Matthias Totzauer

Group CISO / Interim CISO | KRITIS, NIS2, ISMS, Cyber Resilience & Audit Readiness

matthias.totzauer@gmail.com | +49 162 5922574 | Wunsiedel, Deutschland | Reisebereitschaft nach Vereinbarung

CISSP | CISM | ISO 22301 Lead Auditor | AICRS | CISA Exam Passed | Datenschutzbeauftragter

LEADERSHIP	REGULATION	FRAMEWORKS	DELIVERY
Group CISO / Interim CISO	**NIS2, KRITIS, BSI C5, SOC 2**	**ISO 27001, ISO 22301, NIST, IEC 62443**	**Audit- & Umsetzungsexzellenz**
Security-Programme, Gremienarbeit, C-Level Reporting	Readiness, Control Mapping, Evidenzführung	ISMS, BCM, Cyber Resilience, OT Security	GAP-Analysen, Maßnahmen-Backlogs, Finding Closure

Executive Profile

Senior Cybersecurity- und Informationssicherheitsmanager mit CISO-/Interim-CISO-Verantwortung in internationalen, regulierten und sicherheitskritischen Umfeldern. Schwerpunkt auf Aufbau und Steuerung prüffähiger ISMS-, Governance- und Cyber-Resilience-Strukturen nach ISO/IEC 27001, ISO 22301, NIS2, KRITIS, BSI C5, SOC 2, NIST CSF und IEC 62443. Verbindet strategische C-Level-Kommunikation mit operativer Umsetzungsstärke in IT-/OT-Umgebungen, Audit-Readiness, Risiko- und Krisenmanagement.

KERNPROFIL & SECURITY LEADERSHIP

Group CISO / Interim CISO	**NIS2- & KRITIS-Umsetzung**	**BSI C5 & SOC 2 Readiness**
ISMS nach ISO/IEC 27001	**BCM / ISO 22301**	**NIST CSF & IEC 62443**
IT-/OT-Security Governance	**Audit-Readiness & Evidence**	**Risk, Incident & Crisis Management**
C-Level Reporting	**Policy & Control Frameworks**	**Healthcare, Industry & Utilities**

AKTUELLE ANONYMISIERTE MANDATE

Seit 05/2026
laufend

Anonymisiertes Mandat - Industrieunternehmen / Hebezeugtechnik

Cybersecurity Advisory | NIS2-Readiness | Governance & Controls

- Betreuung des Mandanten zu allen wesentlichen Cybersecurity-Themen inklusive NIS2-GAP-Analyse, Risikobewertung und Umsetzungs-Roadmap.
- Ableitung technischer und organisatorischer Maßnahmen für ein prüffähiges Security- und Governance-Modell im industriellen Umfeld.
- Aufbau managementfähiger Reports, Maßnahmen-Backlogs und Entscheidungsunterlagen für Geschäftsführung und Fachbereiche.

Seit 09/2025
laufend

Anonymisiertes Mandat - KRITIS-/Versorgungsgruppe

Cybersecurity | NIS2 | KRITIS | BSI C5 | SOC 2 | Audit Readiness

- Betreuung in Cybersecurity-Governance, NIS2-Umsetzung, KRITIS-Anforderungen sowie Aufbau prüfbarer Kontroll- und Evidenzstrukturen.
- BSI-C5- und SOC-2-Readiness inklusive Control Mapping, GAP-Analyse, Nachweisführung und Remediation-Tracking.
- Abstimmung zwischen Management, IT, OT, Compliance, Datenschutz, Prüfern und externen Dienstleistern.

BERUFLICHE ERFAHRUNG

11/2023 - heute
Deutschland / Interim & Consulting

IT Consulting Totzauer - IT Security Consulting

Informationssicherheit, Cybersecurity Governance, ISMS, Audit Readiness, NIS2/KRITIS

- Aufbau, Weiterentwicklung und Auditvorbereitung von ISMS nach ISO/IEC 27001/27002 für Mittelstand, Konzerne und IT-Dienstleister.
- Durchführung strukturierter GAP-Analysen, Risikoanalysen und Kontrollbewertungen aus Auditoren-Sicht.
- Steuerung von NIS2-, KRITIS-, BSI-C5- und SOC-2-Readiness-Programmen inklusive Management-Reporting und Maßnahmensteuerung.
- Etablierung prüfbarer Prozess-, Kontroll- und KPI-Landschaften mit messbarer Reduktion kritischer Audit-Findings.

01/2025 - 09/2025
Deutschland | C-Level Reporting

BHS Corrugated - Manager Cybersecurity

Hersteller von Corrugators | IT-/OT-Cybersecurity | Governance Framework

- Aufbau und operative Leitung der Cybersecurity-Organisation mit Fokus auf IT- und OT-Umgebungen.
- Entwicklung eines gruppenweiten Cybersecurity-Governance-Frameworks auf Basis von ISO 27001, IEC 62443 und NIS2.
- Einführung zentraler Monitoring-, Reporting- und Incident-Response-Prozesse sowie Risikoberichterstattung an die Geschäftsleitung.

10/2023 - 06/2025
Duisburg | Reporting: Vorstand

Xella Group - Group CISO (Interim)

Baustoffhersteller | Globale Informationssicherheit | Security Governance

- Strategische Leitung unternehmensweiter Informationssicherheitsprogramme und globaler Governance-Strukturen.
- Führung internationaler InfoSec-Teams sowie risikobasierte Steuerung präventiver Kontrollmechanismen.
- Sicherstellung regulatorischer Compliance nach ISO/IEC 27001/27002 und NIS2; Integration des NIST Cybersecurity Frameworks.

03/2022 - 10/2023
Ansbach | Reporting: CEO

Gala Group GmbH - Group Head of Information Security

Internationaler Non-Food-Hersteller | ISMS, SOC, SAP S/4HANA Security

- Aufbau eines internationalen ISMS auf Basis von ISO 27001 und BSI IT-Grundschutz.
- Implementierung moderner Security-Architekturen mit CrowdStrike, Proofpoint, SIEM, Cisco und Microsoft.
- Leitung internationaler IT-Sicherheitsprojekte inklusive SOC-Verantwortung und Integration von Sicherheitsmaßnahmen in SAP S/4HANA.

04/2019 - 02/2022
DACH | Reporting: CEO

naip Group - IT Manager (Supply Chain IT, IT Security, IT Services)

Healthcare Produktlieferant und Dienstleister | ERP, Cloud, Security, Datenschutz

- Verantwortung für IT-Security, Supply Chain IT und IT Services im Healthcare-Umfeld.
- Implementierung ISO-27001- und DSGVO-konformer Sicherheitslösungen sowie Leitung internationaler Teams.
- Steuerung von Digitalisierungsprogrammen, Patienten-Apps, Cloud-Systemen und Schnittstellen in komplexen Supply-Chain-Strukturen.

10/2014 - 02/2022
International | Consulting

ITCST - IT Consultant

Industrie, Automotive, Healthcare, Lebensmittel/Supply Chain | Security & Transformation

- Einführung des NIST Cybersecurity Frameworks und Durchführung strukturierter IT-Sicherheitsaudits nach ISO/IEC 27001, 27002, 27005 und BSI IT-Grundschutz.
- Begleitung von TISAX-Zertifizierungen von der Reifegradanalyse bis zur erfolgreichen Auditierung.
- Konzeption von IT-Sicherheitsarchitekturen, ERP-/Cloud-Landschaften und Business-Continuity-Strukturen in internationalen Projekten.

03/2017 - 04/2019
Deutschland | Reporting: CEO

MTS - CIO

Healthcare Produktlieferant und Dienstleister | ERP, Cloud, Security, Datenschutz

- CIO-Verantwortung für ERP, Cloud, Security, Datenschutz, Backup, KIS-Schnittstellen und Supply-Chain-Systemlandschaften.
- Implementierung ISO-27001-konformer Sicherheitsmaßnahmen sowie DSGVO-konformer Datenschutz- und IT-Sicherheitsprozesse.

05/2015 - 08/2018
Oberpfalz

Bistum Regensburg - Interim Projektmanager Datenschutz & ISMS

Kirchlicher Datenschutz, ISMS, Risikoanalysen

- Implementierung kirchlicher Datenschutzrichtlinien und ISMS-Strukturen nach ISO/IEC 27001/27002.
- Durchführung von Risikomanagementmaßnahmen nach ISO/IEC 27005 sowie Sicherstellung der DSGVO-Konformität.

10/2014 - 07/2016
Weltweiter Einsatz | Reporting: CEO

Saguna GmbH - IT Manager (Projektrolle)

Healthcare Produkt Hersteller | NAV, CRM, Cloud, Infrastruktur

- Einführung von NAV 2016, CRM, Shop-Systemen und digitalen Prozessen zur Unterstützung internationaler Geschäftsprozesse.
- Aufbau europäischer IT- und Cloud-Infrastrukturen inklusive VM-, SQL-, Firewall-Cluster- und DMS-Systemen.

01/2006 - 02/2016
Europaweit | Reporting: CEO

Markgraf Bau - IT Manager

Bauunternehmen | Infrastruktur, Rechenzentrum, Virtualisierung, BCM

- Konzeption, Aufbau und Betrieb europaweiter IT-Infrastrukturen, Cloud- und Virtualisierungsumgebungen.
- Durchführung von Rechenzentrumsumzügen, Einführung von VOIP und Umsetzung von Business-Continuity-Maßnahmen.

REGULATORIK, AUDIT & WIRKUNG

Regulation & Audit

- NIS2, KRITIS, BSI-Gesetz, BSI C5, SOC 2, ISO 27001, ISO 22301, TISAX
- Readiness-Assessments, Audit-Checklisten, Evidenzen, Finding-Management
- Control Mapping, KPI-Reporting, Management-Entscheidungsvorlagen

IT/OT & Security Operations

- IT-/OT-Governance, IEC 62443, NIST CSF, Secure Infrastructure
- SOC, SIEM, Incident Response, Monitoring, Vulnerability & Risk Management
- IAM/PAM, Cloud Security, Endpoint, Netzwerk- und Plattform-Sicherheit

Industrie & regulierte Umfelder

- KRITIS-/Versorgungsumfelder, Fertigungsindustrie, Healthcare, Supply Chain
- SAP S/4HANA, Dynamics/NAV, ERP, Cloud- und Schnittstellenlandschaften
- Zusammenarbeit mit Management, Datenschutz, Fachbereichen und Prüfinstanzen

Wirkung & Führungsprofil

- Aufbau internationaler Security-Organisationen und Entscheidungsstrukturen
- Reduktion kritischer Audit-Findings und Verkürzung von Auditlaufzeiten
- Übersetzung regulatorischer Anforderungen in realistische Umsetzungsprogramme

ZERTIFIKATE & QUALIFIKATIONEN

CISSP	**Certified Information Systems Security Professional - ISC2**	2025
CISM	**Certified Information Security Manager - ISACA**	seit 2023
ISO 22301 LA	**ISO 22301:2019 BCMS Certified Lead Auditor - GIPMC**	2025-2028
AICRS	**AI Cyber Security & Risk Specialist - GIPMC**	2026-2029
CISA Exam	**CISA-Prüfung bestanden - ISACA**	Designation nicht als Zertifizierung geführt
DSB	**Datenschutzbeauftragter nach DSC-Standard**	2018
Scrum Master	**Scrum Master - Agile Akademie / Scrum.org**	2017 / 2023
IHK	**IT System Engineer - IHK Regensburg**	2005

SPRACHEN & VERFÜGBARKEIT

Deutsch	Englisch	Tschechisch	Verfügbarkeit
Muttersprache	verhandlungssicher	Grundkenntnisse	Fest / Advisory / Interim | Reise n.V. | A/B