MANDATSPROFIL INTERIM CISO

Martin Bischoff

Partner, 4T2 Solutions GmbH



Interim CISO, Regulatory Readiness und Security Governance in hochregulierten Umgebungen.

VERFÜGBARKEIT	PENSUM	EINSATZORT	SPRACHEN
ab sofort	80 bis 100 %	Ostschweiz, Zürich, Bern, Liechtenstein, remote DACH	Deutsch, Englisch

PROFIL

Informationssicherheit in regulierten Umgebungen seit 2005, bei der VP Bank zuletzt als Head of IT Risk Management und Information Security im Rang eines Vizedirektors. Aufbau von Managementsystemen nach ISO 27001, Vorbereitung und Begleitung aufsichtsrechtlicher Prüfungen sowie Führung von Security-Programmen an der Schnittstelle zwischen Aufsicht, Management und Technik.

Der Schwerpunkt liegt auf der Übersetzung regulatorischer Anforderungen in belastbare Sicherheitsarchitekturen, auditfähige Governance-Strukturen und steuerbare Programme. Direkte Zusammenarbeit mit den Prüfern der Bundesbank, Umsetzung von Anforderungen aus BAIT, MaRisk und BaFin, Zertifizierungserfahrung als Projektleiter.

28	ISO 27001	ISO 20000	45
Jahre IT, Netzwerk und Informationssicherheit	ISMS bei Bank und Börse aufgebaut	als Projektleiter, erste Bank Europas	Consultants gesteuert

SCHWERPUNKTE

Security Governance. Aufbau und Weiterentwicklung von ISMS nach ISO 27001, Risikomethodik, Rollenmodelle, Weisungswesen und Management-Reporting.

Regulatory Readiness. DORA, NIS2, BAIT und MaRisk. Gap-Analysen, Massnahmensteuerung und Begleitung von Sonderprüfungen bis zur Nachschau.

Detect and Response. SIEM- und SOC-Aufbau, Logging- und Monitoring-Strategie, Incident Response, Betriebsmodelle mit externen Partnern und Segregation of Duties.

Technische Härtung. Kryptografie und PKI, Netzwerksegmentierung und Zero Trust, Identity and Access Management, Patch- und Vulnerability-Management.

AUSGEWÄHLTE ERGEBNISSE

- VP Bank: ISMS nach ISO 27001 und Methodik zur Bewertung von IT-Risiken aufgebaut und in das operationelle Risikomanagement integriert.
- VP Bank 2007 nach ISO 20000 zertifiziert, als erste Bank Europas und dritte weltweit, unter eigener Projektleitung.
- Einen Börsenbetreiber auf eine aufsichtsrechtliche Prüfung vorbereitet und bis zur Nachschau begleitet.
- ISMS-Handbuch, Klassifizierungsschema nach VIVA und IAM-Governance für einen Börsenbetreiber aufgebaut.
- Cyber-Security-Team bei QESTIT von 0 auf 6 Personen aufgebaut, inklusive Portfolio und Go-to-Market.
- Mehrjährige Cyber-Security-Strategie für eine Gruppen-IT erarbeitet und mit dem Management verankert.

ZERTIFIZIERUNGEN

- CISSP (ISC²), seit 2020
- ITIL Expert in IT Service Management
- HERMES Foundation 5.1 (TÜV SÜD)
- Erweiterte Personensicherheitsprüfung VBS, 2019

WEITERBILDUNG

- ISACA AAISM, AI Security Management (in Ausbildung)
- ISO 27001 Lead Auditor, Ausbildung
- HERMES 5 Advanced (Berner Fachhochschule)
- Fachkraft für Datenschutz (DEKRA)
- Swiss Finance Institute, Executive Program

FRAMEWORKS

- ISO 27001 und ISO 27002
- DORA
- NIS2
- BAIT und MaRisk
- NIST CSF
- CIS Controls
- COBIT
- ISO 31000
- EU AI Act

TECHNOLOGIEN

- QRadar SIEM
- Tenable
- CRISAM GRC
- Palo Alto
- CrowdStrike
- Cisco
- VMware
- Python
- Kali und Ubuntu Linux
- KI-Agenten und RAG

PUBLIKATIONEN

- stop.li, eigene Fachbibliothek
- AI Act Framework für Finanzinstitute, 91 Seiten
- Informationssicherheitsrichtlinie DCH
- ISMS-Prozesslandkarte, 25 Prozesse
- CRA-Paket für KMU

Beruflicher Werdegang

QESTIT AG, Schweiz 04/2023 bis 06/2026

Managing Director Schweiz und Head of Cyber Security Consulting DACH

Gesamtverantwortung für Markt, Organisation und Ergebnis der Schweizer Einheit. Parallel Aufbau und strategische Leitung des Cyber-Security-Consultings in der DACH-Region. Mitglied des dreiköpfigen DACH-Management-Teams.

- Aufbau des Cyber-Security-Teams von 0 auf 6 Personen inklusive Strategie, Portfolio, Pricing-Modellen und Go-to-Market.
- Leitung regulatorischer Security-Programme mit Schwerpunkt Audit Readiness, Detect and Response, SIEM, SOC, Kryptografie sowie Patch- und Vulnerability-Management.
- Aufbau von Beratungsleistungen in Governance, Risk und Compliance, Security Architecture und Penetration Testing.
- Disziplinarische Führung von 15 Mitarbeitenden, Gesamtsteuerung von rund 45 Consultants aus der Schweiz, der Gruppe und dem externen Markt.
- P&L-Verantwortung mit einem Umsatzbudget bis CHF 9 Mio.

KUNDENVERANTWORTUNG BEI QESTIT

ACCOUNT	VERANTWORTUNG
Börse Stuttgart	Security-Stream im Transformationsprogramm Phoenix, mehrjährige Cyber-Security-Strategie und Detect and Response. Schwerpunkte DORA, NIS2, ISMS, Kryptografie, SIEM, SOC, Incident Response, Netzwerksegmentierung sowie Patch- und Vulnerability-Management.
WM Datenservice	Key Account Manager und Testmanager des Gesamtmandats im Programm Fontus. Verantwortung für Delivery, Eskalationen und Mandatsausbau auf bis zu 46 Mitarbeitende.
Swisscom	Executive-Kundenverantwortung im Umfeld Infrastruktur-Transformation und grossskaliger Rollout-Programme.

Weitere Key Accounts: Helvetia, Allianz, Die Mobiliar, PostFinance, Worldline, Generali.

4T2 Solutions GmbH seit 11/2015

Gründer, Geschäftsführer und Senior Executive Consultant

Leitung komplexer, sicherheitskritischer Programme und Beratungsmandate in hochregulierten Branchen. Schwerpunkt auf Cyber-Security-Governance, ISMS, DORA, DSGVO, NIS2, Audit Readiness sowie sicherer Infrastruktur- und Rechenzentrums-Transformation.

- Leitung technischer Grossprojekte im Finanzumfeld, im militärischen Umfeld und in der öffentlichen Verwaltung mit bis zu 50 Beteiligten im eigenen Stream.
- Audits und Gap-Analysen entlang BaFin-Anforderungen sowie Überführung regulatorischer Vorgaben in operative Security-Strukturen.
- Aufbau sicherer IT-Infrastrukturen, Rechenzentren, Netzwerkarchitekturen und Governance-Prozesse.

Börse Stuttgart, Kunde seit 2012. Mandate 2012 bis 2016 sowie 2019 bis 2025 über Core Wirtschaftsinformatik, 4T2 Solutions und QESTIT in einem hochregulierten Umfeld.

WM Datenservice 01/2026 bis 06/2026, über QESTIT

Teilprojektleitung Testmanagement im Programm Fontus zur Einführung eines neuen Core-Systems. Verantwortung für 46 externe Mitarbeitende, Teststrategie, Testplanung und Steuerung der Testdurchführung bis zum Ramp-down nach Abschluss der Testphase.

Börse Stuttgart 06/2025 bis 12/2025, über QESTIT

Leitung der prüfungssicheren Ausgestaltung der Detect-and-Response-Fähigkeiten im Rahmen der Nachschau zu einer aufsichtsrechtlichen Prüfung. End-to-End-Verantwortung für Detection, Incident Response und SOC-Governance, Logging- und Monitoring-Strategie, Steuerung des QRadar-Betriebsmodells inklusive Segregation of Duties. Zentrale Schnittstelle zu den Prüfern der Bundesbank.

Börse Stuttgart 12/2024 bis 03/2025, über QESTIT

Erstellung einer mehrjährigen Cyber-Security-Strategie gemeinsam mit dem Leiter Group IT Security. Strukturierung der Handlungsfelder für Security-Governance, technische Härtung und regulatorische Anschlussfähigkeit sowie Priorisierung entlang Wirksamkeit und Umsetzbarkeit.

Börse Stuttgart 04/2023 bis 12/2024, über QESTIT

Gesamtverantwortung für den Security-Stream AP17 im Transformationsprogramm Phoenix. Übersetzung der Vorgaben aus DORA und NIS2 in technische Massnahmen, Aufbau von Vulnerability- und Patch-Management über heterogene Plattformen, Zielbild Netzwerksegmentierung und Zero Trust, Kryptografiekonzept entlang Data at Rest, in Transit und in Use inklusive PKI.

Swisscom 02/2022 bis 08/2023, über 4T2 Solutions

Leitung eines unternehmensweiten Rollouts sicherheitsrelevanter Agenten auf rund 10'000 Servern in einem skalierten agilen Umfeld. Steuerung über mehrere ARTs hinweg, Orchestrierung der Abhängigkeiten zwischen Infrastruktur, Applikationsteams und Plattformverantwortlichen, Integration in hybride On-Prem- und Private-Cloud-Umgebungen.

RUAG 04/2020 bis 12/2021, über 4T2 Solutions

Projektleitung der IT-Zentralisierung von 36 technisch-wissenschaftlichen Infrastrukturen an 25 Standorten. Projektvolumen über CHF 3 Mio., Team mit 12 Mitarbeitenden. Aufbau der zentralen Zielumgebung mit Rechenzentrum, WAN, LAN, Security und Workplace. Direkte Berichterstattung an Geschäftsleitung und Verwaltungsrat.

Börse Stuttgart 11/2019 bis 12/2021, über 4T2 Solutions

Beratung und Vorbereitung auf eine aufsichtsrechtliche Prüfung. Umsetzung der Anforderungen aus BAIT und MaRisk, Erweiterung des ISMS inklusive Methodik, Rollenmodell und Risikoanalyseprozess, unternehmensweites ISMS-Handbuch, Klassifizierungsschema nach VIVA, IAM-Governance mit Joiner-Mover-Leaver-Prozessen, Gap-Analysen zu ISO 27001 und MaRisk.

RUAG 11/2018 bis 04/2020, über 4T2 Solutions

Projektleitung des Infrastruktur-Streams im Transformationsprogramm zur Entflechtung der RUAG-IT. Volumen über CHF 10 Mio., 50 Beteiligte im eigenen Stream. Migration von 2'500 Benutzern, Erneuerung des dezentralen Netzwerks und der Verkabelung an 20 Standorten, Rollout von 2'500 Clients, Migration der Exchange-Postfächer, Parallelbetrieb und Dekommissionierung der Altinfrastruktur.

Bank Julius Bär 04/2018 bis 11/2018, über 4T2 Solutions

Umsetzung zentraler DSGVO-Anforderungen mit Fokus auf Auskunfts- und Löschprozesse in einem heterogenen Applikationsumfeld. Konzeption der Auskunftsprozesse inklusive Reports, Datenextraktionen und ETL-Funktionen sowie Entwicklung eines Löschkonzepts.

Amt für Informatik, Fürstentum Liechtenstein 11/2015 bis 11/2016, über 4T2 Solutions

Projektleitung im Umfeld staatlicher IT-Infrastruktur. Konzeption und Planung der Integration der bestehenden IT-Infrastrukturen der Gemeinden Triesen und Vaduz in die zentrale Zielumgebung.

WEITERE MANDATE

MANDAT	SCHWERPUNKT
KPMG, 03/2016 bis 04/2017	Leitung der Entwicklung einer Applikation für internationales Steuerreporting auf Basis komplexer Bank-Transaktionsdaten inklusive Aufbau und Führung eines interdisziplinären Teams und Steuerung von Nearshore-Entwicklern.
Trivadis und EDEKA Nord, 02/2018 bis 04/2019	Einführung und Modellierung von ISMS-, DSMS- und DSGVO-Strukturen im GRC-Tool CRISAM inklusive Datenschutz-Folgenabschätzungen, Löschkonzepten und Enablement der internen Mitarbeitenden.
Clientis und Axon AG, 10/2017 bis 03/2018	Projektleitung zur Digitalisierung von Neukundenaufnahme und Kreditvergabe für Hypotheken auf Basis von Axon.ivy inklusive Anforderungsdefinition und Automatisierung risikoarmer Prozesse.
Swatch Group, 09/2017 bis 11/2017	Evaluation einer Lösung zur Abbildung von ISMS- und DSGVO-Anforderungen inklusive Anforderungskatalog und Stakeholder-Abstimmung.

Frühere Führungsrollen

Capco, The Capital Markets Company, Zürich 02/2011 bis 04/2012

Principal Consultant

Beratung im Umfeld Finanzmarktinfrastruktur und Datenmanagement.

- Projektleitung DerivateXXL, Standardisierung der Emissionsinformationen in XML, abgestimmt mit Scoach und zehn Emittenten.
- Projektleitung Datenmanagement inklusive Aufbau der Betriebs- und Aufbauorganisation.
- Projektleitung Stammdatenfeed verbriefte Derivate als mandantenfähiger Feed mit Qualitätspaketen je Abnehmer.

Core Wirtschaftsinformatik GmbH 2010 bis 2016

Geschäftsführer und Principal Consultant

Eigene Beratungsgesellschaft für Transformations- und Finanzmarktprojekte. Hauptmandat Börse Stuttgart.

- Streamlead Technisches Design im Transformationsprogramm zur Ablösung der Börsenplattformen XITARO und XONTRO durch Nasdaq Genium INET, rund EUR 16 Mio. Programmvolumen und 6'000 Personentage.
- Migration und Anpassung von 92 Handelsapplikationen, Schnittstellen und Datenfeeds sowie Konfigurationsanpassung von über 500 Windows-Servern.
- Projektleitung Aufbau und Betrieb eines BCM-Systems entlang MaRisk und BaFin inklusive Notfallplänen, Krisenorganisation, Wiederanlaufverfahren und ITSCM.
- Projektleitung und Konzeption eines ISMS auf Basis ISO 27001 und ISO 31000.
- Leitung von RFI- und RFP-Verfahren für ein Risikomanagementsystem inklusive Vertragsverhandlungen.

VP Bank AG, Vaduz 02/2005 bis 01/2010

Vizedirektor, zuletzt Head of IT Risk Management und Information Security

Laufbahn vom Leiter Systems Engineering über Head of IT Quality and Processes bis zum Head of IT Risk Management und Information Security. Ernennung zum Vizedirektor 2007.

- Projektleitung der ITIL-Reorganisation und der Zertifizierung nach ISO 20000 und ISO 9001. Die VP Bank wurde 2007 als erste Bank Europas und dritte Bank weltweit nach ISO 20000 zertifiziert.
- Design und Implementierung der ITIL-Prozesse sowie Aufbau der Funktion IT Service Desk inklusive Integration des ITSM-Tools Marval.
- Aufbau des ISMS nach ISO 27001 sowie einer Methodik zur Identifikation und Bewertung von IT-Risiken mit Integration in das operationelle Risikomanagement.
- Aufbau einer dynamischen Berechtigungsdatenbank für User-Accounts, Avaloq-Rechte und hochprivilegierte Benutzer als Grundlage für IAM und PAM.
- Evaluation und Outsourcing eines Rechenzentrums, Verantwortung für IT-Infrastrukturarchitektur, Storage, Server und Client.
- Planung und Durchführung interner Audits, Begleitung der Informatik-Audits der Revision.
- Führung von Teams bis 15 Mitarbeitende.

Cubenet AG, Schweiz 2000 bis 2005

Mitgründer, Geschäftsführer und Senior Network Architect

Gründung und Aufbau des Unternehmens mit operativer Gesamtverantwortung für Finanzen, Projektgeschäft und Delivery.

- Aufbau und Führung einer Organisation mit neun Mitarbeitenden.
- Anspruchsvolle Netzwerkarchitekturen und Remote-Zugriffslösungen, Consulting sowie wiederkehrende Service- und Wartungsverträge.

Credit Suisse, Zürich 12/1997 bis 09/2000

Telematiker, ab 10/1999 Leiter Network Engineering

Personelle und fachliche Leitung der Dienststelle Network Engineering mit sechs Mitarbeitenden, Verantwortung für das Engineering des TCP/IP-Datennetzes Schweiz.

- Projektleitung Einführung Gigabit-Backbone und Infrastruktur des Server-Rechenzentrums mit Gigabit Ethernet und Layer-3-Switching.
- Aufbau eines schweizweiten ATM-Netzes gemeinsam mit Swisscom.
- Netzwerkprojekte zum Internetauftritt der Bank, darunter Directnet, Youtrade und Yourhome.

AUSBILDUNG

- Dipl. Wirtschaftsinformatiker, eidg. höhere Fachprüfung, 2000
- Elektroniker EFZ, Fachrichtung Geräte- und Anlagenbau, 1991
- Swiss Finance Institute, Executive Program, 2009

Martin Bischoff, Partner
4T2 Solutions GmbH, Wildensteinstrasse 10, 9404 Rorschacherberg
+41 78 892 7960 · mbischoff@4t2s.com · www.4t2s.com