<table>
<thead>
<tr>
<th>Privates IT-Weiterbildungszertifikat</th>
<th>Erlernter Kompetenzlevel nach EQF-Kategorien und EQF-Stufen</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1: The Process of Auditing Information Systems (S. 19)</strong></td>
<td></td>
</tr>
<tr>
<td>1.2 Management of the IS Audit Function (S. 29)</td>
<td></td>
</tr>
<tr>
<td>1.2.1 Organization of the IS Audit Function</td>
<td><strong>EQF-Kategorien</strong></td>
</tr>
<tr>
<td>1.2.2 IS Audit Resource Management</td>
<td>Kenntnisse</td>
</tr>
<tr>
<td>1.2.3 Audit Planning</td>
<td>Fertigkeiten</td>
</tr>
<tr>
<td>Annual Planning</td>
<td>Kompetenz</td>
</tr>
<tr>
<td>Individual Audit Assignments</td>
<td></td>
</tr>
<tr>
<td>1.2.4 Effect of Laws and Regulations on IS Audit Planning</td>
<td></td>
</tr>
<tr>
<td><strong>1.3 ISACA IT Audit and Assurance Standards and Guidelines (S. 31)</strong></td>
<td></td>
</tr>
<tr>
<td>1.3.1 ISACA Code of Professional Ethics</td>
<td></td>
</tr>
<tr>
<td>1.3.2 ISACA IT Audit and Assurance Standards Framework</td>
<td></td>
</tr>
<tr>
<td>Auditing Standards</td>
<td></td>
</tr>
<tr>
<td>1.3.3 ISACA IT Audit and Assurance Guidelines</td>
<td></td>
</tr>
<tr>
<td>Index of IT Audit and Assurance Tools and Techniques</td>
<td></td>
</tr>
<tr>
<td>1.3.4 ISACA IT Audit and Assurance Tools and Techniques</td>
<td></td>
</tr>
<tr>
<td>Index of IT Audit and Assurance Tools and Techniques</td>
<td></td>
</tr>
<tr>
<td>1.3.5 Relationship Among Standards, Guidelines, and Tools and Techniques</td>
<td></td>
</tr>
<tr>
<td>1.3.6 Information Technology Assurance Framework™ (ITAF™)</td>
<td></td>
</tr>
<tr>
<td>Selection 2200 - General Standards</td>
<td>Kenntnisse</td>
</tr>
<tr>
<td>Selection 2400 - Performance Standards</td>
<td>Fertigkeiten</td>
</tr>
<tr>
<td>Selection 2600 - Reporting Standards</td>
<td>Kompetenz</td>
</tr>
<tr>
<td>Selection 3000 - IT Assurance Guidelines</td>
<td></td>
</tr>
<tr>
<td>Selection 3200 - Enterprise Topics</td>
<td></td>
</tr>
<tr>
<td>Selection 3400 - IT Management Processes</td>
<td></td>
</tr>
<tr>
<td>Selection 3600 - IT Audit and Assurance Processes</td>
<td></td>
</tr>
<tr>
<td>Selection 3800 - IT Audit and Assurance Management</td>
<td></td>
</tr>
<tr>
<td><strong>1.4 Risk Analysis (S. 43)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kenntnisse</td>
</tr>
<tr>
<td></td>
<td>Fertigkeiten</td>
</tr>
<tr>
<td></td>
<td>Kompetenz</td>
</tr>
<tr>
<td>Chapter 2: Governance and Management of IT (S. 69)</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>2.1 Quick Reference (S. 82)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>2.2 Corporate Governance (S. 83)</strong></td>
<td></td>
</tr>
<tr>
<td>2.3 IT-Governance (S. 83)</td>
<td>2.4 Information Systems Strategy (S. 90)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>2.3.1 Best Practices for IT Governance</td>
<td>2.4.1 Strategic Planning</td>
</tr>
<tr>
<td>IT Governance and Management Frameworks</td>
<td>2.4.2 Steering Committee</td>
</tr>
<tr>
<td>Audit Role in IT Governance</td>
<td></td>
</tr>
<tr>
<td>2.3.2 IT Governance Committees</td>
<td></td>
</tr>
<tr>
<td>2.3.3 IT Balanced Scorecard</td>
<td></td>
</tr>
<tr>
<td>2.3.4 Information Security Governance</td>
<td></td>
</tr>
<tr>
<td>Effective Information Security Governance</td>
<td></td>
</tr>
<tr>
<td>2.3.5 Enterprise Architecture</td>
<td></td>
</tr>
</tbody>
</table>

| Kenntnisse | Fertigkeiten | Kompetenz | Kenntnisse | Fertigkeiten | Kompetenz |

2.3.6 IT Investment and Allocation Practices (S. 91) Value of IT Implementing IT Portfolio Management IT Portfolio Management vs. Balanced Scorecard

2.7.1 Policies Information Security Policy

2.7.2 Procedures

2.8.1 Developing a Risk Management Program

2.8.2 Risk Management Process

2.8.3 Risk Analysis Methods Qualitative Analysis Methods Semiquantitative Analysis Methods Quantitative Analysis Methods
### 2.9 Information Systems Management Practices (S. 97)

#### 2.9.1 Human Resource Management
- Hiring
- Employee Handbook
- Promotion Policies
- Training
- Scheduling and Time Reporting
- Employee Performance Evaluations
- Required Vacations
- Termination Policies

#### 2.9.2 Sourcing Practices
- Outsourcing Practices and Strategies
- Industry Standards/Benchmarking
- Globalization Practices and Strategies
- Cloud Computing
- Outsourcing and Third-party Audit Reports
- Governance in Outsourcing
- Capacity and Growth Planning
- Third-party Service Delivery Management
- Service Improvement and User Satisfaction

#### 2.9.3 Organizational Change Management

#### 2.9.4 Financial Management Practices
- IT Budgets
- Software Development

#### 2.9.5 Quality Management

#### 2.9.6 Information Security Management

#### 2.9.7 Performance Optimization

---

### 2.10 IS Organizational Structure and Responsibilities (S. 107)

#### 2.10.1 IS Roles and Responsibilities
- Vendor and Outsourcer Management
- Infrastructure Operations and Maintenance
- Data Entry
- Systems Administrations
- Security Administrations
- Quality Assurance
- Database Administration
- System Analyst
- System Architect
- Applications Development and Maintenance
- Infrastructure Development and Maintenance
- Network Management

#### 2.10.2 Segregations of Duties Within IS

#### 2.10.3 Segregations of Duties Controls
- Transaction Authorization
- Custody of Assets
- Access to Data
- Compensating Controls for Lack of Segregation of Duties

---

### 2.11 Auditing IT Governance Structure and Implementation (S. 113)

#### 2.11.1 Reviewing Documentation
#### 2.11.2 Reviewing Contractual Commitments
### 2.12 Business Continuity Planning (S. 114)

- **2.12.1** IS Business Continuity Planning
- **2.12.2** Disasters or Other Disruptive Events
  - Pandemic Planning
  - Dealing With Damage to Image, Reputation or Brand
- **2.12.3** Business Continuity Planning Process
- **2.12.4** Business Continuity Policy
- **2.12.5** Business Continuity Planning Incident Management
- **2.12.6** Business Impact Analysis
  - Classification of Operations and Criticality Analysis
- **2.12.7** Development of Business Continuity Plans
- **2.12.8** Other Issues in Plan Development
- **2.12.9** Components of a Business Continuity Plan
  - Key Decision-making Personnel
  - Backup of Required Supplies
  - Insurance
- **2.12.10** Plan Testing
  - Specification
  - Test Execution
  - Documentation of Results
  - Results Analysis
  - Plan Maintenance
- **2.12.11** Summary of Business Continuity

### 2.13 Auditing Business Continuity (S. 125)

- **2.13.1** Reviewing the Business Continuity Plan
  - Reviewing the Document
  - Review the Applications Covered by the Plan
  - Review the Business Continuity Plan
  - Plan Testing
- **2.13.2** Evaluation of Prior Test Results
- **2.13.3** Evaluation of Offline Storage
- **2.13.4** Interviewing Key Personnel
- **2.13.5** Evaluation of Security at Offline Facility
- **2.13.6** Reviewing Alternative Processing Contract
- **2.13.7** Reviewing Insurance Coverage

---

**Chapter 3: Information Systems Acquisition, Development and Implementation (S. 131)**

### 3.1 Quick References (S. 143)

### 3.2 Benefits Realization (S. 143)

- **3.2.1** Portfolio/Program Management
- **3.2.2** Business Case Development and Approval
- **3.2.3** Benefits Realization Techniques

### 3.3 Project Management Structure (S. 145)

- **3.3.1** General Aspects
- **3.3.2** Project Context and Environment
- **3.3.3** Project Organizational Forms
- **3.3.4** Project Communication and Culture
- **3.3.5** Project Objectives
- **3.3.6** Roles and Responsibilities of Groups and Individuals
<table>
<thead>
<tr>
<th>3.4 Project Management Practices (S. 149)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.1 Initiation of a Project</td>
</tr>
<tr>
<td>3.4.2 Project Planning</td>
</tr>
<tr>
<td>- Software Size Estimation</td>
</tr>
<tr>
<td>- Function Point Analysis</td>
</tr>
<tr>
<td>- FPA Feature Points</td>
</tr>
<tr>
<td>- Cost Budgets</td>
</tr>
<tr>
<td>- Software Cost Estimation</td>
</tr>
<tr>
<td>- Scheduling and Establishing the Time Frame</td>
</tr>
<tr>
<td>- Critical Path Methodology</td>
</tr>
<tr>
<td>- Gantt Charts</td>
</tr>
<tr>
<td>- Program Evaluation Review Technique</td>
</tr>
<tr>
<td>- Timebox Management</td>
</tr>
<tr>
<td>3.4.3 Project Controlling</td>
</tr>
<tr>
<td>- Management of Scope Changes</td>
</tr>
<tr>
<td>- Management of Resource Usage</td>
</tr>
<tr>
<td>- Management of Risk</td>
</tr>
<tr>
<td>3.4.4 Closing a Project</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.5 Business Application Development (S. 155)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.1 Traditional SDLC Approach</td>
</tr>
<tr>
<td>3.5.2 Description of Traditional SDLC Phases</td>
</tr>
<tr>
<td>- Phase 1: Feasibility Study</td>
</tr>
<tr>
<td>- Phase 2: Requirements Definition</td>
</tr>
<tr>
<td>- Phase 3A: Software Selection and Acquisition</td>
</tr>
<tr>
<td>- Phase 3B: Design</td>
</tr>
<tr>
<td>- Phase 4A: Development</td>
</tr>
<tr>
<td>- Phase 4B: Configuration</td>
</tr>
<tr>
<td>- Phase 5: Final Testing and Implementation</td>
</tr>
<tr>
<td>- Phase 6: Postimplementation Review</td>
</tr>
<tr>
<td>3.5.3 Integrated Resource Management Systems</td>
</tr>
<tr>
<td>3.5.4 Risk Associated With Software Development</td>
</tr>
</tbody>
</table>
3.6 Business Application Systems (S. 172)

3.6.1 Electronic Commerce
- E-commerce Models
- E-commerce Architecture
- E-commerce Risks
- E-commerce Requirements
- E-commerce Audit and Control Issues (Best Practices)

3.6.2 Electronic Data Interchange
- General Requirements
- Traditional EDI
- Web-based EDI

3.6.3 EDI Risks and Controls
- Controls in EDI Environment
- Receipt of Inbound Transactions
- Outbound Transactions
- Auditing EDI

3.6.4 Electronic Mail
- Security Issues of Email
- Standards for Email Security

3.6.5 Electronic Banking
- Risk Management Challenges in E-banking
- Risk Management Controls for E-banking

3.6.6 Electronic Finance
- Electronic Money Model
- Electronic Checks Model
- Electronic Transfer Model

3.6.7 Electronic Payment Systems
- Traditional EDI
- Web-based EDI

3.6.8 E-commerce Models
- E-commerce Architecture
- E-commerce Risks
- E-commerce Requirements
- E-commerce Audit and Control Issues (Best Practices)

3.6.9 E-commerce Architecture
- E-commerce Risks
- E-commerce Requirements
- E-commerce Audit and Control Issues (Best Practices)

3.6.10 E-commerce Risks and Controls
- Controls in E-commerce Environment
- Receipt of Inbound Transactions
- Outbound Transactions
- Auditing EDI

3.6.11 E-commerce Audit and Control Issues (Best Practices)
- Traditional EDI
- Web-based EDI

3.6.12 Electronic Funds Transfer
- Controls in an EFT Environment
- Audit of ATM

3.6.13 Electronic Voice Response
- Interactive Voice Response

3.6.14 Electronic Accounting System
- Purchase Accounting System

3.6.15 Image Processing
- Electronic Data Interchange

3.6.16 Artificial Intelligence and Export Systems
- Business Intelligence
- Business Intelligence Governance

3.6.17 Decision Support Systems
- Efficiency vs. Effectiveness
- Decision Focus
- DSS Frameworks
- Design and Development
- Implementation and Use
- Risk Factors
- Implementation Strategies
- Assessment and Evaluation
- DSS Common Characteristics
- DSS Trends

3.6.18 Customer Relationship Management

3.6.19 Supply Chain Management

3.6.20 Electronic Banking
- Risk Management Challenges in E-banking
- Risk Management Controls for E-banking

3.7 Development Methods (S. 190)

3.7.1 Use of Structured Analysis, Design and Development Techniques
- Agile Development
- Prototyping-evolutionary Development
- Rapid Application Development
- Object-oriented System Development
- Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.2 Agile Development
- Prototyping-evolutionary Development
- Rapid Application Development
- Object-oriented System Development
- Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.3 Prototyping-evolutionary Development
- Rapid Application Development
- Object-oriented System Development
- Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.4 Rapid Application Development
- Object-oriented System Development
- Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.5 Object-oriented System Development
- Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.6 Component-based Development
- Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.7 Web-based Application Development
- Software Reengineering
- Revere Engineering

3.7.8 Software Reengineering
- Revere Engineering

3.7.9 Revere Engineering
### 3.8 Infrastruktur Entwicklung/Aquisition Practices (S. 195)

- **3.8.1 Project Phases of Physical Architecture Analysis**
  - Review of Existing Architecture
  - Analysis and Design
  - Draft Functional Requirements
  - Vendor and Product Selection
  - Writing Functional Requirements
  - Proof of Concept

- **3.8.2 Planning Implementation of Infrastructure**
  - Procurement Phase
  - Delivery Time
  - Installation Plan
  - Installation Test Plan

- **3.8.3 Critical Success Factors**

- **3.8.4 Hardware Acquisition**
  - Acquisition Steps

- **3.8.5 System Software Acquisition**

- **3.8.6 System Software Implementation**

---

### 3.9 Information Systems Maintenance Practices (S. 201)

- **3.9.1 Change Management Process Overview**
  - Deploying Changes
  - Documentation
  - Testing Changed Programs
  - Auditing Program Changes
  - Emergency Changes
  - Deploying Changes Back Into Production
  - Change Exposures (Unauthorized Changes)

- **3.9.2 Configuration Management**

### 3.10 System Development Tools and Productivity Aids (S. 205)

- **3.10.1 Code Generators**

- **3.10.2 Computer-aided Software Engineering**

- **3.10.3 Fourth-generation Languages**

---

### 3.11 Process Improvement Practices (S. 207)

- **3.11.1 Business Process Reengineering and Process Change Projects**
  - BPR Methods and Techniques

- **3.11.2 ISO 9126**

- **3.11.3 Capability Maturity Model Integration**

- **3.11.4 ISO/IEC 15504**

---

### 3.12 Application Controls (S. 210)

- **3.12.1 Input/Origination Controls**
  - Input Authorization
  - Batch Controls and Balancing
  - Error Reporting and Handling

- **3.12.2 Processing Procedures and Controls**
  - Data Validation and Editing Procedures
  - Processing Controls
  - Data File Control Procedures

- **3.12.3 Output Controls**

- **3.12.4 Business Process Control Assurance**
## 3.13 Auditing Application Controls (S. 215)
- 3.13.1 Flow of Transactions Through the System
- 3.13.2 Risk Assessment Model to Analyze Application Controls
- 3.13.3 Observing and Testing User Performing Procedures
- 3.13.4 Data Integrity Testing
- 3.13.5 Data Integrity in Online Transactions Processing Systems
- 3.13.6 Test Application Systems
- 3.13.7 Continuous Online Auditing
- 3.13.8 Online Auditing Techniques

## 3.14 Auditing Systems Development, Acquisition And Maintenance (S. 217)
- 3.14.1 Project Management
- 3.14.2 Feasibility Study
- 3.14.3 Requirement Definition
- 3.14.4 Software Acquisition Process
- 3.14.5 Detailed Design and Development
- 3.14.6 Testing
- 3.14.7 Implementation Phase
- 3.14.8 Postimplementation Review
- 3.14.9 System Change Procedures and the Program Migration Process

### Chapter 4: Information Systems Operations, Maintenance and Support (S. 225)

## 4.1 Quick References (S. 236)

## 4.2 Information Systems Operations (S. 237)
- 4.2.1 Management of IS Operations
  - Control Functions
- 4.2.2 IT Service Management
  - Service Level
- 4.2.3 Infrastructure Operations
  - Job Scheduling
- 4.2.4 Incident and Problem Management
  - Process on Incident Handling
  - Problem Management
  - Detection, Documention, Control, Resolution and Reporting of Abnormal Conditions
- 4.2.5 Support/Help Desk
- 4.2.6 Change Management Process
- 4.2.7 Release Management
- 4.2.8 Quality Assurance
- 4.2.9 Information Security Management
- 4.2.10 Media Sanitization

## 4.3 Information Systems Hardware (S. 243)
- 4.3.1 Computer Hardware Components and Architectures
  - Processing Components
  - Input/Output Components
  - Types of Computers
  - Common Enterprise Back-end Devices
  - Universal Serial Bus
  - Memory Cards/Flash Drives
  - Radio Frequency Identification
- 4.3.2 Hardware Maintenance Program
- 4.3.3 Hardware Monitoring Procedures
- 4.3.4 Capacity Management

---

**EQF-Kategorien** | **EQF-Stufe**
---|---
Kenntnisse | Fertigkeiten | Kompetenz

---
| 38 | 4.4 IS Architecture and Software (S. 248) |
|  | 4.4.1 Operating Systems |
|  | Software Control Features or Parameters |
|  | Software Integrity Issues |
|  | Activity Logging and Reporting Options |
|  | 4.4.2 Access Control Software |
|  | 4.4.3 Data Communications Software |
|  | 4.4.4 Data Management |
|  | File Organization |
|  | 4.4.5 Database Management System |
|  | DBMS Architecture |
|  | Detailed DBMS Metadata Architecture |
|  | Data Dictionary/Directory System |
|  | Database Structure |
|  | Database Controls |
|  | 4.4.6 Tape and Disk Management Systems |
|  | 4.4.7 Utility Programs |
|  | 4.4.8 Software Licensing Issues |
|  | 4.4.9 Digital Rights Management |

| 39 | 4.5 IS Network Infrastructure (S. 255) |
|  | 4.5.1 Enterprise Network Architectures |
|  | 4.5.2 Types of Networks |
|  | 4.5.3 Network Services |
|  | 4.5.4 Network Standards and Protocols |
|  | 4.5.5 OSI Architecture |
|  | 4.5.6 Application of the OSI Model in Network Architecture |
|  | Local Area Network |
|  | Wide Area Network |
|  | Wireless Networks |
|  | Public "Global" Internet Infrastructure |
|  | Network Administration and Control |
|  | Applications in a Networked Environment |
|  | On-demand Computing |

| 40 | 4.6 Auditing Infrastructure and Operations (S. 275) |
|  | 4.6.1 Hardware Reviews |
|  | 4.6.2 Operating System Reviews |
|  | 4.6.3 Database Reviews |
|  | 4.6.4 Network Infrastructure and Implementation Reviews |
|  | 4.6.5 IS Operations Reviews |
|  | 4.6.6 Scheduling Reviews |
|  | 4.6.7 Problem Management Reporting Reviews |
4.7 Disaster Recovery Planning (S. 282)
4.7.1 Recovery Point Objective and Recovery Time Objective
4.7.2 Recovery Strategies
4.7.3 Recovery Alternatives
  Contractual Provisions
  Procuring Alternative Hardware
  Application Disaster Recovery Methods
  Data Storage Disaster Recovery Methods
4.7.4 Development of Disaster Recovery Plans
  IT DRP Contents
  IT DRP Scenarios
  Recovery Procedures
4.7.5 Organization and Assignment of Responsibilities
4.7.6 Backup and Restoration
  Offsite Library Controls
  Security and Control of Offsite Facilities
  Media and Documentation Backup
  Types of Backup Devices and Media
  Periodic Backup Procedures
  Frequency of Rotation
  Types of Media and Documentation Rotated
  Backup Schemes
  Method of Rotation
  Record Keeping for Offsite Storage

Chapter 5: Protection of Information Assets (S. 295)

5.1 Quick References (S. 308)

5.2 Importance of Information Security Management (S. 308)
5.2.1 Key Element of Information Security Management
  Information Security Management System
5.2.2 Information Security Management Roles and Responsibilities
5.2.3 Inventory and Classification of Information Assets
5.2.4 System Access Permission
5.2.5 Mandatory and Discretionary Access Controls
5.2.6 Privacy Management Issues and the Role of IS Auditors
5.2.7 Critical Success Factors to Information Security Management
5.2.8 Information Security and External Parties
  Identification of Risks Related to External Parties
  Addressing Security When Dealing With Customers
  Addressing Security in Third-party Agreements
5.2.9 Human Resources Security and Third Parties
  Screening
  Terms and Conditions of Employment
  During Employment
  Termination or Change of Employment
  Removal of Access Rights
5.2.10 Computer Crime Issues and Exposure
  Peer-to-peer Computing, Instant Messaging, Data Leakage and
  Web-based Technologies (e.g., Social Networking, Message Boards, Blogs)
5.2.11 Security Incident Handling and Response
5.3 Logical Access (S. 324)
5.3.1 Logical Access Exposures
5.3.2 Familiarization With the Enterprise's IT Environment
5.3.3 Paths of Logical Access
   General Points of Entry
5.3.4 Logical Access Control Software
5.3.5 Identification and Authentication
   Logon IDs and Passwords
   Token Devices, One-time Passwords
   Biometrics
   Single Sign-on
5.3.6 Authorization Issues
   Access Control Lists
   Logical Access Security Administration
   Remote Access Security
   Remote Access Using Handheld Devices
   Access Issues With Mobile Technology
   Audit Logging in Monitoring System Access
   Naming Conventions for Logical Access Controls
5.3.7 Storing, Retrieving, Transporting and Disposing of Confidential Information
   Preserving Information During Shipment or Storage
   Media-specific Storage Precautions
5.4 Network Infrastructure Security (S. 335)

5.4.1 LAN Security
- LAN Risks and Issues
- Virtualization

5.4.2 Client-server Security
- Client-server Risks and Issues

5.4.3 Wireless Security Threats and Risk Mitigation

5.4.4 Internet Threats and Security
- Network Security Threats
  - Passive Attacks
  - Active Attacks
  - Causal Factors for Internet Attack
- Internet Security Controls
  - Firewall Security Systems
  - Firewall General Features
  - Firewall Types
  - Examples of Firewall Implementations
  - Firewall Issues
  - Firewall Platforms
  - Intrusion Detection Systems
  - Intrusion Prevention Systems
  - Honeypots and Honeynets

5.4.5 Encryption
- Key Elements of Encryption Systems
- Symmetric Key Cryptographic Systems
- Public (Asymmetric) Key Cryptographic Systems
- Elliptical Curve Cryptography
- Quantum Cryptography
- Advanced Encryption Standard
- Digital Signatures
- Digital Envelope
- Public Key Infrastructure
- Applications of Cryptographic Systems
- Encryption Risks and Password Protection

5.4.6 Viruses
- Virus and Worm Controls
- Management Procedural Controls
- Technical Controls
- Antivirus Software Implementation Strategies

5.4.7 Voice-over IP
- VoIP Security Issues

5.4.8 Private Branch Exchange
- PBX Risks
- PBX Audit
- PBX System Features
- PBX System Attacks
- Hardware Wiretapping
- Hardware Conferencing
- Remote Access
- Maintenance
- Special Manufacturer's Features
- Manufacturer's Development and Test Features
- Software Loading and Update Tampering
- Crash-restat Attacks
- Passwords
5.5 Auditing Information Security Management Framework (S. 358)

5.5.1 Auditing Information Security Management Framework
-Reviewing Written Policies, Procedures and Standards
-Logical Access Security Policies
-Formal Security Awareness and Training
-Data Ownership
-Date Owners
-Data Custodians
-Security Administrator
-New IT Users
-Data Users
-Documented Authorizations
-Terminated Employee Access
-Security Baselines
-Access Standards

5.5.2 Auditing Logical Access
-Familiarization With the IT Environment
-Assessing and Documenting the Access Paths
-Interviewing Systems Personnel
-Reviewing Reports From Access Control Software
-Reviewing Application Systems Operations Manual

5.5.3 Techniques for Testing Security
-Terminal Cards und Keys
-Terminal Identification
-Logon IDs and Passwords
-Controls Over Production Resources
-Logging and Reporting of Computer Access Violations
-Follow-up Access Violations
-Bypassing Security and Compensating Controls
-Review Access Controls and Passwords Administration

5.5.4 Investigation Techniques
-Investigation of Computer Crime
-Computer Forensics
-Protection of Evidence and Chain of Custody

5.6 Auditing Network Infrastructure Security (S. 365)

5.6.1 Auditing Remote Access
-Auditing Internet Points of Presence
-Network Penetration Tests
-Full Network Assessment Reviews
-Development and Authorization of Network Changes
-Unauthorized Changes
### 5.7 Environmental Exposures and Controls (S. 369)

5.7.1 Environmental Issues and Exposures
- Alarm Control Panels
- Water Detectors
- Handheld Fire Extinguishers
- Manual Fire Alarms
- Fire Suppression Systems
- Strategically Locating the Computer Room
- Regular Inspection by Fire Department
- Fireproof Walls, Floors and Ceiling of the Computer Room
- Electrical Surge Protectors
- Uninterruptible Power Supply/Generator
- Emergency Power-off Switch
- Power Leads From Two Substations
- Wiring Placed in Electrical Panels and Conduit
- Inhibited Activities Within the IPF
- Fire-resistant Office Materials

5.7.2 Controls for Environmental Exposures
- Documented and Tested Emergency Evacuation Plans

5.7.3 Auditing Environmental Controls
- Water and Smoke Detectors
- Handheld Fire Extinguishers
- Fire Suppression Systems
- Regular Inspection by Fire Department
- Fireproof Walls, Floors and Ceilings of the Computer Room
- Electrical Surge Protectors
- Power Leads From Two Substations
- Fully Documented and Tested Business Continuity Plan
- Wiring Placed in Electrical Panels and Conduit
- UPS/Generator
- Documented and Tested Emergency Evacuation Plans
- Humidity/Temperature Control

---

### 5.8 Physical Access Exposures and Controls (S. 373)

5.8.1 Physical Access Issues and Exposures
- Physical Access Exposures
- Possible Perpetrators

5.8.2 Physical Access Controls

5.8.3 Auditing Physical Access

---

### 5.9 Mobile Computing (S. 375)