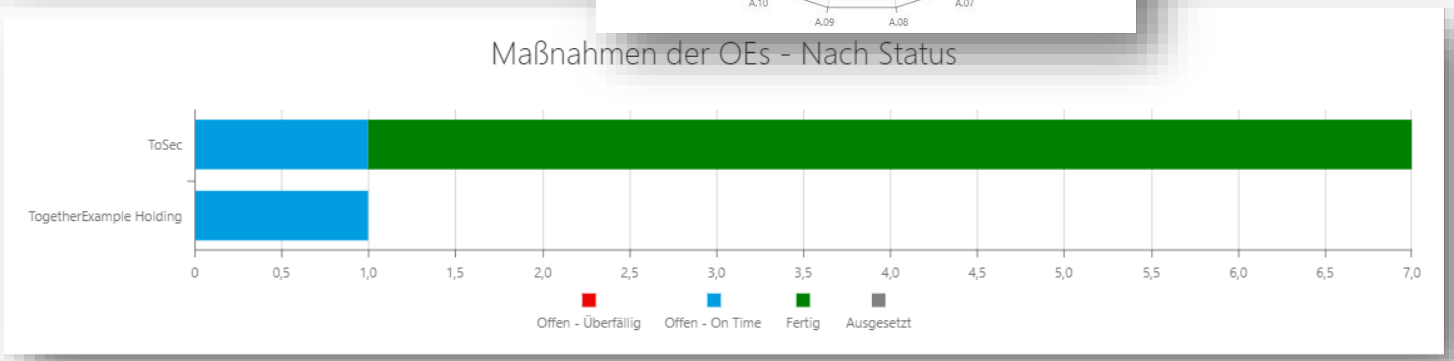
TogetherSecure

HITGuard Impressionen

Interaktive KPIs und Reports, um Ergebnisse auszuwerten und zu präsentieren







TogetherSecure

Erfahren Sie mehr über ein schlagkräftige ISMS unter

https://www.togethersecure.com/informationssicherheitsmanagement/

TogetherSecure

Vielen Dank für Ihre Aufmerksamkeit!

Bauernstraße 1,
A-4600 Wels

+43 (0) 670 200 54 49

office@togethersecure.at

www.togethersecure.com