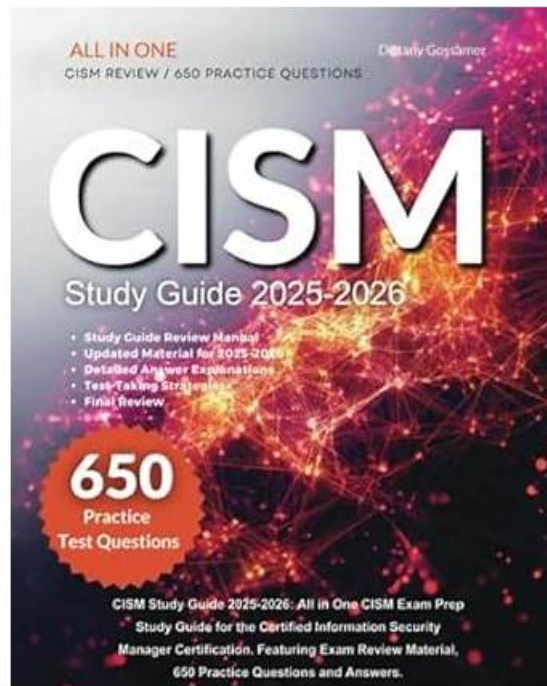


# CISM Übungsmaterialien - CISM Lernressourcen & CISM Prüfungsfragen



P.S. Kostenlose und neue CISM Prüfungsfragen sind auf Google Drive freigegeben von ZertSoft verfügbar:  
[https://drive.google.com/open?id=1-XaNmUjY\\_JGpOmB8FSjU7P1Z3n5o8OAF](https://drive.google.com/open?id=1-XaNmUjY_JGpOmB8FSjU7P1Z3n5o8OAF)

Die Feedbacks von den IT-Kandidaten, die die schulungsunterlagen zur ISACA CISM (Certified Information Security Manager) IT-Prüfung von ZertSoft benutzt haben, haben sich bewiesen, dass es leicht ist, die Prüfung mit Hilfe unserer ZertSoft Produkten zu bestehen. Zur Zeit hat ZertSoft die Schulungsprogramme zur beliebten ISACA CISM (Certified Information Security Manager) Zertifizierungsprüfung, die zielgerichteten Prüfungen beinhalten, entwickelt, um Ihr Know-How zu konsolidieren und sich gut auf die Prüfung vorzubereiten.

Die Certified Information Security Manager (CISM) Zertifizierungsprüfung ist eine weltweit anerkannte Qualifikation für Informationssicherheitsfachleute. Es wird von der Information Systems Audit and Control Association (ISACA), einem gemeinnützigen Berufsverband, der sich auf IT-Governance, Sicherheit und Audit konzentriert, angeboten. Die CISM-Zertifizierung ist darauf ausgelegt, die Fähigkeiten und Kenntnisse zu validieren, die erforderlich sind, um das Informations-Sicherheitsprogramm einer Organisation zu verwalten, zu entwerfen und zu überwachen.

Die ISACA CISM -Prüfung (Certified Information Security Manager) ist ein weltweit anerkanntes Zertifizierungsprogramm zur Überprüfung der Fähigkeiten und des Wissens von Fachkräften für Informationssicherheit. Die Zertifizierung wird von der Information Systems Audit and Control Association (ISACA) vergeben und wird von vielen Organisationen weltweit anerkannt. Die CISM -Zertifizierung wurde speziell für Personen entwickelt, die für die Entwicklung, Verwaltung und Überwachung von Informationssicherheitsprogrammen in ihren Organisationen verantwortlich sind.

>> CISM Testfragen <<

## CISM Schulungsangebot - CISM Simulationsfragen & CISM kostenlos downloaden

Alle Anfang ist schwer. Zögern Sie noch, wie mit der Vorbereitung der ISACA CISM Prüfung anfangen? Die Prüfungsunterlagen der ISACA CISM von uns zu kaufen wird ein notwendiger Schritt Ihrer Vorbereitung. Was wir Ihnen bieten, ist nicht nur was Sie möchten, sondern auch was für Ihre Vorbereitung der ISACA CISM Prüfung unerlässlich ist. Vielleicht haben Sie noch Hemmungen mit diesem Schritt. So können Sie zuerst die Demo der ISACA CISM Prüfungsunterlagen herunterladen. Nachdem Sie probiert haben, werden Sie bestimmt diesen Schritt machen.

Die Zertifizierungsprüfung der ISACA CISM (Certified Information Security Manager) ist eines der angesehensten und anerkannten Zertifizierungsprogramme im Bereich der Informationssicherheit. Die Zertifizierung ist für Fachleute konzipiert, die für die Verwaltung, Gestaltung, Überwachung und Bewertung von Informationssicherheitsprogrammen auf Unternehmensebene verantwortlich sind. Es handelt sich um ein Zertifizierungsprogramm auf fortgeschrittener Ebene, das die Fähigkeit einer Person bewertet, Sicherheitsprogramme zu verwalten, zu entwerfen und zu überwachen und dem Sicherheitsteam Führung zu bieten.

### ISACA Certified Information Security Manager CISM Prüfungsfragen mit Lösungen (Q97-Q102):

#### 97. Frage

Which of the following defines the MOST comprehensive set of security requirements for a newly developed information system?

- A. Key risk indicators (KRIs)
- B. Audit findings
- C. Risk assessment results
- **D. Baseline controls**

**Antwort: D**

Begründung:

Baseline controls are the minimum set of security requirements that apply to all information systems in an organization, regardless of their specific functions or characteristics. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance. Baseline controls provide a consistent and comprehensive foundation for the security of the information systems, and they can be tailored or supplemented by additional controls as needed for specific systems or situations. The other options are not as comprehensive as baseline controls, as they may only address certain aspects or aspects of the security requirements, or they may vary depending on the system or the context. For example, risk assessment results are an important input for defining the security requirements, but they are not the requirements themselves. Audit findings are an output of evaluating the compliance and effectiveness of the security requirements, but they are not the requirements themselves. Key risk indicators (KRIs) are metrics that measure the level of risk exposure and performance of the security requirements, but they are not the requirements themselves. Reference = CISM Review Manual 15th Edition, page 113: "Baseline controls are the minimum security requirements that apply to all systems within the organization." CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, question 478: "Baseline controls are the minimum security requirements that apply to all systems within the organization. They are derived from the organization's security policies, standards, and best practices, and they reflect the organization's risk appetite and tolerance."

#### 98. Frage

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- **A. Residual risk**
- B. Risk exposure
- C. Control risk
- D. Inherent risk

**Antwort: A**

Begründung:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

### 99. Frage

An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

- A. Improper authorization
- **B. Lack of accountability**
- C. Lack of availability
- D. Inadequate authentication

**Antwort: B**

Begründung:

The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. Reference:

<https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam>

<https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices>

<https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam>

### 100. Frage

Management has expressed concerns to the information security manager that shadow IT may be a risk to the organization. What is the FIRST step the information security manager should take?

- A. Update the security policy to address shadow IT
- B. Block the end user's ability to use shadow IT
- C. Determine the value of shadow IT projects
- **D. Determine the extent of shadow IT usage**

**Antwort: D**

Begründung:

The first step is to determine the extent of shadow IT usage (A). CISM emphasizes understanding the current state before implementing controls or policy changes. Without knowing where and how shadow IT exists, actions such as blocking usage (C) or updating policy (B) may disrupt business operations unnecessarily.

Evaluating value (D) is secondary. Identifying scope enables informed risk assessment and proportionate response.

References: ISACA CISM Review Manual (Governance-risk identification and assessment); CISM Exam Content Outline (Domain 2).

### 101. Frage

Which of the following is the MOST important consideration when reporting on the status of information security activities?

- **A. The report is tailored to stakeholder needs**
- B. The report is comprehensive
- C. The report is updated on a regular basis
- D. The report structure is consistent with industry standards

**Antwort: A**

### 102. Frage

.....

**CISM Unterlage:** <https://www.zertsoft.com/CISM-pruefungsfragen.html>

