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

Inhaltsverzeichnis

WIE SIE DIESES BUCH BENUTZEN.....1

Was diese Prüfung wirklich testet---------- 2

Warum dieses Buch anders aufgebaut ist---------- 3

Die vier Strukturelemente jedes Kapitels---------- 6

Zwei Lesedurchgänge – und warum beide nötig sind ---------- 9

Der erste Pass: Die Weitung des Horizonts ---------- 9

Der zweite Pass: Der Prüfungsdrill---------- 10

Die Psychologie der Prüfungsvorbereitung---------- 12

Der Expert Bias---------- 12

Das Vollständigkeitsparadoxon ---------- 12

Die Simulation als Vorbereitung---------- 13

Die Prüfungsdomänen als Rahmen des Buches ---------- 14

Ein Wort zu Format und Lesehaltung---------- 15

Wie dieses Buch entstand – und für wen es ist---------- 15

Exam Essentials und Executive Decisions ---------- 18

Bereit zum Start---------- 19

1 CISM-DOMÄNEN UND ISACA-LOGIK 21

1.1 Prüfungsdomänen als erstes Werkzeug ---------- 21

1.2 Die vier Domänen im Überblick ---------- 22

1.3 Die ISACA-Logik ---------- 24

1.4 Lesestrategien ---------- 28

1.4.1 Der erste Pass: Horizonterweiterung ---------- 28

1.4.2 Der Prüfungspass: Konditionierung ---------- 29

1.5 Die Strukturelemente dieses Buches ---------- 30

1.5.1 Lernziele ---------- 30

1.5.2 Governance Failure Patterns ---------- 31

1.5.3 Executive Decisions ---------- 32

1.6 Exam Essentials ---------- 32

1.7 Die Domänen im Detail: Ein erster Einblick ---------- 33

1.7.1 Domäne 1: Information Security Governance ---------- 33

1.7.2 Domäne 2: Information Risk Management ---------- 34

1.7.3 Domäne 3: Information Security Program ---------- 35

1.7.4 Domäne 4: Incident Management ---------- 35

1.8 Der Expert Bias ---------- 36

1.9 Die ISACA-Sprache ---------- 38

1.10 Executive Decision ---------- 39

1.11 Exam Essentials – Kapitel 1 ---------- 41

2 WAS GOVERNANCE BEDEUTET 45

2.1 Die ISACA-Definition ---------- 46

2.2 Governance vs. Management ---------- 47

2.3 Governance vs. Compliance ---------- 50

2.4 Die Policy-Hierarchie ---------- 51

2.4.1 Die Policy: Das Fundament ---------- 53

2.4.2 Standards: Messbare Mindestanforderungen ---------- 53

2.4.3 Procedures: Der operative Leitfaden ---------- 54

2.4.4 Guidelines: Empfehlungen ohne Verbindlichkeit --------- 55

2.5 Governance-Reife ---------- 56

2.6 Was Governance ermöglicht ---------- 57

2.6.1 Risikokonsistenz ---------- 58

2.6.2 Accountability-Klarheit ---------- 58

2.6.3 Ressourcenlegitimation ---------- 59

2.6.4 Krisenresilienz ---------- 59

2.7 Governance Failure Pattern ---------- 60

2.8 Was Governance ausdrücklich nicht ist ---------- 62

2.9 Executive Decision ---------- 63

2.10 Governance im regulatorischen Kontext ---------- 66

2.10.1 NIS-2: Governance als Managementaufgabe ---------- 66

2.10.2 DORA: Operative Resilienz ---------- 67

2.10.3 EU AI Act: Neue Governance-Anforderungen ---------- 67

2.11 Exam Essentials – Kapitel 2 ---------- 68

3 ROLLEN UND DAS DREI-LINIEN-MODELL 71

3.1 Accountability vs. Responsibility ---------- 72

3.2 Zentrale Rollen im Governance-System ---------- 74
3.2.1 Board of Directors / Aufsichtsrat ---------- 74
3.2.2 Chief Information Security Officer (CISO) ---------- 75
3.2.3 Risk Owner ---------- 76
3.2.4 Data Owner und Data Custodian ---------- 76
3.2.5 Steering Committee ---------- 77

3.3 Das Drei-Linien-Modell ---------- 78
3.3.1 Erste Linie: Operatives Management ---------- 78
3.3.2 Zweite Linie: Risikomanagement und Compliance ------- 79
3.3.3 Dritte Linie: Interne Revision ---------- 80

3.4 Die RACI-Matrix ---------- 82
3.4.1 Die vier RACI-Rollen ---------- 82
3.4.2 Häufige RACI-Fehler in der Prüfung ---------- 84

3.5 Governance Failure Pattern ---------- 85

3.6 Segregation of Duties ---------- 88

3.7 Senior Management Support ---------- 89

3.8 Executive Decision: Der überforderte CISO ---------- 90

3.9 Exam Essentials – Kapitel 3 ---------- 92

4 GOVERNANCE-FRAMEWORKS 95

4.1 Was ein Framework leistet – und was nicht ---------- 96

4.2 COBIT-Framework ---------- 97

4.2.1 Das COBIT-Kernmodell ---------- 98

4.2.2 COBIT-Prinzipien ---------- 99

4.2.3 COBIT in der Prüfung ---------- 99

4.3 ISO 27001 – das Managementsystem ---------- 100

4.3.1 Die ISMS-Logik: Plan-Do-Check-Act ---------- 100

4.3.2 Das Statement of Applicability (SoA) ---------- 103

4.3.3 ISO 27001 vs. ISO 27002 ---------- 104

4.4 NIST Cybersecurity Framework ---------- 104

4.4.1 Die fünf NIST-CSF-Kernfunktionen ---------- 104

4.4.2 NIST CSF in der Prüfung ---------- 105

4.5 Frameworks im Vergleich: Wann welches? ---------- 106

4.6 Governance Failure Pattern ---------- 109

4.7 Frameworks und regulatorische Anforderungen ---------- 110

4.7.2 NIS-2 und Frameworks ---------- 110

4.7.3 DORA und Frameworks ---------- 111

4.8 Executive Decision ---------- 111

4.9 Exam Essentials – Kapitel 4 ---------- 113

5 BUSINESS ALIGNMENT UND LEADERSHIP..... 115

5.1 Was Business Alignment bedeutet ----------116

5.2 Sicherheit als Business Enabler ----------118

5.3 Die Information Security Strategy ----------121

5.3.1 Der strategische Ableitungsprozess ----------121

5.3.2 Strategische Ziele vs. operative Ziele----------122

5.4 Der CISO als Kommunikationsbrücke----------123

5.4.1 Kommunikation mit dem Board ----------124

5.4.2 Kommunikation mit den Fachbereichen----------125

5.4.3 Kommunikation mit Regulatoren----------126

5.5 Governance Failure Pattern ----------128

5.6 Security-Metriken ----------129

5.6 Budgetierung und Business Case ----------131

5.7 Executive Decision ----------133

5.8 Exam Essentials – Kapitel 5----------135

6 SICHERHEITSKULTUR..... 137

6.1 Sicherheitskultur vs. -bewusstsein ----------138

6.2 Human Risk: unterschätzter Angriffsvektor ----------139

6.2.1 Phishing und Social Engineering----------141

6.2.2 Insider Threats: Die unterschätzte interne Gefahr-------142

6.3 Sicherheitskultur als Führungsaufgabe ---------- 144

6.4 Das Security-Awareness-Programm ---------- 147

6.4.1 Phasen eines wirksamen Awareness-Programms --------- 148

6.4.2 Zielgruppensegmentierung ---------- 149

6.4.3 Phishing-Simulationen: Richtig eingesetzt ---------- 150

6.5 Wirksamkeit messen ---------- 150

6.6 Governance Failure Pattern ---------- 152

6.7 Human Risk in der regulatorischen Welt ---------- 153

6.8 Sicherheitskultur messen ---------- 154

6.9 Executive Decision: Die Bestrafungsfrage ---------- 155

6.10 Exam Essentials – Kapitel 6 ---------- 157

7 RISK-BASED THINKING 161

7.1 Das Risiko-Vokabular ---------- 162

7.1.1 Die Risikoformel ---------- 164

7.1.2 Threat vs. Vulnerability ---------- 165

7.2 Inherent Risk und Residual Risk ---------- 167

7.3 Risk Appetite, Risk Tolerance und Risk Capacity ---------- 168

7.4 Qualitative vs. quantitative Risikobewertung ---------- 169

7.4.1 Qualitative Bewertung ---------- 170

7.4.2 Quantitative Bewertung ---------- 170

7.5 Die vier Risikobehandlungsoptionen ---------- 172

7.6 Der Risikomanagementprozess ---------- 176

7.7 Das Risikoregister ---------- 178

7.8 Governance Failure Pattern ---------- 179

7.9 Risikomanagement und Geschäftsprozesse ---------- 180

7.10 Executive Decision ---------- 181

7.11 Exam Essentials – Kapitel 7 ---------- 184

8 RISIKOBEWERTUNG 187

8.1 Asset-Management ---------- 188

8.1.1 Asset-Klassifizierung ---------- 189

8.1.2 Asset-Inventar als lebendes Dokument ---------- 190

8.2 Bedrohungslandschaft ---------- 193

8.2.1 Threat-Kategorien ---------- 193

8.2.2 Threat Intelligence ---------- 194

8.3 Vulnerability-Management ---------- 195

8.3.1 Der Vulnerability-Management-Zyklus ---------- 195

8.3.2 CVSS: Common Vulnerability Scoring System ---------- 196

8.3.3 Patch Management als Kernprozess ---------- 197

8.4 Die Risikobewertungs-Matrix ---------- 198

8.5 Third-Party-Risiken ---------- 199

8.5.1 Third-Party-Risk-Assessment ---- 200
8.5.2 Vertragsklauseln ---- 201

8.6 Governance Failure Pattern ---- 202

8.7 Executive Decision ---- 203

8.8 Exam Essentials – Kapitel 8 ---- 205

9 RISIKOBEHANDLUNG 207

9.1 Risikobehandlung als Entscheidungskette ---- 208

9.2 Risikoavoidance ---- 209

9.3 Risikominderung ---- 211
9.3.1 Control-Typen ---- 211
9.3.2 Kompensierende Kontrollen ---- 214

9.4 Risikotransfer ---- 215
9.4.1 Was eine Cyberversicherung leistet ---- 215
9.4.1 Was eine Cyberversicherung nicht leistet ---- 215

9.5 Risikoakzeptanz ---- 218
9.5.1 Elemente einer vollständigen Risikoakzeptanz ---- 219
9.5.2 Wann Risikoakzeptanz eskaliert werden muss ---- 220

9.6 Risikobehandlung ---- 220

9.7 Governance Failure Pattern ---- 222

9.8 Risikobehandlung kommunizieren ---- 223

9.9 Executive Decision ---- 224

9.10 Exam Essentials – Kapitel 9 ---- 227

10 METRIKEN 229

10.1 KPI vs. KRI ---- 230

10.2 Gute Metriken – schlechte Metriken ---- 232

10.3 Wesentliche KPIs ---- 234

10.3.1 Vulnerability-Metriken ---- 234

10.3.2 Incident-Metriken ---- 235

10.3.3 Control-Wirksamkeitsmetriken ---- 235

10.4 KRIs: Frühwarnsignale für wachsende Risiken ---- 236

10.5 Das Security-Dashboard ---- 238

10.6 Governance Failure Pattern ---- 241

10.7 Kontinuierliche Verbesserung ---- 242

10.8 Executive Decision ---- 243

10.9 Surrogat-Metriken ---- 245

10.10 Benchmarking: Der externe Maßstab ---- 246

10.11 Metriken im Audit-Kontext ---- 247

10.12 Der Metriken-Review-Zyklus ---- 248

10.13 Exam Essentials – Kapitel 10 ---------- 249

11 SECURITY-PROGRAMME 253

11.1 Was ein Security-Programm ausmacht ---------- 254

11.2 Die Programmarchitektur ---------- 256

11.3 Programmkomponenten im Detail ---------- 257

11.3.1 Identity and Access Management (IAM) ---------- 257

11.3.2 Change Management ---------- 258

11.3.3 Data Loss Prevention (DLP) ---------- 259

11.3.4 Vendor und Third-Party Management ---------- 260

11.4 Security by Design ---------- 260

11.5 Programmreife ---------- 263

11.6 Programm-Roadmap ---------- 265

11.7 Budget-Planung ---------- 267

11.8 Outsourcing von Security-Funktionen ---------- 268

11.9 Security-Programm und Kultur ---------- 269

11.10 Governance Failure Pattern ---------- 270

11.11 Executive Decision ---------- 271

11.12 Exam Essentials – Kapitel 11 ---------- 273

12 COMPLIANCE UND REGULATORISCHER DRUCK... 277

12.1 Compliance vs. Sicherheit ---- 278

12.2 NIS-2 – die neue Ära ---- 281
12.2.1 Wer ist betroffen? ---- 281
12.2.2 Die zehn Mindestmaßnahmen nach Art. 21 ---- 282
12.2.3 Die Managementhaftung unter NIS-2 ---- 283
12.2.4 Meldepflichten: Die 24-Stunden-Uhr ---- 284

12.3 DORA ---- 285
12.3.1 Die fünf DORA-Säulen ---- 286
12.3.2 TLPT: Threat-Led Penetration Testing ---- 287
12.3.3 DORA und Third-Party-Anforderungen ---- 288

12.4 Der EU AI Act ---- 289
12.4.1 Die Risikokategorien des EU AI Acts ---- 289
12.4.2 EU AI Act und Security-Systeme ---- 290

12.5 Audit-Management ---- 292
12.5.1 Audit-Typen im Überblick ---- 292
12.5.2 Der Audit-Prozess ---- 293
12.5.3 Audit-Findings: Umgang und Eskalation ---- 295

12.6 Executable Compliance ---- 296
12.6.1 Drei Dimensionen der Executable Compliance ---- 296
12.6.2 Executable Compliance in der Prüfung ---- 297

12.7 Governance Failure Pattern ---- 298

12.8 Compliance-Programme steuern ---- 299

12.9 Executive Decision: Der Regulierungsdruck ---------- 301

12.10 Exam Essentials – Kapitel 12 ---------- 303

13 SECURITY SCHEITERT ORGANISATORISCH..... 305

13.1 Das Scheitern-Modell ---------- 306

13.2 Muster des organisatorischen Scheiterns ---------- 307

13.3 Die Diagnose ---------- 316

13.3.1 Das Governance-Health-Assessment ---------- 316

13.3.2 Signale, die auf Failure Patterns hinweisen ---------- 319

13.4 Der CISO als organisatorischer Gestalter ---------- 320

13.5 Governance Failure Pattern ---------- 322

13.6 Executive Decision: Die Diagnose ---------- 323

13.7 Exam Essentials – Kapitel 13 ---------- 325

14 DIE ILLUSION TECHNISCHER SICHERHEIT 327

14.1 Was technische Sicherheit leisten kann ---------- 328

14.2 Tool-Fixierung ---------- 329

14.3 Die Kosten der Tool-Proliferation ---------- 331

14.4 Alert-Fatigue ---------- 333

14.4.1 Ursachen von Alert-Fatigue ---------- 334

14.4.2 Gegenmaßnahmen gegen Alert-Fatigue ---------- 335

14.5 Technologie-Prozess-Menschen-Gleichgewicht ---- 336
14.5.1 Die Technologie-Dimension ---- 336
14.5.2 Die Prozess-Dimension ---- 337
14.5.3 Die Menschen-Dimension ---- 338

14.6 Der richtige Tool-Stack ---- 339

14.7 Operative Überlastung ---- 341

14.8 Von der Prävention zur Resilienz ---- 342

14.9 Governance Failure Pattern ---- 344

14.10 Tool-Konsolidierung ---- 345

14.11 Executive Decision ---- 346

14.12 Exam Essentials – Kapitel 14 ---- 348

15 INCIDENT MANAGEMENT 353

15.1 Incident Management im CISM-Kontext ---- 354

15.2 Der Incident-Response-Lifecycle ---- 355

15.3 Incident-Klassifizierung ---- 358
15.3.1 Klassifizierungskriterien ---- 359
15.3.2 Ein Klassifizierungsschema ---- 359

15.4 Der Incident-Response-Plan ---- 360
15.4.1 Pflichtbestandteile eines IRP ---- 361
15.4.2 Testen des IRP: Tabletop-Übungen ---- 362

15.5 Meldepflichten im Incident-Response-Plan ---------- 363

15.6 Governance im Krisenfall ---------- 365
15.6.1 Die Krisenrollen ---------- 365
15.6.2 Containment-Entscheidungen ---------- 366

15.7 Post-Incident Review ---------- 368
15.7.2 Struktur eines Post-Incident Reviews ---------- 369
15.7.3 Kulturelle Rahmenbedingungen ---------- 370

15.8 Evidence Management ---------- 371

15.9 Governance Failure Pattern ---------- 372

15.10 Executive Decision ---------- 373

15.11 Exam Essentials – Kapitel 15 ---------- 375

16 BUSINESS CONTINUITY/DISASTER RECOVERY 377

16.1 BCM, BCP und DRP ---------- 378

16.2 Business Impact Analysis ---------- 380
16.2.1 Die BIA-Methodik ---------- 381
16.2.2 Kritische Kennzahlen: RTO und RPO ---------- 382

16.3 Recovery-Strategien für IT-Systeme ---------- 385

16.4 Der Business Continuity Plan ---------- 386
16.4.1 Pflichtbestandteile eines BCP ---------- 386
16.4.2 Aktivierungsstufen ---------- 387

16.5 BCM testen ---------- 388

16.6 BCM und Incident Management ---------- 390

16.7 BCM und regulatorische Anforderungen ---------- 391

16.8 Governance Failure Pattern ---------- 392

16.9 Executive Decision: RTO vs. Budget ---------- 393

16.10 Exam Essentials – Kapitel 16 ---------- 395

17 KOMMUNIKATION UND ESKALATION..... 397

17.1 Kommunikationslandschaft im Incident ---------- 398

17.2 Eskalationspfade ---------- 400

17.2.1 Das Eskalations-Prinzip ---------- 401

17.2.2 Der Eskalationsbaum ---------- 401

17.3 Interne Kommunikation ---------- 403

17.4 Externe Kommunikation ---------- 406

17.4.1 Kundenkommunikation: Schneller als die Medien ------ 406

17.4.2 Medienkommunikation ---------- 407

17.4.3 Regulatorische Kommunikation: ---------- 408

17.5 Krisenkommunikation und Social Media ---------- 408

17.6 Der Communications Lead ---------- 410

17.7 Häufige Krisenkommunikationsfehler ---------- 411

17.8 Krisenkommunikation und Recht ----------412

17.9 Governance Failure Pattern ----------413

17.10 Executive Decision: Die Presseanfrage ----------414

17.11 Exam Essentials – Kapitel 17 ----------416

18 ENTSCHEIDUNGSSZENARIEN 421

18.1 Szenario 1: Governance trifft Supply-Chain----------423

18.2 Szenario 2: Der Insider-Verdacht----------427

18.3 Szenario 3: Der kompromittierte Lieferant ----------429

18.4 Szenario 4: die Governance-Lücke----------431

18.5 Szenario 5: Die Krise mit Vertrauensschaden ----------433

18.6 Was die fünf Szenarien gemeinsam haben----------435

18.7 Selbsttest: Zehn Kernfragen----------436

18.8 Exam Essentials – Kapitel 18 ----------438

19 PRÜFUNGSSTRATEGIE..... 441

19.1 Die CISM-Prüfung: Fakten und Format----------442

19.2 Fragen methodisch lesen----------443

19.3 Die 15 häufigsten Denkfehler ----------447

19.4 Zeitmanagement in der Prüfung ---------- 450
19.4.1 Die drei Durchgänge ---------- 450
19.4.2 Zeitwarnsignale ---------- 451

19.5 Die letzten Wochen: Der Lernplan ---------- 451

19.6 Die letzten 72 Stunden ---------- 452

19.7 Der Prüfungstag ---------- 454

19.8 Was tun, wenn es nicht geklappt hat? ---------- 455

19.9 Die ISACA-Entscheidungslogik ---------- 456

19.10 Ein letztes Wort ---------- 457

19.11 Exam Essentials – Kapitel 19 ---------- 458

ANHANG A – ONLINE-PLATTFORM XXI

Zugriff auf die Plattform ---------- XXI

Lernfortschritt und kontinuierliche Verbesserung ---------- XXIII

ANHANG B – CISM QUICK REFERENCE GUIDE XXIV

Governance-Prinzipien ---------- XXIV

Risk-Response-Modelle ---------- XXVII

Wichtigste Frameworks ---------- XXX

Governance-Entscheidungslogik ---------- XXXII

CISM Quick Review ---------- XXXV

ANHANG C – REGULATORY MAPPING XXXIX

NIS-2-Anforderungen (Art. 21) ---------- XXXIX

DORA-Anforderungen ---------- XL

ISO 27001:2022 ---------- XLII

ISO 42001:2023 ---------- XLII

Gesamtübersicht ---------- XLIV

GLOSSAR XLV

ABKÜRZUNGSVERZEICHNIS LIII

LITERATUR- UND QUELLENVERZEICHNIS LVI

STICHWORTVERZEICHNIS LIX

MEHR VON BRAIN-MEDIA.DE LXV

Wie Sie dieses Buch benutzen

Die Entscheidung, sich auf die CISM-Zertifizierung vorzubereiten, ist selten eine rein akademische. Meist steht dahinter der Wunsch – oder die Notwendigkeit –, aus der operativen, technischen Rolle in eine steuernde Management-Position aufzusteigen. Vielleicht hat Ihr Vorgesetzter die CISM-Zertifizierung als Voraussetzung für die nächste Beförderung genannt. Vielleicht haben Sie selbst erkannt, dass Ihr Einfluss in Sicherheitsfragen größer wäre, wenn Sie die Sprache des Managements sprechen. Oder Sie stehen einfach vor einem Regal mit CISM-Lehrbüchern und fragen sich: Welches davon bringt mich wirklich durch die Prüfung?

Dieses Buch gibt eine ehrliche Antwort auf diese Frage – und die Antwort beginnt mit einem Eingeständnis: Der Weg zum CISM ist kein Sprint durch ein technisches Handbuch. Er ist ein Prozess des Umdenkens. Viele erfahrene IT-Experten scheitern an dieser Prüfung nicht, weil sie zu wenig wissen, sondern weil sie zu viel wissen. Oder genauer: weil sie das Richtige auf die falsche Weise wissen.

Dieses Kapitel erklärt Ihnen, wie dieses Buch gebaut ist, warum es so gebaut ist, und wie Sie es benutzen sollten, um den maximalen Nutzen zu erzielen. Es ist kein Pflichtkapitel im klassischen Sinne – aber es ist das Kapitel, das den Unterschied macht zwischen einer Investition und einer vergeudeten Vorbereitung.

Was diese Prüfung wirklich testet

Bevor wir darüber sprechen, wie dieses Buch aufgebaut ist, müssen wir verstehen, was die CISM-Prüfung eigentlich misst. Diese Frage wird in der Vorbereitung häufig übersprungen – ein Fehler, der teuer werden kann . Die meisten IT-Zertifizierungen testen Wissen. Sie fragen, welche Verschlüsselungsstärke ein Algorithmus hat, welche Ports für ein bestimmtes Protokoll geöffnet werden müssen oder wie man ein VLAN konfiguriert. Wer auswendig gelernt hat, besteht. Der CISM tut das nicht.

Der CISM testet Urteilsfähigkeit. Er setzt voraus, dass Sie wissen, dass Verschlüsselung existiert – aber er will von Ihnen wissen: Sollten wir sie hier einsetzen? Wer trägt die Verantwortung, wenn wir es nicht tun? Wie messen wir, ob sie effektiv ist? Das sind keine Wissensfragen. Das sind Managemententscheidungen.

ISACA, der Herausgeber der CISM-Zertifizierung, beschreibt den idealen Kandidaten nicht als jemanden, der Sicherheitstechnologien beherrscht. Er beschreibt ihn als jemanden, der ein Sicherheitsprogramm entwickeln, steuern und verantworten kann – im vollen Bewusstsein der Geschäftsziele, der Risikotoleranz des Unternehmens und der regulatorischen Anforderungen der Branche.

Das klingt abstrakt. Doch in der Prüfung wird es sehr konkret. Sie werden mit Szenarien konfrontiert, in denen Sie als Security Manager eine Entscheidung treffen müssen. Die vier Antwortoptionen sind oft alle technisch korrekt. Ihre Aufgabe ist es, die „beste“ Antwort zu finden – die management-relevanteste, die strategisch nachhaltigste, die risikobewussteste.

Was „beste Antwort" bedeutet

In CISM-Prüfungsfragen bedeutet „beste Antwort" nicht: die technisch korrekteste. Es bedeutet: Die Antwort, die ein erfahrener, strategisch denkender Information Security Manager in einer gut geführten Organisation zuerst ergreifen würde.

Es gibt drei Filter für die „beste" Antwort:

1. Strategie vor Taktik: Welche Antwort legt das Fundament für alle anderen?
2. Bewertung vor Reaktion: Welche Antwort beginnt mit Analyse statt mit Aktion?
3. Governance vor Technik: Welche Antwort adressiert die strukturelle Ursache, nicht das Symptom?

Warum dieses Buch anders aufgebaut ist

Wer das offizielle ISACA-Lernmaterial kennt, wird beim Aufschlagen dieses Buches eine Überraschung erleben: Die Kapitelreihenfolge entspricht nicht der offiziellen Domänensequenz. Das ist kein Versehen. Es ist eine bewusste didaktische Entscheidung, die auf einem einfachen Prinzip basiert:

Die CISM-Denkweise kommt zuerst. Die Prüfungsdomänen rahmen das Buch von Anfang an. Und die Kapitel folgen der Reihenfolge, in der ein Lernender sie braucht – nicht der Reihenfolge, in der sie im Curriculum gedruckt stehen.

Klassische CISM-Bücher starten mit Domäne 1 (Information Security Governance) und arbeiten sich durch. Das hat Logik – aber es hat auch einen Nachteil: Ein Kandidat, der in Kapitel 1 mit abstrakten Governance-Konzepten konfrontiert wird, ohne zu verstehen, warum diese Konzepte prüfungsrelevant sind und wie sie mit dem Rest des Stoffs zusammenhängen, entwickelt kein tragfähiges mentales Modell. Er lernt Fakten, aber das Verständnis für die Zusammenhänge bleibt vielfach auf der Strecke.

Dieses Buch beginnt deshalb mit dem Metawissen: Wie ist die Prüfung aufgebaut? Welche Logik steckt dahinter? Wie lese ich Fragen, und wie trainiere ich die Entscheidungsgewalt, die der CISM verlangt? Erst wenn dieses Fundament steht, gehen wir in die Domänen – und dort folgen wir einer Reihenfolge, die dem Lernprozess entspricht, nicht der Druckreihenfolge.

Die Gliederungslogik im Überblick

Das Buch ist in fünf Bereiche unterteilt:

Bereich	Titel	Inhalt
Einführung und Kapitel 1	Die CISM-Prüfung verstehen	Buchaufbau, Lernstrategien, Domänenüberblick, ISACA-Logik
Teil I (Kap. 2–6)	Information Security Governance	Domäne 1: Governance, Rollen, Frameworks, Kultur
Teil II (Kap. 7–10)	Information Risk Management	Domäne 2: Risikomodelle, Bewertung, Behandlung, Metriken
Teil III (Kap. 11–14)	Information Security Program	Domäne 3: Programmaufbau, Compliance, Failure Patterns
Teil IV (Kap. 15–17)	Incident Management	Domäne 4: Incident Response, BCM, Kommunikation
Abschluss (Kap. 18–19)	Prüfungsvorbereitung	Entscheidungsszenarien, Prüfungsstrategie, Denkfehler

Die vier Strukturelemente jedes Kapitels

Jedes Kapitel dieses Buches folgt einem festen Aufbau. Diese Konsistenz ist kein stilistisches Mittel – sie ist ein Lernwerkzeug. Im ersten Lesedurchgang gibt sie Ihnen Orientierung. Im zweiten Durchgang ermöglicht sie gezieltes Nachschlagen, ohne das gesamte Kapitel erneut lesen zu müssen.

Element 1: Der theoretische Kern

Hier vermitteln wir das konzeptionelle Fundament. Wir orientieren uns strikt an den vier Domänen der ISACA, reichern diese aber mit dem Konzept der Executable Compliance an. Während klassische Lehrbücher oft bei der Beschreibung von Frameworks stehen bleiben, stellen wir immer die Anschlussfrage: Wie sieht dieses Framework aus, wenn es am Montagmorgen in einer Organisation mit 3.000 Mitarbeitern und begrenztem Budget implementiert werden muss?

Der theoretische Kern verzichtet bewusst auf technische Details, die Sie in Sekundenbruchteilen googeln können. Er konzentriert sich auf die Konzepte, Modelle und Unterscheidungen, die die ISACA in ihren Prüfungsfragen voraussetzt. Er erklärt nicht nur was, sondern immer auch warum – und in welchem Verhältnis das Gelernte zu den anderen Domänen steht.

Element 2: Governance Failure Patterns

Dies ist das Herzstück des Buches und sein deutlichstes Alleinstellungsmerkmal. Menschen lernen am effektivsten durch Narrative – und besonders gut durch Katastrophen, die sie noch nicht selbst erlebt haben.

Die Governance Failure Patterns sind archetypische Fehlkonstellationen aus der Praxis. Sie beschreiben nicht, was in einer einzelnen Organisation schiefgelaufen ist, sondern warum es schiefläuft – strukturell, systemisch, domänenübergreifend. Sie sind fiktional ausgearbeitet, aber jeder Praktiker, der sie liest, wird mindestens eines wiedererkennen.

Typische Patterns in diesem Buch: das CISO-Paradoxon (Verantwortung ohne Befugnis), der Compliance-Tunnel (Papierkonformität ohne echte Sicherheit), die Tool-Gläubigkeit (Technologieinvestition statt Risikostrategie) oder die stille Eskalation (Incidents, die niemand meldet, weil der Prozess zu schmerzhaft ist).

Der Nutzen dieser Abschnitte für die Prüfungsvorbereitung ist zweifach. Erstens schärfen sie Ihren Blick für Distraktoren: jene Antwortoptionen, die in einer schlecht geführten Organisation normal klingen, aber fundamental falsch sind. Zweitens trainieren sie das Mustererkennen, das schnelle Entscheidungen unter Zeitdruck ermöglicht.

Element 3: Executive Decisions

Ein Security Manager, der keine Entscheidungen treffen kann, ist ein teurer Berater. In den Executive-Decision-Abschnitten konfrontieren wir Sie mit echten Dilemmata – Situationen, in denen es keine perfekte Lösung gibt, sondern nur Optionen mit unterschiedlichen Risikoprofilen.

Das Ziel ist nicht, die richtige Antwort auswendig zu lernen. Das Ziel ist, den Entscheidungsprozess zu internalisieren: Welche Faktoren werden gewichtet? Welche Interessen stehen im Konflikt? Welchen Weg würde die ISACA einschlagen – und warum?

Die Executive Decisions sind bewusst so konstruiert, dass alle Antwortoptionen vertretbar wirken. Das spiegelt die Prüfungsrealität wider: ISACA-Fragen haben selten eine offensichtlich falsche Option. Sie haben eine beste Option – und drei gute, aber nicht optimale. Wer hier trainiert, schärft genau die Urteilsfähigkeit, die zwischen Bestehen und Scheitern entscheidet.

Element 4: Exam Essentials

Am Ende jedes Kapitels finden Sie die Exam Essentials. Dies ist die komprimierte Essenz für den letzten Meter vor der Prüfung. Die Exam Essentials sind keine Zusammenfassung des Kapitels – sie sind eine Checkliste der Begriffe, Konzepte und Unterscheidungen, die Sie in der Prüfungssituation in Sekundenbruchteilen abrufen müssen.

Residual Risk und Inherent Risk. Risk Appetite und Risk Tolerance. RACI-Matrix und Drei-Linien-Modell. Post-Incident Review und Root Cause Analysis. Diese Begriffe sind in der ISACA-Welt präzise definiert und werden in Fragen bewusst abgrenzend verwendet. Die Exam Essentials verankern diese Definitionen so, dass Sie in der Prüfungssituation nicht mehr über ihre Bedeutung nachdenken müssen – Sie handeln instinktiv richtig.

Zwei Lesedurchgänge – und warum beide nötig sind

Dieses Buch ist explizit für zwei Lesemodi konzipiert. Die meisten Kandidaten, die bei der CISM-Prüfung scheitern, haben nur einen davon durchgeführt – und dann erstaunt festgestellt, dass Wissen allein nicht ausreicht.

Der erste Pass: Die Weitung des Horizonts

Im ersten Durchgang lesen Sie dieses Buch wie ein Sachbuch. Ihr Ziel ist nicht, Fakten zu memorieren. Ihr Ziel ist, ein neues mentales Modell aufzubauen – das des Information Security Managers.

Lassen Sie sich auf die Analysen ein. Verstehen Sie, warum die reine Tool-Gläubigkeit eine Sackgasse ist. Begreifen Sie, wie Governance und Incident Response zusammenhängen – und warum eine schlecht definierte Eskalationskette in Domäne 1 dazu führt, dass ein Incident in Domäne 4 eskaliert, statt gesteuert zu werden. Fragen Sie sich bei jedem Governance Failure Pattern: Kenne ich diese

Situation aus meinem eigenen Umfeld? Und bei jeder Executive Decision: Was hätte ich entschieden – und warum liegt meine Intuition möglicherweise daneben?

Im ersten Pass markieren Sie nicht, lernen Sie nichts auswendig, erstellen Sie keine Karteikarten. Sie lesen. Sie denken. Sie kalibrieren Ihren inneren Kompass.

- Lesen Sie linear, von Kapitel 0 bis Kapitel 19.
- Markieren Sie nur Stellen, die Ihre bisherige Intuition konterkarieren.
- Notieren Sie am Rand Fragen – keine Antworten.
- Geplante Zeit: drei bis fünf Wochen bei einem Kapitel pro Tag.

Der zweite Pass: Der Prüfungsdrill

Der zweite Durchgang ist zielgerichteter und messbarer. Jetzt geht es darum, die ISACA-Logik unter Zeitdruck abrufbar zu machen. Die CISM-Prüfung umfasst 150 Fragen in 240 Minuten – das entspricht knapp 96 Sekunden pro Frage. In dieser Zeit müssen Sie nicht nur die richtige Antwort erkennen, Sie müssen die falschen Antworten aktiv disqualifizieren können.

Für den zweiten Pass nutzen Sie die Exam Essentials als primäre Referenz. Testen Sie sich selbst: Können Sie den Unterschied zwischen Risk Appetite und Risk Tolerance in zwei Sätzen erklären? Können Sie das Drei-Linien-Modell aus dem Gedächtnis skizzieren? Können Sie ad hoc drei Argumente nennen, warum ein technisch perfektes

Security-Tool ohne Governance-Rahmen trotzdem ein Risiko darstellt?

- Fokus auf Exam Essentials und Executive Decisions.
- Karteikarten für ISACA-spezifische Terminologie.
- Self-Assessment-Fragen unter Zeitdruck (max. 96 Sekunden pro Frage).
- Jede falsch beantwortete Frage vollständig analysieren: nicht nur warum B richtig ist, sondern warum A, C und D falsch sind.
- Kapitel mit unter 75 Prozent Trefferquote vollständig wiederholen.
- Geplante Zeit: zwei bis drei Wochen vor der Prüfung.

Häufiger Fehler: Den zweiten Pass weglassen

Viele Kandidaten absolvieren einen gründlichen ersten Pass, bauen Karteikarten, lesen Zusammenfassungen – und treten dann direkt zur Prüfung an. Das Ergebnis: Sie kennen die Begriffe, aber sie scheitern an den Szenarien. Der zweite Pass ist kein optionales Extra. Er ist der Moment, in dem Wissen zu Urteilsfähigkeit wird.

Planen Sie den zweiten Pass als eigenständige Lernphase mit eigenem Zeitplan.

Die Psychologie der Prüfungsvorbereitung

Die Vorbereitung auf den CISM ist nicht nur eine intellektuelle, sondern auch eine mentale Herausforderung. Es gibt einige psychologische Muster, die Kandidaten systematisch in die Irre führen. Sie hier zu benennen ist der erste Schritt, sie zu überwinden.

Der Expert Bias

Das verbreitetste Muster: Kandidaten mit umfangreicher IT-Security-Erfahrung tendieren dazu, Prüfungsfragen aus ihrer operativen Brille zu lesen. Sie wählen die Antwort, die in ihrer Organisation funktioniert – nicht die Antwort, die in einer idealen, governance-gesteuerten Welt nach ISACA-Standard richtig wäre.

Der Expert Bias ist kein Zeichen mangelnder Kompetenz. Er ist das Gegenteil: ein Zeichen tiefer, gelebter Erfahrung, die in der Prüfung systematisch gegen den Kandidaten arbeitet. Die Therapie ist nicht, die Erfahrung zu vergessen – es ist, sie bewusst in Klammern zu setzen und sich bei jeder Antwort zu fragen: Antworte ich als Manager oder als Techniker?

Das Vollständigkeitsparadoxon

Ein anderes Muster betrifft das Lerntempo. Manche Kandidaten versuchen, alles vollständig zu verstehen, bevor sie weiterlesen. Sie bleiben an einzelnen Konzepten hängen, recherchieren jedes unklare Detail, und kommen nie durch das Buch. Das Ergebnis:

perfektes Wissen über 30 Prozent des Stoffs – und Lücken in den restlichen 70 Prozent.

Die CISM-Prüfung deckt alle vier Domänen ab. Wer in einer Domäne exzellent ist und in einer anderen schwach, riskiert das Scheitern. Breadth beats depth – zumindest in der ersten Lernphase. Lesen Sie das Buch vollständig durch, bevor Sie anfangen, einzelne Kapitel zu vertiefen.

Die Simulation als Vorbereitung

Der häufigste ungenutzte Hebel in der CISM-Vorbereitung: simuliertes Prüfen unter realen Bedingungen. Viele Kandidaten üben Fragen, aber ohne Zeitdruck, ohne die emotionale Qualität einer echten Prüfungssituation, und mit dem Buch griffbereit.

Das ist wertvoll für das Lernen – aber es ist keine Prüfungsvorbereitung. Prüfungsvorbereitung bedeutet: 150 Fragen, 240 Minuten, keine Hilfsmittel, einmal pro Woche in der letzten Vorbereitungsphase. Nur wer unter diesen Bedingungen übt, weiß, wie er unter diesen Bedingungen performt.

Um Ihnen das Lernen zu vereinfachen und Sie optimal bei der Vorbereitung zu unterstützen, stellen wir Ihnen einen Online-Fragebogen bereit, der sich aus 800 Fragen bedient. So können Sie sich unter realistischen Bedingungen optimal vorbereiten.

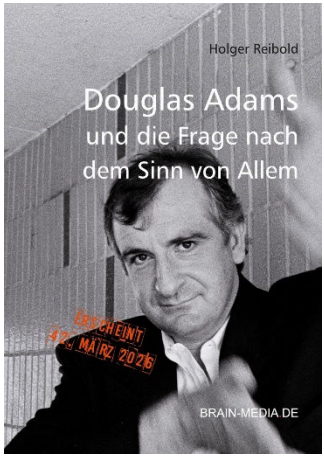
Die Prüfungsdomänen als Rahmen des Buches

Die vier Domänen des CISM sind nicht nur eine Prüfungsstruktur. Sie sind ein mentales Modell der Rolle eines Information Security Managers – und sie rahmen dieses Buch von Anfang an. In Kapitel 1 werden wir die Domänen im Detail einführen, ihr relatives Gewicht erklären und die Zusammenhänge zwischen ihnen sichtbar machen. Für den Moment reicht ein erster Orientierungspunkt:

- Domäne 1 – Information Security Governance: Das Fundament. Wer entscheidet was, mit welchem Mandat und in welchem Rahmen?
- Domäne 2 – Information Risk Management: Der Kompass. Wie identifizieren, bewerten und priorisieren wir Risiken?
- Domäne 3 – Information Security Program: Das Programm. Wie bauen, steuern und messen wir ein funktionierendes Sicherheitsprogramm?
- Domäne 4 – Information Security Incident Management: Die Belastungsprobe. Was tun wir, wenn trotz allem etwas schiefgeht?

Diese vier Fragen – Wer entscheidet? Was riskieren wir? Wie bauen wir? Was tun wir im Krisenfall? – begleiten uns durch das gesamte Buch. Jedes Kapitel, jedes Governance Failure Pattern, jede Executive Decision lässt sich auf eine oder mehrere dieser Fragen zurückführen. Wenn Sie an einem Punkt des Buches den Faden verlieren, ist diese Rückführung Ihr Kompass.

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

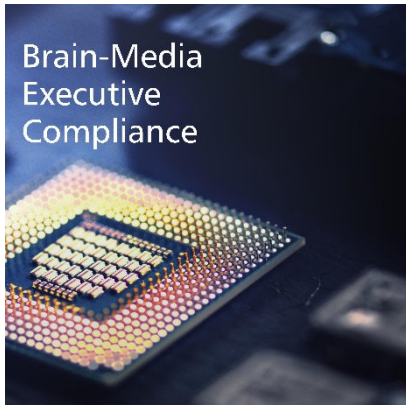
Towelday, das ultimative Handtuch für alle Fans

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.