CISSP®

Certified Information
Systems Security Professional

Zusammenfassung

Claudius Link

Über mich

Claudius Link

Dipl. Mathematiker

System Admin, SW Entwickler, Führungskraft, SIcherheitverantwortlicher

CISSP (pending), ISO 27001 Lead Implementer

claudius.link@gmail.com

@realn2s

Agenda

- Was ist CISSP?
- Inhalte
  - Domains
- Ist CISSP was für mich?
- Resources

Was ist CISSP?

- **Was ist CISSP?**
- Inhalte
  - Domains
- Ist es was für mich?
- Resources

Was ist CISSP?

- Certification Programm by (ISC)2
- (ISC)2 code of ethics
- Certification exam
- “Professional” - 5 years of experience
- Kontinuierliche Weiterbildung

Security and Risk Management

(ISC)2 Code of Ethics

Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Canons:

1. Protect society, the commonwealth, and the infrastructure.
2. Act honorably, honestly, justly, responsibly, and legally.
3. Provide diligent and competent service to principals.
4. Advance and protect the profession

Was ist CISSP?

Informationssicherheit aus Vogelperspektive

Mile wide, inch deep

oder metrisch

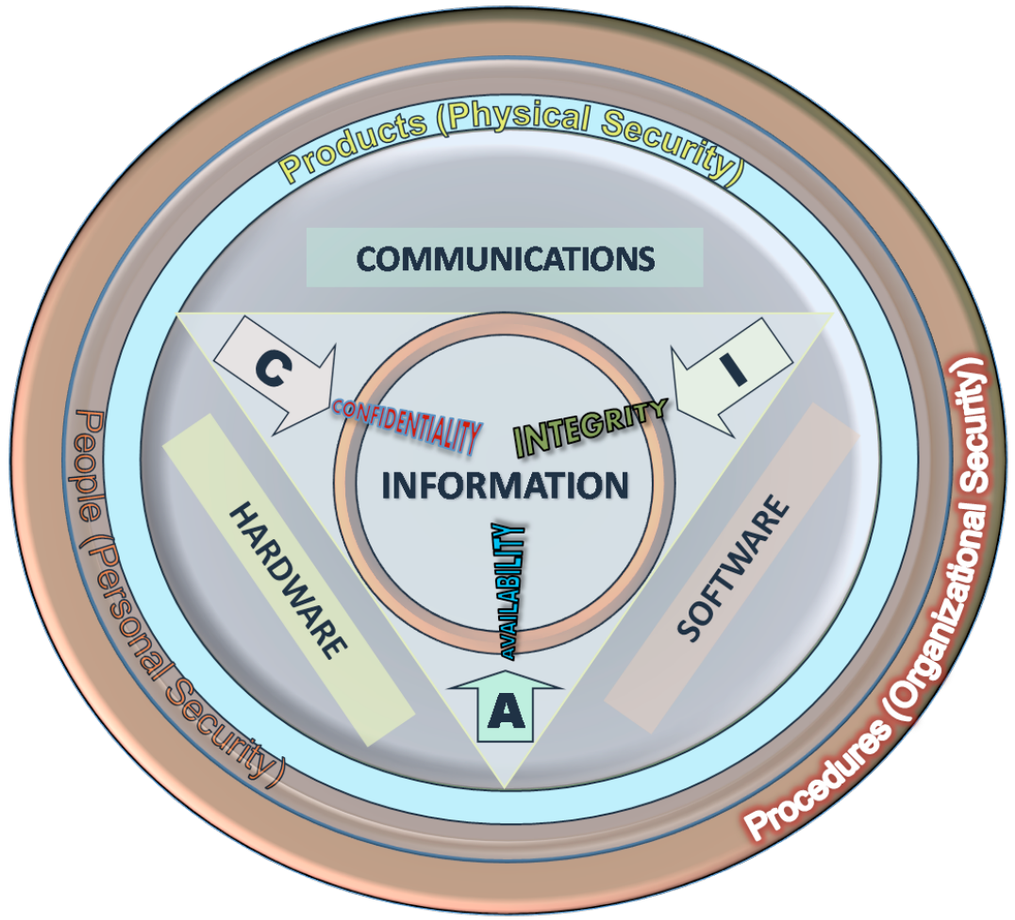
1 km breit, 1.5 cm tief

CISSP Inhalte

- Was ist CISSP?
- Inhalte
- Domains
- Ist CISSP was für mich?
- Resources

Thema

- CIA
- Schutz von Leben und Gesundheit
- C-Level
- Prozesslastig
- Business



8 Domains

Security and Risk Management

Asset Security

Security Architecture & Engineering

Communications & Network Security

Identity & Access Management

Security Assessment & Testing

Security Operations

Software Development Security

1. Security and Risk Management (16%)

- Confidentiality, Integrity and Availability
- Security Governance
- Due Care vs. Due Diligence
- Legal and Regulatory Compliance
- Policies, Standards, Procedures and Guidelines
- Employee, Vendor, Consultant and Contractor Security
- Risk Management
- Threat Modeling

CIA

- Confidentiality, Integrity and Availability

  + non-reputation & authentication

Security and Risk Management

- Security Governance - **support the business**
- Due Care - **responsibility** to customer
  Due Diligence - **activity** to provide or demonstrate due care
- Policies, Standards, Procedures and Guidelines

Risk Management

- Risk Avoidance, Mitigation, Transfer, Acceptance
- Loss expectancy
    - Asse Value (AV)
    - Exposure Factor (% damage)
    - Single Loss Expectancy (SLE = AV * EF)
    - Annual Rate of Occurrence (ARO x/Year)
    - Annual Loss Expectancy (ALE = ARO * SLE)

Control Categories & Types

- Control Types
  - Technical / Logical
  - Physical
  - Administrative

- Control Categories
  - Deterrent
  - **Preventative**
  - Compensating
  - **Detective**
  - **Corrective**
  - Recovery

Threat Modeling

- Spoofing **S**
- Tampering **T**
- Reputation **R**
- Information Disclosure **I**
- Denial of service **D**
- Elevation of privilege **E**

Security and Risk Management - Beispielfrage

Which of the following control categories does not accurately describe a fence around a facility?

A. Physical

B. Detective

C. Deterrent

D. Preventative

Security and Risk Management - Beispielfrage

Which of the following control categories does **not** accurately describe a fine around a facility?

A. Physical

B. Detective

C. Deterrent

D. Preventative

Security and Risk Management - Beispielfrage

Which of the following control categories does **not** accurately describe a fine around a facility?

A. Physical

B. Detective

C. Deterrent

D. Preventive

Security and Risk Management - Beispielfrage

WTF Version

Tim’s organisation recently receive a government contract to conduct research. What law likely apples to the information systems involved in this contract?

A. FISMA

B. PCI DSS

C. HIPAA

D. GISRA

Security and Risk Management - Beispielfrage

WTF Version

Tim’s organisation recently receive a government contract to conduct research. What law likely apples to the information systems involved in this contract?

A. FISMA

B. PCI DSS

C. HIPAA

D. GISRA

2. Asset Security (10%)

- Information and Asset Classification
- Data and System Ownership
- Privacy
- Retention
- Data Security Controls
- Data Handling Requirements
- Public Key Infrastructure (PKI)

Was sind Assets

- People
- Information
- Data
- Hardware
- Processes
- Functions
- Ideas
- Intellectual Property
- Reputation
- Brand
- Identity
- Facilities
- …

Asset Security

- Data Owner & Data custodian
- Classification
  - Public: Sensitive, Confidential, Private, Proprietary, Public
  - Gov: Top secret, secret, confidential, Sensitive but unclassified, unclassified

Controls

- Labeling
- Destruction
- Encryption
- …

Asset Security - Beispielfrage

What protocol is preferred over Telnet for remote server administration via the command line?

A. SCP

B. SFTP

C. WDS

D. SSH

Asset Security - Beispielfrage

What protocol is preferred over Telnet for remote server administration via the command line?

A. SCP

B. SFTP

C. WDS

D. SSH

Asset Security - Beispielfrage

WTF Version

Which mapping correctly matches data classifications between nongovernment and government classification schemes?

A. Top Secret - Confidential/Proprietary; Secret - Private; Confidential - Sensitive

B. Secret - Business Confidential, Classified - Proprietary, Confidential - Business Internal

C. Top secret - Business sensitive, Secret - Business Internal, Confidential - Business Proprietary

D. Secret - Proprietary, Classified - Private, Unclassified - public

Asset Security - Beispielfrage

WTF Version

Which mapping correctly matches data classifications between nongovernment and government classification schemes?

A. Top Secret - Confidential/Proprietary; Secret - Private; Confidential - Sensitive

B. Secret - Business Confidential, Classified - Proprietary, Confidential - Business Internal

C. Top secret - Business sensitive, Secret - Business Internal, Confidential - Business Proprietary

D. Secret - Proprietary, Classified - Private, Unclassified - public

3. Security Architecture and Engineering (12%)

- Secure design
- Security models
- Security evaluation models
- Certification and Accreditation
- Security capabilities
- Vulnerabilities
- Database Security
- Cryptography
- Physical security

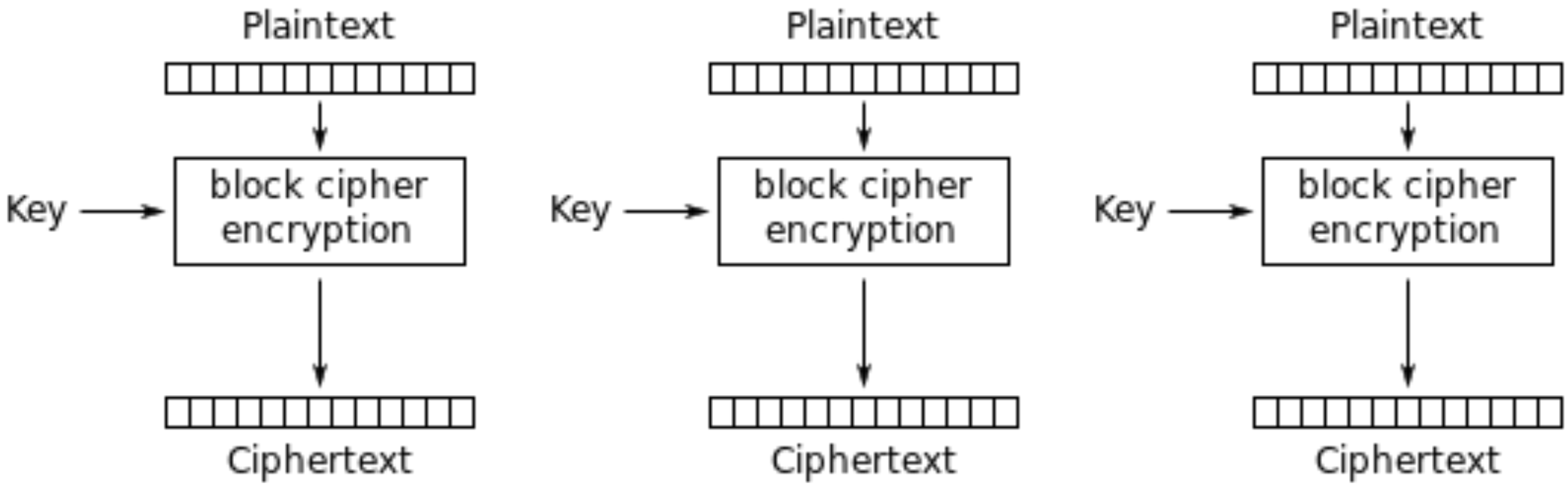
Security Models

- Bell–LaPadula Model (BLP)
  State-machine, **Confidentiality**
  No read up, no write down

- Biba
  State-machine, **Integrity**
  No read down, no write up

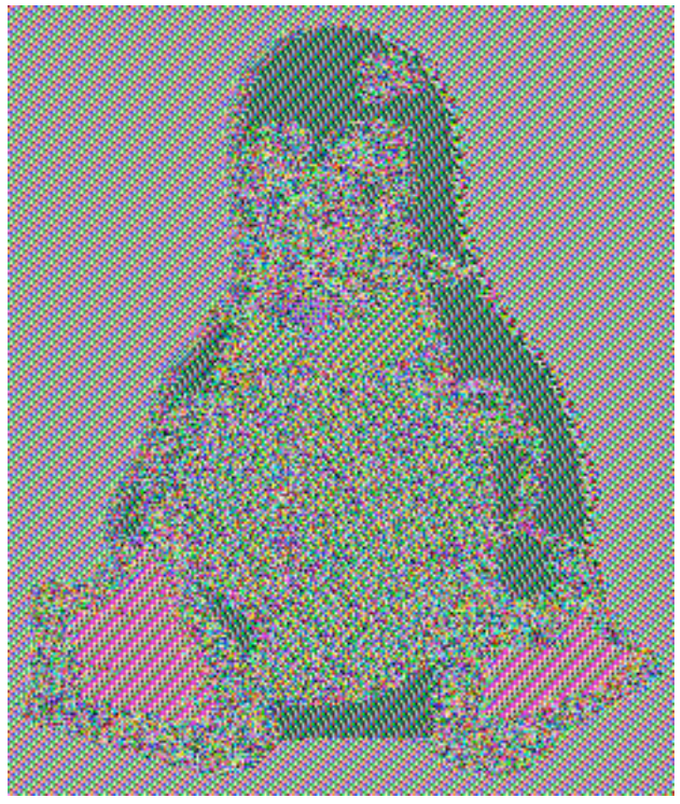
- Brewer and Nash/Chinese Wall
  Information flow model

Beispiel Schwäche ECB

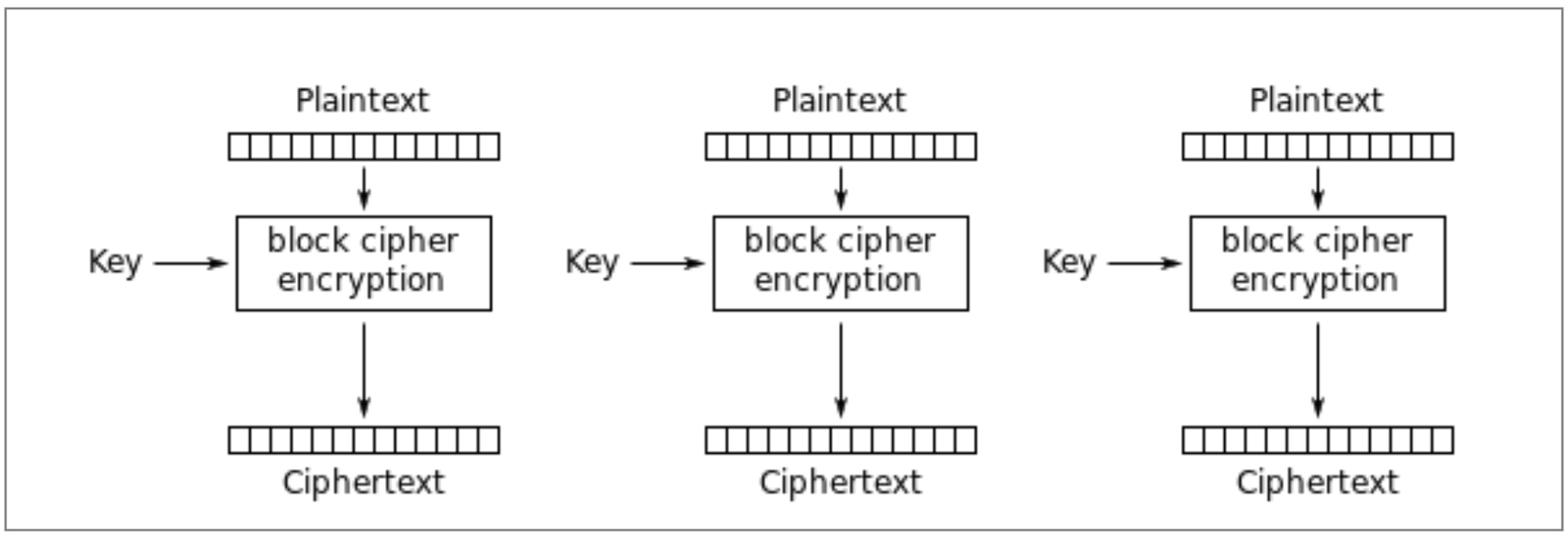


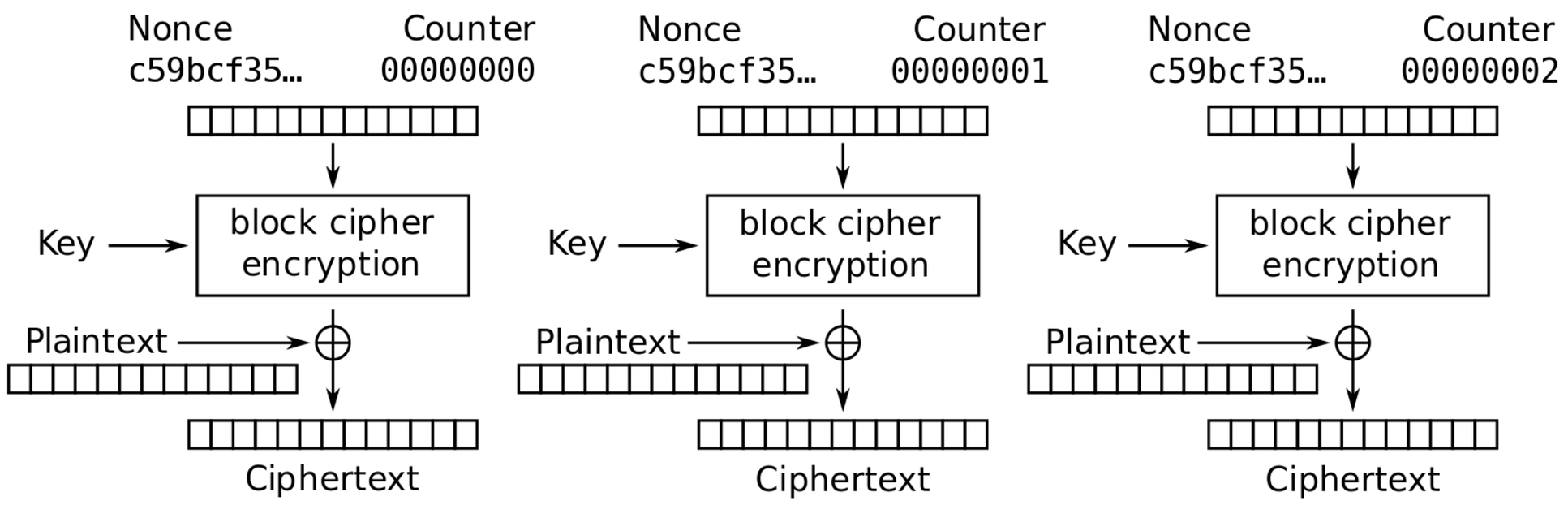
Electronic Codebook (ECB) mode encryption

Beispiel Schwäche ECB



ECB vs CTR





Counter (CTR) mode encryption

Security Architecture and Engineering - Beispielfrage

Harry would like to access a document owned by Sally and stored on a file server. Applying the subject/object model to this scenario, who or what is the subject of the request?

A. Harry

B. Sally

C. Server

D. Document

Security Architecture and Engineering - Beispielfrage

Harry would like to access a document owned by Sally and stored on a file server. Applying the subject/object model to this scenario, who or what is the subject of the request?

A. Harry

B. Sally

C. Server

D. Document

4. Communications & Network Security (12%)

- Secure network architecture
- Secure network components
- Secure communication channels
- Network attacks and countermeasures

Communications & Network Security - Beispielfrage

Chris has been asked to choose between implementing PEAP and LEAP for wireless authentication. What should he choose and why?

A. LEAP, because it fixes problem with TKIP

B. PEAP, because it implements CCMP for security

C. LEAP, because it implements EAP-TLS for end-to-end session encryption

D. PEAP, because it can provide a TLS tunnel the encapsulates EAP methods, protecting the entire session

Communications & Network Security - Beispielfrage

Chris has been asked to choose between implementing PEAP and LEAP for wireless authentication. What should he choose and why?

A. LEAP, because it fixes problem with TKIP

B. PEAP, because it implements CCMP for security

C. LEAP, because it implements EAP-TLS for end-to-end session encryption

D. PEAP, because it can provide a TLS tunnel the encapsulates EAP methods, protecting the entire session

5. Identity & Access Management (13%)

- Access Control Categories
- Identification and Authentication
- Authorization
- Identity as a Service
- Attacks
- Identity and Access Provisioning Lifecycle

Identity & Access Management - Beispielfrage

Place the following steps in the order in which they occur during the Kerberos authentication process

A. Client /server ticket generated

B. TGT generated

C. Client/TGS key generated

D. User accesses service

E. User provides authentication credentials

Identity & Access Management - Beispielfrage

Place the following steps in the order in which they occur during the Kerberos authentication process

A. Client /server ticket generated

B. TGT generated

C. Client/TGS key generated

D. User accesses service

E. User provides authentication credentials

E C B A D

6. Security Assessment & Testing (11%)

- Assessment and test strategies
- Management and operational controls)
- Security control testing
- Security architectures vulnerabilities

Security Assessment & Testing - Beispielfrage

Misconfiguration, logical and functional flaws, and poor programming practices are all causes of what common security issue?

A. Fuzzing

B. Security vulnerabilities

C. Buffer overflows

D. Race conditions

Security Assessment & Testing - Beispielfrage

Misconfiguration, logical and functional flaws, and poor programming practices are all causes of what common security issue?

A. Fuzzing

B. Security vulnerabilities

C. Buffer overflows

D. Race conditions

7. Security Operations (16%)

- Investigations / Forensics
- Logging and monitoring
- Roles, Privileges, information lifecycle
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery
- Business continuity planning
- Physical security
- Personnel safety concerns

Security Operations - Beispielfrage

Garry is preparing to develop controls around access to the root encryptions keys and would like to apply a principle of security designed specifically for very sensitive operations. Which principle should he apply?

A. Least privilege

B. Defense in depth

C. Security through obscurity

D. Two-person control

Security Operations - Beispielfrage

Garry is preparing to develop controls around access to the root encryptions keys and would like to apply a principle of security designed specifically for very sensitive operations. Which principle should he apply?

A. Least privilege

B. Defense in depth

C. Security through obscurity

D. Two-person control

8. Software Development Security (10%)

- Security in the software development lifecycle
- Development environment security controls
- Software development models
- Software security effectiveness
- Acquired software security impact
- Software testing

Software Development Security - Beispielfrage

What approach to technology management integrates the three components of technology management “Software development”, “Quality assurance” and “Operations”?

A. Agile

B. Lean

C. DevOps

D. ITIL

Software Development Security - Beispielfrage

What approach to technology management integrates the three components of technology management “Software development”, “Quality assurance” and “Operations”?

A. Agile

B. Lean

C. DevOps

D. ITIL

Ist es was für mich?

- Was ist CISSP?
- Inhalte
  - Domains
- **Ist CISSP was für mich?**
- Resources

CISSP Cons

Cons

- Teuer
- Breit
- Aufwendig
- Temporär
- C-Level

CISSP Pros

Pros

- Teuer & Temporär
- Breit
- C-Level

Cons

- Teuer
- Breit
- Aufwendig
- Temporär
- C-Level

Ist es was für mich? - Fazit

?

Resources

- Was ist CISSP?
- Inhalte
  - Domains
- Ist es was für mich?
- **Resources**

Resources

- (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide
- Eleventh Hour CISSP, Second Edition: Study Guide
- CISSP Official (ISC)2 Practice Tests
- http://www.mindcert.com/category/mind-maps/cissp/