cmt GmbH

200-x
BSI-STANDARDS
IM FOKUS

BSI IT-Grundschutz meistern.

Framework, Zertifizierung und Praxis - dein Weg zur Informationssicherheit mit den BSI-Standards 200-1 bis 200-4

ISMS · BSI 200-1 BIS 200-4 · ISO 27001 · NIS2 · GRUNDSCHUTZ++ · BCM · RISIKOANALYSE

Stand: Mai 2026

cmt GmbH · cmt.de

Warum Informationssicherheit?

Bedrohungslage, Regulatorik und wirtschaftliche Konsequenzen

Cyberangriffe treffen nicht nur Konzerne. 87 Prozent aller deutschen Unternehmen waren 2025 von einem Angriff betroffen. Der wirtschaftliche Gesamtschaden durch Datendiebstahl, Sabotage und Spionage liegt bei 289 Milliarden Euro pro Jahr - davon rund 202 Milliarden Euro direkt durch Cyberangriffe (Bitkom Wirtschaftsschutz 2025).

Drei Treiber für systematische Informationssicherheit

01

Bedrohungslage auf Rekordniveau

Das BSI registriert durchschnittlich 119 neue Schwachstellen pro Tag. 34 Prozent der Unternehmen waren 2025 von Ransomware betroffen - fast dreimal so viele wie 2022. Angriffe werden gezielter, professioneller und sind zunehmend staatlich gelenkt.

02

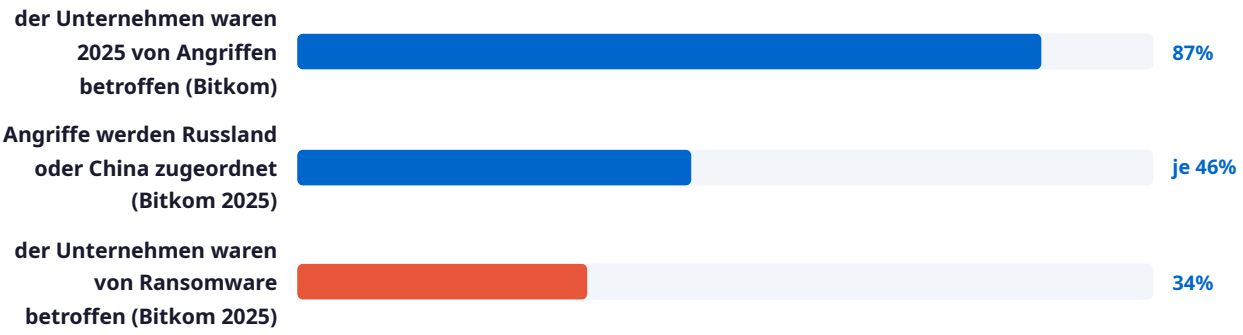
Regulatorische Pflichten verschärfen sich

Seit Dezember 2025 ist das NIS-2-Umsetzungsgesetz in Kraft. Statt bisher rund 4.500 fallen nun rund 30.000 Organisationen unter die BSI-Aufsicht. Geschäftsleitungen haften persönlich für die Umsetzung von Cybersicherheitsmaßnahmen und müssen an Schulungen teilnehmen.

03

Wirtschaftlicher Schaden vs. Investition

Der durchschnittliche Schaden eines erfolgreichen Ransomware-Angriffs übersteigt die Kosten eines ISMS um ein Vielfaches. Ein strukturiertes Sicherheitsmanagement nach BSI IT-Grundschutz schützt nicht nur vor Angriffen, sondern schafft auch Vertrauen bei Kunden und Partnern.



BSI IT-Grundschutz: der bewährte Rahmen für Deutschland

Der IT-Grundschutz des BSI bietet als einziges Framework sowohl eine anerkannte Methodik als auch ein konkretes Maßnahmenkompendium. Eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz gilt als Goldstandard der Informationssicherheit in Deutschland.

BSI IT-Grundschutz: Das Framework

Aufbau, Standards und Kompendium im Überblick

Der IT-Grundschutz des BSI ist ein ganzheitliches Framework für Informationssicherheit. Er besteht aus den BSI-Standards 200-1 bis 200-4, dem IT-Grundschutz-Kompendium und einer strukturierten Vorgehensweise zur Einführung eines ISMS.

Drei Säulen des IT-Grundschutzes

01 BSI-Standards 200-x

Vier Standards bilden das methodische Fundament: ISMS-Anforderungen (200-1), Vorgehensweise (200-2), Risikoanalyse (200-3) und Business Continuity Management (200-4).

02 IT-Grundschutz-Kompendium

111 Bausteine in 10 Schichten - von Anwendungen (APP) über Industrielle IT (IND) bis Sicherheitsmanagement (ISMS). Jeder Baustein enthält konkrete Anforderungen und Umsetzungshinweise.

03 Zertifizierung

ISO 27001 auf Basis von IT-Grundschutz - die höchste Stufe der Anerkennung. BSI-zertifizierte Auditoren prüfen Konformität und Wirksamkeit. Das Zertifikat gilt drei Jahre mit jährlichen Überwachungsaudits.

++ Grundschutz++ ab 2026

Seit Januar 2026 gibt es IT-Grundschutz++ - maschinenlesbar im OSCAL/JSON-Format, mit Praktiken statt Bausteinen und rund 85% weniger Redundanz. Parallelphase bis ca. 2029.

Die 10 Schichten des Kompendiums

Kürzel	Schicht	Beispiele
ISMS	Sicherheitsmanagement	Sicherheitsmanagement, Organisation
ORP	Organisation und Personal	Schulung, Personal, Identitätsmanagement
CON	Konzeption und Vorgehensweise	Kryptokonzept, Datenschutz, Datensicherung
OPS	Betrieb	Patch-Management, Protokollierung
APP	Anwendungen	E-Mail, Webbrowser, Datenbanken, SAP
SYS	IT-Systeme	Server, Clients, Mobile Devices
NET	Netze und Kommunikation	Firewall, WLAN, VPN
INF	Infrastruktur	Rechenzentrum, Serverraum, Büro
IND	Industrielle IT	ICS, Sensoren, Maschinensteuerung
DER	Detektion und Reaktion	Vorfallbehandlung, Forensik, Audits

Der Weg zur Zertifizierung

ISO 27001 auf Basis von IT-Grundschutz - Schritt für Schritt

Eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz ist der anerkannte Nachweis für ein wirksames Informationssicherheits-Managementsystem. Der Prozess dauert erfahrungsgemäß etwa 18 Monate von der Schutzbedarfsfeststellung bis zum erfolgreichen Audit.

01 Informationsverbund festlegen

Definiere den Geltungsbereich (Scope) deines ISMS: Welche Geschäftsprozesse, IT-Systeme, Räumlichkeiten und Kommunikationsverbindungen gehören dazu? Ein klar abgegrenzter Informationsverbund ist die Grundlage für alle weiteren Schritte.

02 Schutzbedarfsfeststellung

Bewerte die Geschäftsprozesse und Informationen nach Vertraulichkeit, Integrität und Verfügbarkeit. Der Schutzbedarf (normal, hoch, sehr hoch) bestimmt, welche Maßnahmen umgesetzt werden müssen.

03 Modellierung und Baustein-Zuordnung

Ordne die passenden Bausteine aus dem IT-Grundschutz-Kompendium den Zielobjekten zu. Die Modellierung nach BSI-Standard 200-2 stellt sicher, dass kein relevanter Aspekt vergessen wird.

04 IT-Grundschutz-Check (Soll-Ist-Vergleich)

Prüfe den Umsetzungsstand aller zugeordneten Anforderungen. Dokumentiere Abweichungen und erstelle einen Maßnahmenplan für offene Punkte. Für erhöhten Schutzbedarf folgt eine ergänzende Risikoanalyse nach BSI-Standard 200-3.

05 Umsetzung und Dokumentation

Setze fehlende Maßnahmen um und dokumentiere Richtlinien, Prozesse und Nachweise. Die Dokumentation ist ein wesentlicher Bestandteil des Audits und muss aktuell, vollständig und nachvollziehbar sein.

06 Zertifizierungsaudit

Ein BSI-zertifizierter Auditor prüft in zwei Phasen: Phase 1 ist eine Dokumentenprüfung, Phase 2 die Umsetzungsprüfung vor Ort. Das Zertifikat gilt drei Jahre mit jährlichen Überwachungsaudits.

Einstieg: BSI IT-Grundschutz-Praktiker

Das Seminar BSI IT-Grundschutz-Praktiker vermittelt alle Grundlagen für die ersten Schritte auf dem Weg zur Zertifizierung. Ideal für künftige ISBs und Projektverantwortliche.

BSI-Standards im Detail

200-1 (ISMS), 200-2 (Methodik), 200-3 (Risiko), 200-4 (BCM)

Die vier BSI-Standards bilden das methodische Fundament des IT-Grundschutzes. Sie definieren, was ein ISMS leisten muss, wie du es aufbaust, wie Risiken analysiert werden und wie Geschäftskontinuität sichergestellt wird.

1

BSI-Standard 200-1: Managementsysteme für Informationssicherheit

Anforderungen an ein ISMS - kompatibel mit ISO/IEC 27001

Definiert allgemeine Anforderungen an Aufbau, Betrieb und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems. Beschreibt Rollen, Verantwortlichkeiten, Leitlinie und den PDCA-Zyklus.

Kernfrage: Was muss ein ISMS leisten und welche Strukturen braucht es?

2

BSI-Standard 200-2: IT-Grundschutz-Methodik

Die bewährte Vorgehensweise für solide Informationssicherheit

Beschreibt drei Vorgehensweisen: Basis-Absicherung (Einstieg), Standard-Absicherung (für den normalen Betrieb) und Kern-Absicherung (für besonders schutzwürdige Bereiche). Deckt Strukturanalyse, Schutzbedarfsfeststellung, Modellierung und Grundschutz-Check ab.

Kernfrage: Wie setze ich den IT-Grundschutz Schritt für Schritt um?

3

BSI-Standard 200-3: Risikoanalyse auf Basis von IT-Grundschutz

Systematische Bewertung von Risiken für erhöhten Schutzbedarf

Bündelt alle risikobezogenen Arbeitsschritte: Gefährdungsidentifikation, Risikobewertung und Risikobehandlung. Greift dort, wo die Standard-Absicherung nicht ausreicht - also bei hohem und sehr hohem Schutzbedarf.

Kernfrage: Wo reicht der Standard-Grundschutz nicht aus und wie gehe ich mit Restrisiken um?

4

BSI-Standard 200-4: Business Continuity Management

Geschäftskontinuität und Notfallmanagement strukturiert aufbauen

Der modernisierte Standard 200-4 bietet praktische Anleitungen für Aufbau und Betrieb eines Business Continuity Management Systems (BCMS). Er ergänzt die Informationssicherheit um die Perspektive der Geschäftskontinuität und ist kompatibel mit ISO 22301.

Seminartipp: Business Continuity Management gemäß BSI-Standard 200-4 & ISO 27001

Praxisleitfaden: Grundschutz einführen

Von der Strukturanalyse bis zum Audit in fünf Phasen

Die Einführung des IT-Grundschutzes folgt einer bewährten Methodik. Dieser Leitfaden zeigt die fünf zentralen Phasen und gibt praktische Hinweise für die Umsetzung.

1

Phase 1: Strukturanalyse

Erfasse deinen Informationsverbund

Dokumentiere Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räumlichkeiten. Nutze Netzpläne und Inventarlisten als Grundlage. Definiere den Scope klar - lieber klein starten und später erweitern.

2

Phase 2: Schutzbedarfsfeststellung

Bewerte Vertraulichkeit, Integrität und Verfügbarkeit

Ordne jedem Zielobjekt eine Schutzbedarfskategorie zu: normal, hoch oder sehr hoch. Orientiere dich an möglichen Schäden bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit. Der Schutzbedarf wird vererbt - Server erben den höchsten Schutzbedarf ihrer Anwendungen.

3

Phase 3: Modellierung

Ordne passende Bausteine zu

Weise jedem Zielobjekt die relevanten Bausteine aus dem IT-Grundschutz-Kompendium zu. Die Modellierung nach BSI-Standard 200-2 stellt sicher, dass alle relevanten Anforderungen abgedeckt werden. Die Zuordnung folgt klaren Regeln - einige Bausteine sind obligatorisch für bestimmte Objekttypen.

4

Phase 4: IT-Grundschutz-Check und Umsetzung

Soll-Ist-Vergleich und Maßnahmenplanung

Prüfe den Umsetzungsstand jeder Anforderung: ja, teilweise oder nein. Erstelle einen priorisierten Maßnahmenplan. Für erhöhten Schutzbedarf führe eine ergänzende Risikoanalyse nach BSI-Standard 200-3 durch. Dokumentiere alles - die Dokumentation ist ein zentraler Audit-Bestandteil.

5

Phase 5: Audit und Zertifizierung

Externer Nachweis durch BSI-Auditor

Bereite die Referenzdokumente vor und beauftrage einen BSI-zertifizierten Auditor. Das Audit besteht aus Dokumentenprüfung (Phase 1) und Umsetzungsprüfung vor Ort (Phase 2). Nach bestandenem Audit erhältst du das ISO 27001-Zertifikat auf Basis von IT-Grundschutz - gültig für drei Jahre.

Praxis-Seminare für den Einstieg

Das BSI IT-Grundschutz Praxis Training begleitet dich durch alle Phasen mit konkreten Übungen. Ergänzend bietet das BSI IT-Sicherheitsberater-Seminar die vertiefte Beraterkompetenz.

BSI-Grundschutz und NIS2

Wie der IT-Grundschutz bei der NIS2-Compliance hilft

Seit dem 6. Dezember 2025 ist das NIS-2-Umsetzungsgesetz in Kraft. Rund 30.000 Organisationen fallen jetzt unter die BSI-Aufsicht. Der IT-Grundschutz bietet einen bewährten Rahmen, um die neuen Pflichten strukturiert zu erfüllen.

Was NIS2 fordert

01

Registrierung beim BSI

Betroffene Unternehmen müssen sich über das BSI-Portal registrieren (seit Januar 2026 freigeschaltet). Die Selbstprüfung der Betroffenheit liegt bei den Unternehmen selbst.

02

Meldepflicht bei Vorfällen

Erhebliche Sicherheitsvorfälle müssen dem BSI gemeldet werden - mit Erstmeldung innerhalb von 24 Stunden und vollständigem Bericht innerhalb von 72 Stunden.

03

Risikomanagement-Maßnahmen

Organisationen müssen angemessene technische und organisatorische Maßnahmen implementieren und dokumentieren. Für Bundeseinrichtungen ist IT-Grundschutz als Basis vorgeschrieben.

04

Geschäftsleitungs-Haftung

Cybersicherheit ist explizit Chefsache: Geschäftsleitungen haften persönlich und sind verpflichtet, an Schulungen zur Cybersicherheit teilzunehmen.

Wie BSI-Grundschutz bei NIS2 hilft

NIS2-Anforderung	BSI-Grundschutz-Abdeckung
Risikomanagement-Maßnahmen	BSI-Standard 200-2 und 200-3 bieten strukturierte Methodik
Business Continuity	BSI-Standard 200-4 deckt BCM vollständig ab
Vorfallbehandlung	Baustein DER.2.1 Behandlung von Sicherheitsvorfällen
Sicherheit der Lieferkette	Bausteine OPS.2.x für Dienstleister und Outsourcing
Nachweis der Compliance	ISO 27001-Zertifizierung auf Basis IT-Grundschutz als Nachweis
Schulungspflicht Geschäftsleitung	BSI-Praktiker und Awareness-Seminare als Nachweis

Weiterbildung: NIS2-Richtlinie für Unternehmen

Das Seminar NIS2-Richtlinie für Unternehmen erklärt die neuen Pflichten und zeigt konkret, wie du BSI-Grundschutz als Compliance-Nachweis nutzen kannst. KRITIS-Betreiber müssen ihren Nachweis innerhalb von drei Jahren erbringen.

Rollen und Qualifikationen

Vom Informationssicherheitsbeauftragten bis zum BSI-Auditor

Der BSI IT-Grundschutz definiert ein zweistufiges Qualifizierungssystem: IT-Grundschutz-Praktiker als Einstieg, IT-Grundschutz-Berater als Vertiefung mit BSI-Personenzertifikat. Die zentrale Rolle in jeder Organisation ist der Informationssicherheitsbeauftragte (ISB), der das ISMS verantwortet und die Umsetzung koordiniert.

P

BSI IT-Grundschutz-Praktiker

Einstiegsqualifikation - typische Rolle: (Junior-)ISB oder Projektmitarbeiter

Vermittelt Grundlagen des IT-Grundschutzes, die BSI-Standards 200-1 bis 200-3, das Kompendium und die praktische Vorgehensweise. Abschluss mit Prüfung beim Schulungsanbieter - die Voraussetzung für die weitergehende Berater-Zertifizierung.

Zielgruppe: Angehende IT-Sicherheitsbeauftragte, Projektmitarbeiter ISMS, IT-Verantwortliche

B

BSI IT-Grundschutz-Berater (IT-Sicherheitsberater)

BSI-Personenzertifikat - Beraterkompetenz für ISMS-Aufbau

Aufbauend auf dem Praktiker-Zertifikat. Befähigt zur Begleitung von Organisationen bei Einführung, Betrieb und Verbesserung des ISMS nach BSI-Vorgaben bis zur Zertifizierungsreife. Zertifizierung durch das BSI direkt.

Zielgruppe: Erfahrene ISBs, Berater, Projektleiter für ISMS-Einführungen

A

BSI IT-Auditor

Berechtigung zur Durchführung von ISO 27001-Audits auf Basis IT-Grundschutz

BSI-Auditoren prüfen die Konformität und Wirksamkeit des ISMS. Sie führen Zertifizierungsaudits und jährliche Überwachungsaudits durch. Die Zulassung erfolgt durch das BSI und setzt umfangreiche Praxiserfahrung voraus.

Zielgruppe: Erfahrene Berater, Auditoren, Prüfungsleiter

S

ISO 27001 Security Officer

Komplementäre Qualifikation - internationaler Standard

Vertieft die ISO 27001 unabhängig von der BSI-Methodik. Ideal als Ergänzung für internationale Kontexte oder Organisationen, die ISO 27001 ohne BSI-Grundschutz-Basis anstreben.

Alternativ: ISO 27001 Kompakt (Foundation & Security Officer) als beschleunigte Variante

Qualifizierungspfad auf einen Blick

Schritt 1: BSI IT-Grundschutz-Praktiker (Einstieg, Prüfung beim Anbieter) → **Schritt 2:** BSI IT-Grundschutz-Berater (Aufbau, BSI-Zertifikat) → **Schritt 3:** BSI IT-Auditor (Spezialisierung, BSI-Zulassung)

Grundschutz++ und Ausblick 2026

Die größte Reform des IT-Grundschutzes seit 30 Jahren

Mit IT-Grundschutz++ hat das BSI zum 1. Januar 2026 die grundlegendste Modernisierung des Frameworks gestartet. Weg vom statischen PDF, hin zu einem agilen, maschinenlesbaren und deutlich schlankeren System. Die bisherige Edition bleibt bis etwa 2029 parallel gültig.

Was ändert sich mit Grundschutz++?

✕ 111 Bausteine als PDF	→	✓ Thematische Praktiken in JSON
✕ Statische Zuordnung	→	✓ Kontextbezogene Ableitung
✕ Manuelle Dokumentation	→	✓ OSCAL-basierte Automatisierung
✕ Hohe Redundanz	→	✓ Rund 85% weniger Anforderungen

Zeitplan für die Migration

2026
Grundschutz++ veröffentlicht, Parallelphase beginnt

2027
Vorbereitung starten, Tooling evaluieren

2029
Migration abschließen, alte Edition endet

Was bedeutet das für dich?

- Bestehende Zertifizierungen bleiben während der Parallelphase gültig
- Neueinsteiger können direkt mit Grundschutz++ starten
- ISMS-Tools müssen OSCAL/JSON unterstützen - prüfe die Kompatibilität
- Rechne damit, dass 30-40% der Migration manuellen Aufwand erfordern
- Die BSI-Qualifizierungen (Praktiker, Berater, Auditor) werden angepasst

Grundschutz-Wissen bleibt relevant

Die Grundprinzipien des IT-Grundschutzes ändern sich nicht. Wer heute die BSI-Standards versteht, ist auch für Grundschutz++ gut vorbereitet. Die Seminare bei cmt werden laufend an die Neuerungen angepasst.

Seminarübersicht

BSI, ISO 27001 und Informationssicherheit bei cmt

Über 30 Seminare rund um BSI IT-Grundschutz, ISO 27001, NIS2, Cybersecurity und Incident Response. Alle Seminare als offener Kurs, Inhouse oder Online-Live buchbar.

BSI IT-Grundschutz und ISMS

Seminar	Schwerpunkt
BSI IT-Grundschutz-Praktiker	BSI-Standards, Kompendium, Einstieg
BSI IT-Sicherheitsberater	ISMS-Aufbau, BSI-Personenzertifikat
BSI IT-Auditor Training	Audit-Methodik, Zertifizierung
BSI IT-Grundschutz Praxis Training	Hands-on Umsetzung
BSI Grundschutz für die Rüstungsindustrie	Branchenspezifische Anforderungen
Business Continuity Management (BSI 200-4 & ISO 27001)	BCM-Aufbau, Notfallmanagement
ISO 27001 Security Officer	Internationaler ISMS-Standard
ISO 27001 Kompakt (Foundation & Security Officer)	Beschleunigte ISO 27001-Qualifikation

Regulatorik und Compliance

Seminar	Schwerpunkt
NIS2-Richtlinie für Unternehmen	NIS2-Pflichten, Umsetzung
Risikomanagement für KI: sicher und konform	KI-Risiken, EU AI Act
KI Compliance: Rechtssicherer Einsatz	KI-Regulierung, Compliance

Awareness und Grundlagen

Seminar	Schwerpunkt
IT-Security Awareness - Mitarbeitersensibilisierung	Phishing, Social Engineering
A4Q Security Essentials	Security-Grundlagen, Zertifizierung
Internet Security - Datenschutz und Sicherheit	Datenschutz, sichere Nutzung

Seminarübersicht (Fortsetzung)

Cybersecurity, Incident Response und Cloud-Sicherheit

Cybersecurity und Hacking

Seminar	Schwerpunkt
IT-Sicherheit: (Anti-) Hacking für Admins	Angriffstechniken, Abwehr
Cybersecurity-Training für Techniker und Administratoren	Praxis-Cybersecurity
Linux Security Intensivkurs	Linux-Härtung, Monitoring
KI-Sicherheit in der Cloud Grundkurs	Cloud-Security, KI-Workloads

Incident Response und Forensik

Seminar	Schwerpunkt
Certified Incident Handler (ECIH v3)	Vorfallbehandlung, EC-Council
Digitale Forensik (Grundkurs)	Beweissicherung, Analyse
Digitale Forensik (Linux/Unix)	Linux-Forensik
Digitale Forensik (Windows)	Windows-Forensik

Microsoft Security

Seminar	Schwerpunkt
SC-200: Microsoft Security Operations Analyst	Microsoft Sentinel, Defender
SC-100: Microsoft Cybersecurity Architect	Security-Architektur, Zero Trust
SC-900: Security, Compliance and Identity Fundamentals	Microsoft Security Grundlagen
AZ-500: Microsoft Azure Security Technologies	Azure-Sicherheit

Alle Seminare auch als Inhouse-Training

Jedes Seminar ist als offener Kurs, Inhouse-Training oder Online-Live buchbar. Inhouse-Trainings werden an die spezifischen Anforderungen deiner Organisation angepasst - inklusive branchenspezifischer Fallbeispiele und interner Richtlinien.

Dein Qualifizierungsplan

Drei Lernpfade für unterschiedliche Ausgangssituationen

Ob Einstieg, Vertiefung oder Spezialisierung - drei Lernpfade zeigen den Weg, abgestimmt auf deinen tatsächlichen Bedarf.

A

Lernpfad ISMS-Einstieg: Grundschutz verstehen und anwenden

Für Neueinsteiger, künftige ISBs und Projektmitarbeiter

BSI IT-Grundschutz-Praktiker → BSI IT-Grundschutz Praxis Training → IT-Security Awareness

Ergebnis: Du verstehst den IT-Grundschutz, kannst Strukturanalysen durchführen und die Mitarbeitersensibilisierung begleiten.

B

Lernpfad Zertifizierung: Vom Praktiker zum Berater

Für ISBs und Berater, die Organisationen zur Zertifizierung führen

BSI IT-Grundschutz-Praktiker → BSI IT-Sicherheitsberater → BCM nach BSI 200-4

Ergebnis: Du bist BSI-zertifizierter Berater und kannst Organisationen durch den gesamten Zertifizierungsprozess begleiten - inklusive BCM.

C

Lernpfad Defensive Security: Technische Härtung und Incident Response

Für Administratoren und technische Sicherheitsverantwortliche

Cybersecurity für Techniker → (Anti-) Hacking für Admins → Certified Incident Handler (ECIH)

Ergebnis: Du erkennst Angriffstechniken, härtest Systeme gezielt und reagierst strukturiert auf Sicherheitsvorfälle.

Individuelle Zusammenstellung möglich

Alle Seminare sind einzeln buchbar oder als maßgeschneidertes Inhouse-Programm kombinierbar. Wir beraten dich bei der Zusammenstellung für deine Organisation.

Warum cmt?

Dein Partner für Informationssicherheit und IT-Schulung

2.100+
Seminarthemen
Von BSI IT-Grundschutz über ISO 27001 bis Microsoft Security - eines der umfassendsten IT-Schulungsprogramme in Deutschland.

25+
Jahre Erfahrung
Seit über 25 Jahren bilden wir IT-Fachkräfte und Führungskräfte weiter - mit praxiserprobten Konzepten und aktuellen Inhalten.

100%
Garantie-Termine
Alle offenen Seminartermine finden garantiert statt. Keine Absagen wegen zu geringer Teilnehmerzahl.

30+
BSI- und Security-Seminare
BSI-Grundschutz, ISO 27001, NIS2, Cybersecurity, Forensik, Incident Response - alles aus einer Hand.

Drei Formate - ein Qualitätsstandard

Offene Seminare
Kleine Gruppen (4-8 Teilnehmer), feste Termine, Garantie-Durchführung. Ideal für einzelne Mitarbeiter.

Inhouse-Training
Bis 12 Teilnehmer, auf deine Organisation zugeschnitten. Branchenspezifische Fallbeispiele und interne Richtlinien inklusive.

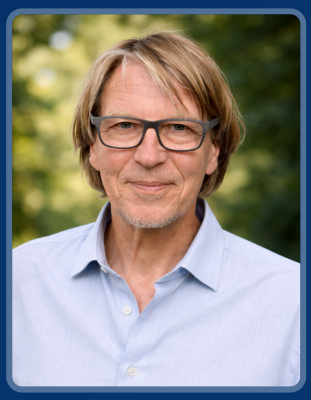
Online-Live
Interaktiv, ortsunabhängig, gleiche Qualität wie vor Ort. Ideal für verteilte Teams und kurzfristigen Bedarf.

Beratung und Planung

Du brauchst ein Schulungskonzept für dein ISMS-Projekt? Norbert Jansen, Leiter Management-Trainings & Consulting, berät dich persönlich bei der Zusammenstellung. Kontakt: jansen@cmt.de oder 0800 71 20 000.

cmt GmbH

Informationssicherheit planen? Sprich uns an.



Norbert Jansen

Leiter Management-Trainings & Consulting

0800 71 20 000 · jansen@cmt.de

cmt GmbH · Telefon: 0800 71 20 000 · info@cmt.de

www.cmt.de