CISM

Prüfung bestehen

Governance verstehen

ISACA-Logik meistern

Testcenter

800 Prüfungsfragen

Holger Reibold

Brain-Media.de

Holger Reibold

CISM

Prüfung bestehen.
Governance verstehen.
ISACA-Logik meistern.

BRAIN-MEDIA.DE

ISBN: 978-3-95444-369-7

Cover: Freepik / wirestock

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Anhang B – CISM Quick Reference Guide

Um Sie optimal auf den finalen Endspurt vorzubereiten, fasst dieser kompakte Leitfaden die essenziellen Kernkonzepte des Lehrbuchs übersichtlich zusammen. Er dient als Ihr mentaler Kompass für die Prüfung, damit Sie komplexe Szenariofragen jederzeit treffsicher aus der geforderten Management- und Governance-Perspektive beantworten können.

Governance-Prinzipien

Die vier CISM-Domänen

Domäne	Kernfrage	Prüfungsanteil	Kapitel
D1: Information Security Governance	Wer entscheidet was, mit welchem Mandat?	~17 %	2–6
D2: Information Risk Management	Welche Risiken haben wir, wie priorisieren wir?	~20 %	7–10
D3: Information Security Program	Wie bauen und steuern wir das Programm?	~33 %	11–14
D4: Incident Management	Was tun wir, wenn es schiefgeht?	~30 %	15–17

Governance vs. Management vs. Compliance

Konzept	Fragestellung	Entscheidungsträger
Governance	Wohin wollen wir? Was ist unser Risikoappetit?	Board, Senior Management
Management	Wie setzen wir das um? Wann und womit?	CISO, IT-Management
Compliance	Erfüllen wir externe Mindestanforderungen?	Compliance-Funktion, Auditor

Rollen und Accountability

Rolle	Accountability / Responsibility	Typische Person
Board / Aufsichtsrat	Accountable für strategische Risikoentscheidungen und Governance.	Vorstand, Aufsichtsrat
CISO	Responsible für das Security-Programm. Accountable gegenüber Senior Management.	Chief Information Security Officer
Risk Owner	Accountable für ein spezifisches Risiko im eigenen Verantwortungsbereich.	Geschäftsbereichsleiter, Prozessverantwortlicher
Data Owner	Accountable für Klassifizierung und Schutz von Daten.	Fachabteilungsleiter

Rolle	Accountability / Responsibility	Typische Person
Data Custodian	Responsible für technische Datenspeicherung und -pflege.	IT-Abteilung, DBA
Internal Audit	Unabhängige Bewertung der Governance-Wirksamkeit (3. Linie).	Interne Revision

Drei-Linien-Modell

Linie	Funktion	Security-Kontext
1. Linie: Operatives Management	Tägliches Risikomanagement. Kontrollen implementieren.	Risk Owner, Data Owner, Geschäftsbereiche
2. Linie: Risk & Compliance	Rahmen vorgeben, überwachen, koordinieren.	CISO, Risikomanagement, Compliance
3. Linie: Interne Revision	Unabhängige Prüfung der Linien 1 und 2.	Internal Audit → berichtet direkt an Board

Policy-Hierarchie

Ebene	Inhalt
Policy (Richtlinie)	Was wollen wir erreichen? Prinzipien und Verbote. Board-Mandat. Selten geändert.
Standard	Welche messbaren Mindestanforderungen gelten? Technisch konkret. Jährliche Review.

Ebene	Inhalt
Procedure (Verfahren)	Wie genau wird es gemacht? Schritt-für-Schritt. Operativ. Bei Systemänderungen aktualisieren.
Guideline (Leitlinie)	Was empfehlen wir? Nicht verbindlich. Kein formaler Genehmigungsprozess.

Risk-Response-Modelle

Risiko-Grundformel: Risiko = Wahrscheinlichkeit (Threat nutzt Vulnerability aus) × Impact

Risikokonzepte im Überblick

Begriff	Definition	Prüfungs-Merkhilfe
Inherent Risk	Risiko vor allen Controls.	Ausgangsniveau. Immer höher als Residual Risk.
Residual Risk	Risiko nach Controls. Ziel: unterhalb Risk Appetite.	Was nach Schutzmaßnahmen verbleibt.
Risk Capacity	Absolutes Maximum. Existenzielle Grenze.	Wird durch Realität bestimmt, nicht durch Entscheidung.
Risk Appetite	Strategische Bereitschaft. Board-Entscheidung.	Klar unter Risk Capacity. In Policy verankert.

Begriff	Definition	Prüfungs-Merkhilfe
Risk Tolerance	Operatives Abweichungsband um Appetite.	Management-Entscheidung. Eskalationsschwelle.
ALE	Annual Loss Expectancy = SLE × ARO	Business Case: ALE > Kontrollkosten → investieren.

Vier Risikobehandlungsoptionen

Option	Was es bedeutet	Wann richtig?	Prüfungsfalle
Avoidance	Risikobringende Aktivität einstellen.	Residual Risk unakzeptierbar, Aktivität nicht geschäftskritisch.	Selten erste Wahl. Bedeutet Verzicht auf Geschäftsmöglichkeiten.
Mitigation	Controls implementieren.	Control-Kosten < Risikoreduktion (positiver Business Case).	Mitigation um jeden Preis ist kein Risikomanagement.
Transfer	Finanzielles Risiko auf Dritte (Versicherung, Vertrag).	Residual Risk nach Mitigation finanziell absichern.	Überträgt Geld-Risiko, nicht operatives Risiko.
Acceptance	Bewusste, dokumentierte Akzeptanz.	Residual Risk innerhalb Risk Appetite. Mitigation unverhältnismäßig.	Ohne Dokumentation und Risk-Owner-Unterschrift ist es Ignorieren.

Qualitative vs. quantitative Risikobewertung

Qualitativ	Quantitativ
Skala: hoch / mittel / niedrig.	Geldwerte: ALE = SLE × ARO.
Schnell, wenig Datenbedarf.	Präzise, Business-Case-fähig, datenbedürftig.
Gut für breite Risikolandschaft.	Gut für spezifische Control-Investitionsentscheidungen.
Subjektiv, schwer vergleichbar.	Objektiv, aber aufwändig und scheingenau.

Risikoregister – Pflichtfelder

Feld	Inhalt
Risikoidentifikation	Nummer, Bezeichnung, betroffenes Asset, Geschäftsprozess
Threat & Vulnerability	Konkrete Bedrohung und Schwachstelle, die das Risiko erzeugen
Inherent Risk	Wahrscheinlichkeit × Impact vor Controls (qualitativ oder quantitativ)
Controls	Bestehende Controls, Wirksamkeitsbewertung
Residual Risk	Verbleibendes Risiko nach Controls
Behandlung & Risk Owner	Gewählte Option (Avoid/Mitigate/Transfer/Accept), namentlicher Risk Owner

Feld	Inhalt
Review-Datum	Letzte Überprüfung und nächste geplante Review

Wichtigste Frameworks

Framework-Vergleich

Framework	Typ & Zweck	Zertifizierbar?	CISM-Schwerpunkt
COBIT 2019	IT-Governance-Framework. EDM (Governance) + operative Domänen (Management).	Nein	Governance-Struktur, Board-Verantwortung, EDM-Prozesse
ISO 27001:2022	ISMS-Standard. Plan-Do-Check-Act. 93 Kontrollen (Annex A).	Ja	ISMS-Aufbau, SoA, Zertifizierung, Compliance-Nachweis
ISO 27002:2022	Implementierungsleitfaden zu ISO 27001. Kein eigener Standard.	Nein	Control-Details, Umsetzungshinweise
NIST CSF 2.0	Risikoorientiertes Strukturierungsmodell. 6 Funktionen.	Nein	Kommunikation mit Board, Lagedarstellung, Detect/Respond
ISO 22301:2019	Business-Continuity-Managementsystem.	Ja	BCM-Framework, BCP-Anforderungen
ISO 42001:2023	KI-Managementsystem. Governance für KI-Systeme.	Ja	KI-Governance, AI-Act-Alignment

NIST CSF 2.0 – Sechs Kernfunktionen

Funktion	Typische Aktivitäten
Govern	Governance-Rahmen für Cybersecurity. Rollen, Policies, Risk Appetite. (Neu in v2.0)
Identify	Asset Management, Risikobewertung, Supply-Chain-Risikomanagement.
Protect	Zugangskontrolle, Awareness, Datensicherheit, Schutztechnologien.
Detect	Anomalieerkennung, Monitoring, Detection Processes.
Respond	Incident Response, Kommunikation, Mitigation, Verbesserung.
Recover	Recovery Planning, Verbesserung, Kommunikation nach Incident.

BCM-Schlüsselbegriffe

Begriff	Definition	Beziehung
MTD (Max Tolerable Downtime)	Absolute Obergrenze der Ausfallzeit.	MTD > RTO immer. Sonst Plan unzureichend.
RTO (Recovery Time Objective)	Ziel-Wiederherstellungszeit.	Muss kürzer sein als MTD.
RPO (Recovery Point Objective)	Max. tolerierbarer Datenverlust in Zeit.	Bestimmt Backup-Frequenz.

Recovery-Strategie	RTO-Bereich	Kosten
Hot Standby (aktiv-aktiv)	Sekunden bis Minuten	Hoch – parallele Infrastruktur
Warm Standby (aktiv-passiv)	1–24 Stunden	Mittel – Bereitschaft, nicht aktiv
Cold Standby (Backup-Restore)	24 Stunden bis Tage	Niedrig – nur Backups
Cloud-Recovery	Variabel, oft 1–4 Stunden	Flexibel – Third-Party-Risiko beachten

Governance-Entscheidungslogik

Die zehn ISACA-Faustregeln

Faustregel	Anwendung in der Prüfung
1. Strategie vor Taktik	Strategischere Antwort fast immer besser als die operative.
2. Bewertung vor Reaktion	Ohne Risikobewertung keine Maßnahme – auch wenn die Situation drängt.
3. Governance vor Technik	Policy / Prozess / Governance-Struktur kommt vor technischem Control.
4. Risk Owner entscheidet	Risikoakzeptanz liegt beim Business Owner, nicht beim CISO.
5. Senior Management Support	Wichtigster Erfolgsfaktor für Security-Programme. Immer.

Faustregel	Anwendung in der Prüfung
6. Klassifizieren vor Reagieren	Erster Schritt bei Incident: Klassifizieren und Eskalationsstufe aktivieren.
7. Kommunikation parallel	Krisenkommunikation beginnt gleichzeitig mit technischer Reaktion.
8. Gap-Analyse zuerst	Kein Programm / keine Initiative ohne Ist-Zustand-Analyse.
9. Executable Compliance	Controls müssen messbar, automatisierbar und krisenresistent sein.
10. CISO steuert, schraubt nicht	CISO berät, koordiniert, ermöglicht. Kein unilateraler Entscheider.

Häufige Distraktoren und ihre Disqualifizierung

Distraktor-Typ	Erkennungsmerkmal	Warum falsch
Techniker-Reflex	Operative Maßnahme als erste Antwort auf strategisches Problem.	CISO ist Manager, kein Operator. Erst Governance, dann Technik.
CISO als Alleinentscheider	CISO trifft Risikoentscheidung ohne Risk/Business Owner.	Accountability liegt beim Risk Owner, nicht beim CISO.
Compliance-Ersatz	Zertifikat / Audit als Lösung für aktives Sicherheitsrisiko.	Compliance ≠ Sicherheit. Risiko bleibt trotz Zertifikat.
Zu frühes Handeln	Maßnahme vor notwendiger vorheriger Phase.	IR-Lifecycle ist sequenziell. Erst Contain, dann Eradicate.

Distraktor-Typ	Erkennungsmerkmal	Warum falsch
Zu frühes Melden	NIS-2-Meldung vor Incident-Bestätigung.	Meldepflicht bei Kenntnis, nicht bei Verdacht.
Vollständigkeitsfalle	Auf vollständige Analyse warten bevor gehandelt wird.	Bei aktiver Exfiltration / laufendem Incident: sofort handeln.

Incident-Response-Lifecycle: Sequenz

Phase	Governance-Fokus des CISO
1. Preparation	IRP entwickeln, testen, pflegen. Rollen definieren. Melde-Templates bereitstellen.
2. Identification	Klassifizierung vornehmen – das ist die erste Aufgabe des CISO im Krisenfall.
3. Containment	Business-Owner-Entscheidung bei Systemabschaltung einbeziehen. Forensische Integrität wahren.
4. Eradication	Root Cause sicherstellen, bevor Systeme wiederhergestellt werden.
5. Recovery	Recovery-Kriterien vorab definiert. Wer erklärt Normalzustand?
6. Lessons Learned	PIR: Timeline, Root Cause, Detection, Response, Prävention, Regulatorik.

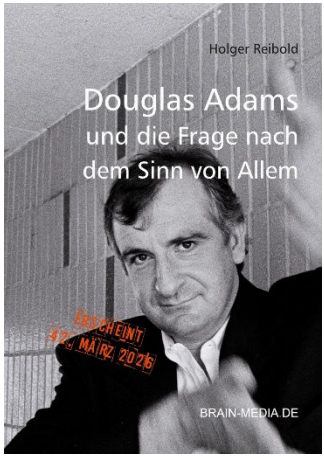
Meldepflichten-Schnellübersicht

Regulierung	Trigger	Frist (Erstmeldung)	Empfänger
NIS-2	Bedeutender Vorfall (wesentliche/wichtige Einrichtung)	24 Stunden (Frühwarnung)	Nationale Behörde (BSI in DE)
DSGVO	Datenpanne mit personenbezogenen Daten	72 Stunden	Datenschutzaufsichtsbehörde
DORA	Bedeutender IKT-Vorfall (Finanzunternehmen)	4 Stunden	BaFin, EZB, ESMA
PCI-DSS	Kompromittierung von Kartendaten	Sofort	Kartenorganisation, Acquirer

CISM Quick Review

Die folgenden Tabellen fassen die prüfungsrelevantesten Konzepte je Domäne zusammen. Sie sind als letzter Scan vor der Prüfung konzipiert – keine vollständige Zusammenfassung, sondern eine Checkliste der häufig abgefragten Unterscheidungen.

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026

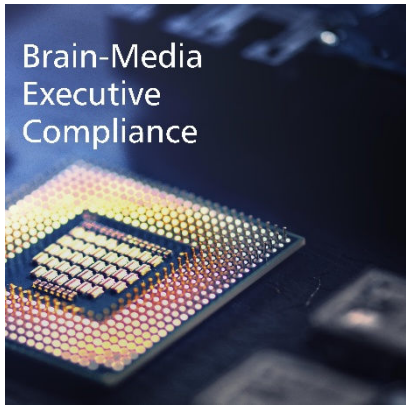
Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.

Executable Compliance

Compliance, die läuft.



Regulierung wird komplexer – klassische Ansätze stoßen an ihre Grenzen. Executable Compliance überführt Anforderungen in eine strukturierte, maschinenlesbare Compliance-Schicht, die direkt in Ihre Systeme integriert wird. Im Zentrum: das Brain-Media Audit Model (BAM):

Requirement → Gap-Check → Remediation → Risk → Control → Evidence

Das Ergebnis: ein durchgängiger, auditfähiger Datenstrom.

- Audit-Ready auf Knopfdruck
- Collect Once, Comply Many
- Nahtlose Integration in GRC & IT
- KI-Ready durch strukturierte Daten

Executable Compliance ist keine Software, sondern eine Infrastruktur. Für mehr Effizienz, Transparenz und Wettbewerbsvorteile.

Compliance als System. Nicht als Projekt.