Curriculum
Cyber, Cloud & Information Security

10+Years of Building Careers

Full-time: 20 weeks / 5 months

English **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)**

Annual salary: 57.000 - 89.000 €

The curriculum shown here is an exemplary guide to course content. We reserve the right to slightly adjust content and schedule for didactic and organizational reasons, or to reflect current labor-market requirements. Any adjustments will not affect the quality or the learning outcomes of the course.

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 Development

Attention to Detail **Communication** **Ownership** **Storytelling** **Resilience** **Stakeholder Management** **research skills** **Curiosity** **Time Management** **Problem Solving** **Teamwork** **creativity** **Adaptability** **Analytical Thinking**

Certificate ISC2 CC

Certificate Information Security Officer (TÜV)

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

Supported Job Search
Our career team of 4 coaches actively run the Career Compass program that train and support job searches, and we organize regularly masterclasses and events with industry experts.

neue fische | SPICED

Cyber, Cloud and Information Security Training
Why now is the ideal time for further training

1 Why Cyber Security is an important competency in Germany?

According to LinkedIn Skills im Trend 2026 (Deutschland), AI Competence is Germany's fastest-growing skill area.

At the same time LinkedIn Jobs im Trend 2026 also ranks IT Specialist as the #6 fastest-growing profession in Germany.

As businesses increasingly rely on cloud services, digital infrastructure, and AI, cybersecurity has become a core competency across virtually every industry.

2 Why companies are looking for Cyber Security Specialists?

According to Bitkom, 80% of German companies report an increase in cyberattacks, while cybercrime continues to cause significant economic damage.

Companies need Cyber Security Specialists who can identify vulnerabilities, protect IT systems, and respond to evolving security threats.

Growing cloud adoption, stricter cybersecurity regulations such as NIS2, and wider AI adoption are further driving demand for skilled cybersecurity professionals.

3 Cyber Security Job postings in Germany

Cybersecurity professionals remain in high demand across Germany. As of August 2026, Glassdoor lists more than 1,300 open Information Security positions, with opportunities spanning across industries.

As of August 2026, there are more than 5,000 open positions for Cyber Security-related roles in StepStone.

Roles on StepStone	Job Postings *(August 2026)*
Cyber Security Engineer	3,631
Information Security Manager	452
Cyber Security Analyst	235
IT Security Specialist	726

LinkedIn News

SKILLS 2026 IM TREND Deutschland

#1 AI Competence

Key Skills: Generative AI, LLMs, prompt engineering, chatbot development, transformers, CNNs, and RAG techniques (connecting LLMs to external data).

Relevance: Knowledge of AI application is required in almost all professions today, even outside the tech industry.

💡 Boost your productivity with AI agents.

#6 IT Specialists

Responsibilities: Manage and secure enterprise IT infrastructure, maintain IT systems, implement cybersecurity measures, and support IT audits.

Top Skills: ISO 27001, Information Security Management, Vulnerability Management

Top Industries: IT Services & Consulting, Financial Services, Insurance

Sources & References

LinkedIn Skills im Trend 2026
LinkedIn Jobs im Trend 2026
Bitkom Research - Increase in Cyberattacks on Germany

neue fische | SPICED

Curriculum
Cyber, Cloud & Information Security

10+Years of Building Careers

Vollzeit: 20 Wochen / 5 Monate

Englisch **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)**

Jahresgehalt: 57.000 - 89.000 €

Der hier dargestellte Lehrplan dient als beispielhafter Leitfaden für die Kursinhalte. Wir behalten uns das Recht vor, die Inhalte und den Zeitplan aus didaktischen oder organisatorischen Gründen sowie zur Anpassung an aktuelle Anforderungen des Arbeitsmarktes geringfügig zu ändern. Etwaige Anpassungen haben keine Auswirkungen auf die Qualität oder die Lernergebnisse des Kurses.

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)

Entwicklung von Soft Skills

Detailgenauigkeit **Resilienz** **Stakeholder-Management** **Kommunikation** **Storytelling** **Recherchefähigkeiten** **Problemlösung** **Teamwork** **Eigenverantwortung** **Kreativität** **Anpassungsfähigkeit** **Analytisches Denken** **Zeitmanagement** **Neugier**

Praxisprojekt
Umsetzung des erworbenen Wissens in einem realen Szenario.

Unterstützte Jobsuche
Unser vierköpfiges Karriere-Team leitet aktiv das „Career-Compass"-Programm, das bei der Jobsuche schult und unterstützt; zudem organisieren wir regelmäßig Masterclasses und Veranstaltungen mit Branchenexperten.

neue fische | SPICED

Cyber-, Cloud- und Informationssicherheits-Training
Warum jetzt der ideale Zeitpunkt für Weiterbildung ist

1 Warum Cybersicherheit eine wichtige Kompetenz in Deutschland ist

Laut LinkedIn Skills im Trend 2026 (Deutschland) ist KI-Kompetenz der am schnellsten wachsende Kompetenzbereich Deutschlands.

Gleichzeitig führt LinkedIn Jobs im Trend 2026 IT Specialist als #6 der am schnellsten wachsenden Berufe in Deutschland.

Da Unternehmen zunehmend auf Cloud-Dienste, digitale Infrastruktur und KI setzen, ist Cybersicherheit in nahezu jeder Branche zur Kernkompetenz geworden.

2 Warum suchen Unternehmen nach Cybersicherheits-Spezialist:innen?

Laut Bitkom melden 80 % der deutschen Unternehmen einen Anstieg von Cyberangriffen, während Cyberkriminalität weiterhin erheblichen wirtschaftlichen Schaden verursacht.

Unternehmen benötigen Cybersicherheits-Spezialist:innen, die Schwachstellen erkennen, IT-Systeme schützen und auf neue Bedrohungen reagieren können.

Wachsende Cloud-Nutzung, strengere Cybersicherheitsvorschriften wie NIS2 und die zunehmende KI-Nutzung treiben die Nachfrage nach qualifizierten Cybersicherheits-Fachkräften weiter voran.

3 Cybersicherheits-Stellenausschreibungen in Deutschland

Cybersicherheits-Fachkräfte bleiben in ganz Deutschland stark gefragt. Mit Stand August 2026 listet Glassdoor mehr als 1.300 offene Stellen im Bereich Informationssicherheit, mit Chancen branchenübergreifend.

Mit Stand August 2026 gibt es bei StepStone mehr als 5.000 offene Stellen im Bereich Cybersicherheit.

Jobs auf StepStone	Stellenausschreibungen (August 2026)
Cyber Security Engineer	3,631
Information Security Manager	452
Cyber Security Analyst	235
IT Security Specialist	726

LinkedIn News

SKILLS 2026 IM TREND Deutschland

#1 KI-Kompetenz

Schlüsselkompetenzen: Generative KI, LLMs, Prompt Engineering, Chatbot-Entwicklung, Transformer, CNNs und RAG-Techniken (Verknüpfung von LLMs mit externen Daten).

Relevanz: Wissen über KI-Anwendung wird heute in fast allen Berufen benötigt, auch außerhalb der Tech-Branche.

💡 Steigere deine Produktivität mit KI-Agenten.

#6 IT Specialists

Verantwortlichkeiten: Verwaltung und Absicherung von Unternehmens IT-Infrastruktur, Pflege von IT-Systemen, Umsetzung von Cyber Sicherheitsmaßnahmen, Unterstützung bei IT-Audits. Top-Kompetenzen: ISO 27001, Informationssicherheitsmanagement, Schwachstellenmanagement
Top-Branchen: IT-Dienstleistungen & Beratung, Finanzdienstleistungen, Versicherungen

Sources & References

LinkedIn Skills im Trend 2026
LinkedIn Jobs im Trend 2026
Bitkom Research - Increase in Cyberattacks on Germany

neue fische | SPICED