Curriculum
Cyber, Cloud & Information Security

Full-time: 20 weeks / 5 months

German **Remote**

More security, clear standards, real resilience – your path into information security. Cloud, AI, and new regulations such as NIS2 are currently reshaping how organizations think about security. In our 20-week bootcamp, you'll learn to understand IT and cloud environments, assess risks in a structured way, and organize security so that it is auditable, compliant, and practical.

You'll combine technical fundamentals (networks, IAM, hardening, logging) with management expertise (ISO 27001, BSI IT-Grundschutz, risk analysis, business continuity management, GRC). By the end, you won't just be able to explain security measures — you'll be able to implement, document, and continuously improve them.

Future jobs for you:

- **Information Security Manager**
- **Compliance Manager (Security/GRC)**
- **Business Continuity Manager**
- **IT Security Manager**
- **AI / Cloud Governance Specialist**
- **Data Protection Officer (DPO)**

A Cybersecurity Specialist earns between 60.000 € and 90.000 € a year.

Tech Stacks

IT & Networking Fundamentals
- ICT key components & modern end device structure
- Operating Systems, OS controls & settings
- File Mgmt & Storage Media
- Network & Web Structure
- Network Components & Tools
- Web & Digital Comm, WWW structure, URLs

ICDL Computer
- ICT Literacy
- OS & File Management
- Web & Browser Use
- Email & Digital Comm
- Networking Concepts

Cybersecurity Concepts & Tools
- Cyber Threats & CIA Triad
- Security Controls & MFA
- SIEM Tools & Log Analysis
- Vulnerability & Risk Mgmt
- Cryptography & Encryption

Operating System & Cloud Security
- System Hardening & CIS
- Cloud IAM & RBAC Models
- Zero Trust Architecture
- AI Model Security Risks
- Endpoint Security Focus

Cybersecurity Projects & Practical Applications
- Risk Assessment Exercise
- Security Policy Drafting
- IR Phase Implementation
- Technical Documentation
- Security Reporting & Audits

ISC2 Certified in Cybersecurity (CC) Certification
- Security Principles (CIA)
- Access Control Basics
- Network Security Intro
- Security Ops & Risk
- Incident Response Found

AI Governance, EU AI Act, GDPR & Compliance
- NIS2 Directive Scope
- Foundations of the EU AI Act
- Risk Classification & Requirements for High-Risk AI Systems
- Security & Compliance Requirements for AI & Cloud Services
- Roles & Responsibilities Across the AI Lifecycle
- AI Compliance Assessment & Integration into Governance Processes
- IT-SiG 2.0 (Germany)
- Compliance Assessment

Business Continuity & Incident Management
- BCM & BIA Analysis
- Emergency Plans
- BAO Management
- BCM Risk Methodology
- Business Impact Analysis
- RTO/RPO Planning
- Emergency Response
- Testing & Auditing BCM

ISO 27001 & ISMS Frameworks
- ISO 27001 ISMS Lifecycle
- BSI Standards & Controls
- SoA & Documentation
- Risk Treatment Options
- ISMS Governance Model

Information Security Officer Certification
- ISMS Structure (ISO 27001)
- ISMS Policy Creation
- Security Governance
- Risk Management ISMS
- Legal Compliance (GRC)

Soft Skills

Click here for final projects

- **Communication Skills**
- **Creativity**
- **Domain Knowledge**
- **Problem Solving**
- **Collaboration**
- **Time Management**
- **Flexibility**
- **Ethical Considerations**

Certificate ISC2 CC

Certificate Information Security Officer (ISB)

Practical Project
Implementation of acquired knowledge in a real-life scenario.

Supported Job Search
We actively support job searches, offering regular networking events where participants connect with experienced tech professionals.

neue fische | SPICED

Curriculum
Cyber, Cloud & Information Security

Vollzeit: 20 Wochen / 5 Monate

Deutsch **Remote**

Mehr Sicherheit, klare Standards, echte Resilienz – dein Weg in die Informationssicherheit. Cloud, KI und neue Regulierung wie NIS2 verändern gerade, wie Unternehmen Sicherheit denken. In unserem 20-wöchigen Bootcamp lernst du, IT- und Cloud-Umgebungen zu verstehen, Risiken sauber zu bewerten und Sicherheit so zu organisieren, dass sie auditierbar, compliant und praxisnah ist.

Du kombinierst technische Basics (Netzwerke, IAM, Hardening, Logging) mit Management-Know-how (ISO 27001, BSI Grundschutz, Risikoanalyse, BCM, GRC). Am Ende kannst du Sicherheitsmaßnahmen nicht nur erklären – sondern umsetzen, dokumentieren und weiterentwickeln.

Zukunftsjobs für dich:

- **Information Security Manager**
- **Compliance Manager (Security/GRC)**
- **Business Continuity Manager**
- **IT Security Manager**
- **AI / Cloud Governance Specialist**
- **Data Protection Officer (DPO)**

Ein Cybersecurity Specialist verdient im Durchschnitt zwischen 60.000 € und 90.000 € im Jahr.

Tech Stacks

IT- und Netzwerkgrundlagen
- Informations- & Kommunikationstechnologie (IKT) & Aufbau moderner Endgeräte
- Betriebssysteme: Steuerung & Systemeinstellungen
- Dateiverwaltung & Speichermedien
- Netzwerk- & Webstruktur
- Netzwerkkomponenten & -werkzeuge
- Web- & digitale Kommunikation, Struktur des World Wide Web (WWW), URLs

ICDL Computerkenntnisse
- IKT-Grundkompetenz (ICT Literacy)
- Betriebssysteme und Dateiverwaltung
- Nutzung von Web und Browsern
- E-Mail & digitale Kommunikation
- Netzwerkkonzepte

Cybersicherheitskonzepte & -werkzeuge
- Cyberbedrohungen & die CIA-Triade
- Sicherheitskontrollen & Multi-Faktor-Authentifizierung (MFA)
- SIEM-Tools & Log-Analyse
- Schwachstellen- & Risikomanagement
- Kryptographie & Verschlüsselung

Betriebssystem- & Cloud-Sicherheit
- Systemhärtung & CIS-Benchmarks
- Cloud Identity & Access Management (IAM) & Role-Based Access Control (RBAC) Modelle
- Zero-Trust-Architektur
- Sicherheitsrisiken von KI-Modellen
- Endpunktsicherheit (Endpoint Security)

Cybersicherheitsprojekte & praktische Anwendungen
- Risikoanalyse-Übung (Risk Assessment)
- Erstellung von Sicherheitsrichtlinien
- Umsetzung von Incident-Response-Phasen
- Technische Dokumentation
- Sicherheitsberichte und Audits

ISC2 Zertifizierung: Certified in Cybersecurity (CC)
- Sicherheitsprinzipien (CIA-Triade)
- Grundlagen der Zugriffskontrolle
- Einführung in Netzwerksicherheit
- Security Operations und Risikomanagement
- Grundlagen der Incident Response

KI-Governance, Regulierung & Compliance
- EU AI Act & Governance-Frameworks
- DSGVO (GDPR) & Compliance
- Anwendungsbereich der NIS2-Richtlinie
- Grundlagen des EU AI Act
- Risikoklassifizierung & Anforderungen für Hochrisiko-KI-Systeme
- Sicherheits- & Complianceanforderungen für KI- und Cloud-Services
- Rollen und Verantwortlichkeiten im KI-Lebenszyklus
- KI-Compliance-Bewertung & Integration in Governance-Prozesse
- IT-Sicherheitsgesetz 2.0 (Deutschland)
- Compliance-Bewertung

Business Continuity & Incident Management
- Business Continuity Management (BCM) und Business Impact Analyse (BIA)
- Notfallpläne
- BAO-Management
- BCM-Risiko Methodik
- Business Impact Analyse
- Planung von RTO/ RPO
- Notfallreaktion (Emergency Response)
- Tests und Audits im BCM

ISO 27001 & ISMS Frameworks
- Lebenszyklus eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001
- BSI-Standards und Sicherheitskontrollen
- Statement of Applicability (SoA) & Dokumentation
- Optionen zur Risikobehandlung
- ISMS-Governance-Modell

Zertifizierung zum Informations-sicherheitsbeauftragten
- ISMS-Struktur nach ISO 27001
- Erstellung von ISMS-Richtlinien
- Sicherheits-Governance
- Risikomanagement im ISMS
- Rechtliche Compliance und Governance, Risk & Compliance (GRC)

Soft Skills

Hier klicken für finale Projekte

Kreativität
Fachwissen
Kommunikationsfähigkeiten
Problemlösung
Zusammenarbeit
Zeitmanagement
Flexibility
Ethische Überlegungen

Zertifikat ISC2 CC

Zertifikat Information Security Officer (ISB)

Praxisprojekt
Umsetzung des erworbenen Wissens in einem realen Szenario.

Unterstützte Jobsuche
Zusätzlich unterstützen wir aktiv bei der Jobsuche. Schon während des Lehrgangs können Teilnehmer:innen in regelmäßig stattfindenden Netzwerkveranstaltungen wertvolle Kontakte zu erfahrenen Fachkräften der Tech-Szene knüpfen.

neue fische | SPICED