Berufsbild CISO

Ausgabe 03/2024

Version:	*1.0*
Datum:	*03.03.2024*
Nächste Überprüfung:	*Spätestens 03/2027*
Klassifizierung:	***ÖFFENTLICH***
Status:	*in Arbeit / vorgelegt **/ freigegeben***
Autor(en):	*Alexander BIEHL, Robert HELLWIG*, Ulrich HEUN, Ralf KLEINFELD, Martin MACKE, Sven MENDLER*
Dokumentenverantwortung:	**Leiter Arbeitskreis „Berufsbilder Informationssicherheit“*
Ablage:	*SharePoint CISO Alliance, AK Berufsbilder Informationssicherheit Veröffentlichung: Webseite CISO Alliance e.V.*
Verteiler:	
Alle	alle Mitglieder

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	03.03.2024	Robert HELLWIG et al.	Erste zur Veröffentlichung freigegebene Fassung

Hinweis:

Im gesamten Text wird zur besseren Lesbarkeit und aus Vereinfachungsgründen grundsätzlich die männliche Form verwendet. Es handelt sich um keine Einschränkung, sondern beinhaltet immer alle Formen: männlich, weiblich und divers.

Definitionen, Abkürzungen, Verweise

Begriff	Definition
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAIT	Bankenaufsichtliche Anforderungen an die IT
BISB	Bereichs-Informationssicherheitsbeauftragter
BISO	Business Information Security Officer
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISM®	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Security Systems Professional
CSO	Chief Security Officer/Corporate Security Officer
DORA	Digital Operational Resilience Act(EU-Verordnung 2022/2254)
DSB	Datenschutzbeauftragter
HIPAA	Health Insurance Portability and Accountability Act
ISB	Informationssicherheitsbeauftragter
ISO	Information Security Officer
ISO/IEC	International Organization of Standardization/International Electro-technical Commission
IT	Informationstechnologie
IT-SiBe	IT-Sicherheitsbeauftragter
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT
KRITIS	Kritische Infrastruktur
NIS2	Network and Information Security Directive v2 (EU-Richtlinie 2022/2555)
NIST	National Institute of Standardization and Technology
PCI DSS	Payment Card Industry Data Security Standard
TISAX®	Trusted Information Security Assessment Exchange
TKG	Telekommunikationsgesetz
VAIT	Versicherungsaufsichtliche Anforderungen an die IT
VdS	Verband der Schadensversicherer

Abstimmungstabelle

Empfänger	Organisation	RACI	Bemerkung
Vorstand	CISO Alliance e.V.	A	
Arbeitskreis	CISO Alliance e.V.	R	
Mitglieder	CISO Alliance e.V.	C/I	
Alle	Externe	I	Nach offizieller Freigabe

RACI Legende: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed

Tabelle 1: RACI Abstimmungstabelle[1]

Verbundene Dokumente

Stammpfad:

Dokumentenname	Ablageort
Berufsethik der Informationssicherheit (erscheint bei der CISO Alliance in 2024)	NA

[1] **Responsible** - verantwortlich (**Durchführungsverantwortung**), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (durch Andere) gibt oder die die Aktivität selbst durchführt.
Accountable - rechenschaftspflichtig (**Kostenverantwortung**), verantwortlich im Sinne von „genehmigen", „billigen" oder „unterschreiben". Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.
Consulted - konsultiert (**Fachverantwortung**). Eine Person, deren Rat eingeholt wird. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
Informed - zu informieren (Informationsrecht)

Aufgabenbeschreibung CISO

Gesetzliche Grundlagen / Verknüpfungen

Regulatorische Anforderungen: BNetzA, BaFin-Vorgaben (BAIT, VAIT, KAIT etc.), …
Gesetze: IT-Sicherheitsgesetze, BSI-KRITIS Verordnung, NIS2, DORA, …
Allgemeine Standards: ISO/IEC 27001 (international), BSI IT-Grundschutz (DACH), NIST (USA), …
Branchen-Standards: TISAX® (Automotive), PCI DSS (Kreditkarten), VdS 10000, HIPAA, …

Organisatorische Einordnung

Der CISO ist das Bindeglied zwischen der Organisationsleitung (Geschäftsführung, Vorstand etc.) bzw. dem operativen Management des Unternehmens und der Informationssicherheit. Er steht in engem Kontakt mit den Stakeholdern des Kerngeschäfts und koordiniert die Zusammenarbeit mit ihnen, um die Schutzbedarfe ihrer Informationen und Geschäftswerte zu gewährleisten.

Hierzu verfügt er über ein klares Verständnis von der Geschäftsstrategie des Unternehmens und ein effektives Netzwerk zu den Stakeholdern des Kerngeschäfts. Er ist in der Lage, aus dem Geschäftsmodell des Unternehmens die Anforderungen an die Informationssicherheit zu identifizieren. Er kann in Bezug auf die Informationssicherheit direkt an die Führungsebenen des Unternehmens und die Organisationsleitung eskalieren und ist berechtigt, Entscheidungen zur Informationssicherheit zu treffen.

Die Gesamtverantwortung und Haftung (“Accountability”) bleibt naturgemäß immer bei der Organisationsleitung. Die operative Verantwortung für Informationssicherheit wird an den CISO delegiert (“Responsibility”).

Abgrenzungen

Die nachfolgenden Rollen oder Rollenbezeichnungen existieren im Umfeld der Informationssicherheit ebenfalls und sind, sofern in direktem Zusammenhang mit der Informationssicherheit und nicht gesetzlich geregelt, in separaten Dokumenten beschrieben.

- DSB (Datenschutzbeauftragter)
    - Pflicht-Rolle aus gesetzlicher Anforderung mit Pflichten und Aufgaben im Rahmen von DSGVO und weiterer Datenschutzgesetzgebung
    - Vertritt die Interessen der Betroffenen innerhalb und außerhalb der eigenen Organisation
    - Teilweise getrennt vom CISO, teilweise gleiche Person (wenn, dann potentieller Interessenskonflikt)
- Datenschutzmanager oder Datenschutzkoordinator
    - Setzt die Anforderungen des Datenschutzes in seiner Organisation um
    - Personalunion mit dem CISO möglich und sinnvoll
- TKG-Sicherheitsbeauftragter
    - Pflicht-Rolle aus gesetzlicher Anforderung mit Pflichten und Aufgaben nach TKG §166
- IT-Sicherheitsbeauftragter (IT-SiBe)
- Informationssicherheitskoordinator
- ISO (Information Security Officer) / ISB (Informationssicherheitsbeauftragter)
- Bereichs-ISB
- Business-ISO (BISO)
- CSO (Corporate Security Officer/Chief Security Officer)

Die Rollenbezeichnungen IT-Sicherheitsbeauftragter, ISO oder ISB werden in der Praxis teilweise als Synonym für die Rolle CISO verwendet. In solchen Fällen sollte ein Abgleich des Aufgabenprofils mit dem Berufsbild erfolgen und eine Umbenennung der Rolle erwogen werden.

Qualifikation

- Ausbildung: Hochschulabschluss, vergleichbare Ausbildung, vergleichbare Berufserfahrung
- Einschlägige langjährige Berufserfahrung (mindestens 5 Jahre) in Informationssicherheit, Geschäftsprozessen, Management sowie ein globales Wissen über die Zusammenhänge von IT-Strukturen und IT-Sicherheit; einige Jahre eigene Erfahrung in IT-Abteilungen sind von Vorteil
- Fachliche Zertifizierungen (gültig & aktiv): CISM®, CISSP, ISO/IEC 27001 Implementer, etc.
- Perspektivisch CISO Alliance Zertifizierung

Kompetenzen

Persönliche Kompetenzen

- Hohes Sicherheitsbewusstsein und persönliche Identifikation mit den Zielen der Informationssicherheit und den Geschäftszielen
- Bereitschaft zur Zusammenarbeit und ausgezeichnete Kommunikationsfähigkeiten
- Analytische Kompetenzen zur Aggregation und Abstraktion von Daten und Erkennen von Mustern und Auffälligkeiten verbunden mit der Kompetenz, Informationen zielgruppengerecht aufzubereiten
- Kreativität und die Fähigkeit, in neuen Situationen lösungsorientiert Alternativen zu entwickeln sowie andere Denkweisen und Perspektiven einzunehmen
- Strategische Kompetenz zur Einordnung des Themas Informationssicherheit in die Aufgaben, Ziele und Geschäftsprozesse des Unternehmens
- Zielgruppengerechte Kommunikation, Enabler und Übersetzer zwischen Geschäfts- und Informationssicherheitsperspektive
- Die Fähigkeit, auch in stressigen Situationen Ruhe zu bewahren
- Durchsetzungsvermögen und Führungsfähigkeiten
- Fähigkeit, mehrere Initiativen gleichzeitig bearbeiten zu können und nach Dringlichkeit und Wichtigkeit zu priorisieren
- Innovationsfähigkeit und die Fähigkeit, technologische Innovationen in Bezug auf Informationssicherheitsanforderungen grundsätzlich zu bewerten und diese Anforderungen weiterzuentwickeln

Fachliche Kompetenzen

- Wissen und Erfahrung auf den Gebieten der Informationssicherheit und IT bezüglich Bedrohungen/Gefahren und Sicherheitslösungen; Kenntnisse in der Anwendung technischer Maßnahmen und Prozesse
- Gestaltung und Umsetzung vonSensibilisierungs-Maßnahmen auf allen Mitarbeiter- und Management-Ebenen zur Förderung einer Informationssicherheitskultur
- Vermittlung zwischen Informationssicherheit und fachlichen sowie technischen Organisationsbereichen
- Kompetenz der Erstellung und Überarbeitung von regelnden Dokumenten sowie der Herstellung des geschäftsrelevanten Kontextes
- Informationsrisikomanager: Methodenkompetenz zur Durchführung von Bedrohungs- und Risikoanalysen und Ableitung von Maßnahmen sowie der Bewertung der Effektivität oder Effizienz der Umsetzung von Maßnahmen
- Verständnis für Datenschutzvorschriften und -bestimmungen, insbesondere in Bezug auf die Anforderungen an den Schutz personenbezogener Daten
- Vertrautheit mit Cloud-Sicherheit sowie den spezifischen Herausforderungen und Best Practices im Cloud Computing

Verantwortlichkeiten

- Definition und Kommunikation einer Informationssicherheits-Strategie, die an der Geschäfts- und IT-Strategie des Unternehmens ausgerichtet ist
- Erstellung einer Informationssicherheitsleitlinie
- Regelmäßiger Bericht zum Status der Informationssicherheit an die Organisationsleitung
- Betrieb des ISMS für den definierten Anwendungsbereich
- Regelmäßige Auditierung der Organisation in Bezug auf die Informationssicherheit
- Definition, Umsetzung und kontinuierliche Prüfung/Steuerung eines Informationssicherheits-Prozesses für die gesamte Organisation
- Kontinuierliche Schulung und Sensibilisierung der Mitarbeiter zu relevanten Themen
- Erstellung und Pflege der Dokumente zur Informationssicherheit
- Unterstützung bei der Definition und Wirksamkeitsüberprüfung von Maßnahmen der Informationssicherheit
- Untersuchung, Dokumentation und Bewertung von neuen oder geänderten Anforderungen an die Informationssicherheit (in Abstimmung mit den Information-Asset-Ownern)
- Untersuchung, Nachverfolgung und Bewertung von neuen oder geänderten Anforderungen an die Informationssicherheit
- Entwicklung, Umsetzung und Koordination von Awareness-Maßnahmen zur Informationssicherheit
- Fachliche Leitung des Informationssicherheitsteams im Anwendungsbereich des ISMS
- Beratung der gesamten Organisation zu allen Themen der Informationssicherheit
- Zentraler Ansprechpartner bei externen Audits zur Informationssicherheit
- Bewertung von Drittanbietern und Lieferanten hinsichtlich ihrer Sicherheitspraktiken und -standards sowie Durchführung von Lieferantenaudits zur Informationssicherheit
- Oberster Informationsrisikomanager (Führen des Risikoregisters und Unterstützung des operativen Risikomanagements)
- Umfassende Information der Leitung zur Sicherstellung bewusster Risikoentscheidungen
- Mitarbeit bei der Auswahl, Implementierung und Überwachung von Sicherheitstechnologien und -tools als von der IT-Sicherheit vorgeschlagene Risikomitigationsmaßnahmen
- Umsetzung der internen Datenschutzvorgaben in Abstimmung mit dem Datenschutzmanager/Datenschutzkoordinator, insbesondere in Branchen mit strengen Compliance-Anforderungen wie dem Gesundheitswesen oder der Finanzindustrie
- Zusammenarbeit mit internen und externen Behörden oder Institutionen, um auf Sicherheitsvorfälle angemessen zu reagieren und gesetzlichen Anforderungen gerecht zu werden

Berufsethik

Die Berufsethik eines CISOs richtet sich nach der „Berufsethik der Informationssicherheit“ (erscheint bei der CISO Alliance in 2024).

Ausschlüsse zur besseren Klarstellung

Diese Aufgaben gehören nicht zum Verantwortungsbereich des CISOs:

- Ein CISO verantwortet und plant keine Geschäftsprozesse
- Er ist nicht verantwortlich für die Umsetzung der Anforderungen an die Informationssicherheit in Geschäftsprozessen
- Er trifft eigenständig keine weitreichenden Risikoentscheidungen
- Der CISO legt nicht den Risikoakzeptanzlevel fest

Der CISO sollte dennoch dafür sorgen, dass das Thema Informationssicherheit in Geschäftsprozessen einbezogen und eine Risikostrategie erstellt wird.

Anhang 1 Übersicht Standards, Richtlinien und Gesetze (ohne Anspruch auf Vollständigkeit) Stand: 3. März 2024

Titel	Aktuelle Fassung	Erscheinungsjahr	Kurzbeschreibung	Quelle(n)
ISO/IEC 27001 - Informationssicherheit	ISO/IEC 27001:2022	2022	Internationale Norm für Informationssicherheitsmanagementsysteme (ISMS).	https://www.iso.org/standard/54534.html
ISO/IEC 27002 - Leitfaden für Informationssicherheitsmaßnahmen	ISO/IEC 27002:2022	2022	Ergänzender Leitfaden zur ISO/IEC 27001 für Informationssicherheitsmaßnahmen.	https://www.iso.org/standard/54533.html
IT-Grundschutz (BSI)	IT-Grundschutz 200-1, 200-2, 200-3	2017	Deutsche Methode zur Umsetzung von IT-Sicherheitsmaßnahmen.	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kurzbeschreibung/Kurzbeschreibung.html
EU-DSGVO - Datenschutz-Grundverordnung	EU-DSGVO	2018	Datenschutzregelung für die Europäische Union.	https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679
BSI-Gesetz (BSIG)	BSI-Gesetz	1990	Gesetz zur Stärkung der IT-Sicherheit in Deutschland.	https://www.gesetze-im-internet.de/bsig/BJNR258810010.html
IT-Sicherheitsgesetz (IT-SiG)	IT-Sicherheitsgesetz	2015	Deutsches Gesetz zur Erhöhung der IT-Sicherheit kritischer Infrastrukturen.	https://www.gesetze-im-internet.de/it-sig/BJNR267610015.html
KRITIS-Verordnung	KRITIS-Verordnung	2016	Verordnung zur Bestimmung kritischer Infrastrukturen in Deutschland.	https://www.gesetze-im-internet.de/kritisv/BJNR108710016.html

Titel	Aktuelle Fassung	Erscheinungsjahr	Kurzbeschreibung	Quelle(n)
IT-Sicherheitsgesetz 2.0	IT-Sicherheitsgesetz 2.0	2021	Aktualisierte Version des deutschen IT-Sicherheitsgesetzes.	Aktuelle Informationen bei Bundesministerium für Inneres, Bau und Heimat
NIS2-Richtlinie (Network and Information Security Directive v2)	EU 2022/2555	2022	EU-Richtlinie zur Stärkung der Netz- und Informationssicherheit.	Aktuelle Informationen bei der Europäischen Kommission https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/diskussionspapier-NIS-2-umsetzung.html
NIST SP 800-53 - Sicherheitskontrollen	NIST SP 800-53 Rev. 5	2020	US-amerikanischer Standard für Informationssicherheitskontrollen.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
PCI DSS - Payment Card Industry Data Security Standard	PCI DSS 4.0	2022	Sicherheitsstandard für Zahlungskarteninformationen.	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
HIPAA - Health Insurance Portability and Accountability Act	HIPAA	1996	US-amerikanisches Gesetz zum Schutz von Gesundheitsdaten.	https://www.hhs.gov/hipaa/index.html
TISAX® - Trusted Information Security Assessment Exchange	TISAX 6	2023	Branchenspezifisches Sicherheitsbewertungssystem für die Automobilindustrie.	
DORA – Digital Operational Resilience Act	EU 2022/2555	2022	Lex specialis Finanz- und Versicherungswesen	https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html