ISACA®

Trust in, and value from, information systems

2016 CISA® Review Course

Introduction
Agenda

This introduction will address:

- The CISA Certification
- Course format
- Examination format
- Introduction of Attendees

CISA

Certified Information Systems Auditor

- Designed for personnel that will audit and review information systems
- Assurance that systems are designed, developed, implemented and maintained to support business needs and objectives
- Tough but very good quality examination
- Requires understanding of the concepts behind information systems audit - not just the definitions
CISA Exam Review Course Overview

- The CISA Exam is based on the CISA job practice
- The ISACA CISA Certification Committee oversees the development of the exam and ensures the currency of its content
- There are five content areas that the CISA candidate is expected to know

CISA Job Practice Areas

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets
CISA Qualifications

To earn the CISA designation, information security professionals are required to:

- Successfully pass the CISA exam
- Submit an Application for CISA certification
- Minimum of five years information systems auditing, control or security work experience (waivers for education)
- Adhere to the ISACA Code of Professional Ethics
- Adherence to the CISA continuing education policy
- Compliance with Information Systems Auditing Standards

Daily Format

- Lecture and Sample questions
- Approximately two domains per day
  - Domain structure
  - Learning Objectives
  - Content
  - Sample Questions

Please note that the information in every domain overlaps with the information in other domains - during the course we will introduce topics that are expanded upon in later domains.
The Examination

Description of the Exam

- The exam consists of 200 multiple choice questions that cover the CISA job practice areas.
- Four hours are allotted for completing the exam.
- See the Candidate Guide 2016 included in the course booklet for further details.
Examination Job Practice Areas

The exam items are based on the content within 5 information systems audit areas:

- Process of Auditing Information Systems - 21%
- Governance and Management of IT - 16%
- Information Systems Acquisition, Development and Implementation - 18%
- Information Systems Operations, Maintenance and Support - 20%
- Protection of Information Assets - 25%

Exam Day

- Be on time!!
  - The doors are locked when the instructions start - approximately 30 minutes before examination start time.
  - Bring the admission ticket (sent out prior to the examination from ISACA) and an acceptable form of original photo identification (passport, photo id or drivers license).
Completing the Examination Items

- Bring several #2 pencils and an eraser
- Read each question carefully
- Read ALL answers prior to selecting the BEST answer
- Mark the appropriate answer on the test answer sheet
- When correcting an answer be sure to thoroughly erase the wrong answer before filling in a new one.
- There is no penalty for guessing. Answer every question

Grading the Exam

- Candidate scores are reported as a scaled score based on the conversion of a candidate’s raw score on an exam to a common scale
- ISACA uses and reports scores on a common scale from 200 to 800. A candidate must receive a score of 450 or higher to pass
- Exam results will be mailed (and emailed) out approximately 8 weeks after the exam date
- Good Luck!
Introduction of Classmates

End of Introduction
ISACA®
Trust in, and value from, information systems

2016 CISA® Review Course

The Process of Auditing Information Systems
Exam Relevance

- Ensure that the CISA candidate...
- Has the knowledge necessary to provide audit services in accordance with IT audit standards to assist the organisation with protecting and controlling information systems
- The content area in this chapter will represent approximately 21% of the CISA examination

(approximately 32 questions)

Agenda

- Definition and Planning of Audit
- Risk Management
- Audit Planning
- Performing the Audit
- Audit, Analysis and Reporting
- Conclusion
Chapter 1 Learning Objectives

- Develop and implement a risk-based IT audit strategy based on IT audit standards
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organisation
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives

Learning Objectives (continued)

- Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary
- Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner
Audit Charter

- Audit begins with the acceptance of an Audit Charter
- Provides:
  - Authority for audit
  - Responsibility
  - Reporting requirements
- Signed by Audit Committee or Senior Management

Definition of Auditing

- Definition of auditing
  - Systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards.
Definition of Information Systems Auditing

- Definition of IS auditing
  - Any audit that encompasses review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes and the interfaces between them.

Audit Objectives

- An audit compares (measures) actual activity against standards and policy
- Specific goals of the audit
  - Confidentiality
  - Integrity
  - Reliability
  - Availability
  - Compliance with legal and regulatory requirements
Audit Planning

- Involves short and long term planning (annual basis)
  - New control issues.
  - Changes / Upgrades to technologies.
  - Business process / Need / Goals.
  - Auditing / Evaluation Techniques.

Audit Planning (continued)

- Based on concerns of management or areas of higher risk
  - Process failures
  - Financial operations
  - Compliance requirements
Audit Program Challenges

- Limited number of IS auditors
- Maintenance of their technical competence
- Assignment of audit staff

Types of Audits

- Financial audits
- Operational audits
- Integrated audits
- Administrative audits
- IS audits
- Specialised audits
- Forensic audits
Elements of an Audit

- Audit scope
- Audit objectives
- Audit criteria
- Audit procedures
- Evidence
- Conclusions and opinions
- Reporting

Creating the Plan for an Audit

1. Gather Information
2. Identify System and Components
3. Assess Risk
4. Perform Risk Analysis
5. Conduct Internal Control Review
6. Set Audit Scope and Objectives
7. Develop Auditing Strategy
8. Assign Resources
Planning the Audit

- Based on the scope and objective of the particular assignment
- IS auditor’s concerns:
  - Security (confidentiality, integrity and availability)
  - Quality (effectiveness, efficiency)
  - Fiduciary (compliance, reliability)
  - Service and capacity

Audit Methodology

- A set of documented audit procedures designed to achieve planned audit objectives
- Composed of:
  - Statement of scope
  - Statement of audit objectives
  - Statement of audit programs
- Set up and approved by the audit management
- Communicated to all audit staff
Phases of an Audit

- Audit subject
- Audit objective
- Audit scope
- Pre-audit planning
- Audit procedures and steps for data gathering
- Procedures for evaluating the test or review results
- Procedures for communication with management
- Audit report preparation

Audit Work papers

- Audit plans
- Audit programs
- Audit activities
- Audit tests
- Audit findings and incidents
Audit Procedures

- Understanding of the audit area/subject
- Risk assessment and general audit plan
- Detailed audit planning
- Preliminary review of audit area/subject
- Evaluating audit area/subject
- Verifying and evaluating controls
- Compliance testing
- Substantive testing
- Reporting (communicating results)
- Follow-up

Types of Tests for IS Controls

- Use of audit software to survey the contents of data files
- Assess the contents of operating system parameter files
- Flow-charting techniques for documenting automated applications and business process
- Use of audit reports available in operation systems
- Documentation review
- Observation
Forensic Audits

- Audits specifically related to a crime or serious incident
  - Determine
  - Scope of incident
  - Root cause
  - Personnel and systems involved
  - Obtain and examine evidence
  - Report for further action

Fraud Detection

- Fraud detection is Management’s responsibility
- Benefits of a well-designed internal control system
- Deterring fraud at the first instance
- Detecting fraud in a timely manner
- Fraud detection and disclosure
- Auditor’s role in fraud prevention and detection
Risk- Based Auditing
A Quick Review of Risk Assessment and Mitigating Controls

Definition of Risk

- Risk is the likelihood of a threat exploiting a vulnerability and the resulting impact on business mission
- Risk assessment must be based on business requirements, not solely on information systems
Purpose of Risk Management

- Risk Assessment
  - Identify and prioritise risk
  - Recommend risk-based controls
- Risk Mitigation
  - Reduce risk
  - Accept risk
  - Transfer risk
  - Avoid risk
- Ongoing assessment of risk levels and control effectiveness

Risk Management

1. Identify Business Objectives (BO)
2. Identify Business Assets that Support the BO
3. Perform Risk Assessment (RA) [Threat - Vulnerability - Probability - Impact]
4. Perform Risk Mitigation (RM) [Map Risks with controls in place]
5. Perform Risk Treatment (RT) [Treat existing risks not mitigated by existing controls]
6. Perform Periodic Risk Re-evaluation (BO, RA, RM, RT)

© Firebrand Training Ltd
ISACA CISA Certification | Certified Information Systems Auditor Courseware version 5
Purpose of Risk Analysis

- Identity threats and vulnerabilities
- Helps auditor evaluate countermeasures/controls
- Helps auditor decide on auditing objectives
- Support Risk-Based auditing decision
- Leads to implementation of internal controls

Why Use Risk Based Auditing

- Enables management to effectively allocate limited audit resources
- Ensures that relevant information has been obtained from all levels of management
- Establishes a basis for effectively managing the audit plans
- Provides a summary of how the individual audit subject is related to the overall organisation as well as to the business plan
Assessing security risks
- Risk assessments should identify, quantify and prioritise risks against criteria for risk acceptance and objectives relevant to the organisation
- Performed periodically to address changes in:
  - The environment
  - Security requirements and when significant changes occur

Treating security risks
- Each risk identified in a risk assessment needs to be treated in a cost-effective manner according to its level of risk
- Controls should be selected to ensure that risks are reduced to an acceptable level
General Controls

- Apply to all areas of an organisation and include policies and practices established by management to provide reasonable assurance that specific objectives will be achieved.

Internal Controls

- Policies, procedures, practices and organisational structures implemented to reduce risks
- Classification of internal controls
  - Preventive controls
  - Detective controls
  - Corrective controls
Areas of Internal Control

- Internal control system
  - Internal accounting controls
  - Operational controls
  - Administrative controls

IS Controls Versus Manual Controls

- Internal control objectives apply to all areas, whether manual or automated. Therefore, conceptually, control objectives in an IS environment remain unchanged from those of a manual environment.
IS Controls

- Strategy and direction
- General organisation and management
- Access to IT resources, including data and programs
- Systems development methodologies and change control
- Operations procedures
- Systems programming and technical support functions

IS Controls (continued)

- Quality assurance procedures
- Physical access controls
- Business continuity/disaster recovery planning
- Networks and communications
- Database administration
- Protection and detective mechanisms against internal and external attacks
Internal Control Objectives

- Internal control objectives
  - Safeguarding of IT assets
  - Compliance to corporate policies or legal requirements
  - Input
  - Authorisation
  - Accuracy and completeness of processing of data input/transactions
  - Output
  - Reliability of process
  - Backup/recovery
  - Efficiency and economy of operations
  - Change management process for IT and related systems

Assessing and Implementing Countermeasures

- Cost
- Assess management’s tolerance for risk
- Effectiveness at mitigating Risk
Performing an Audit Risk Assessment

- Identify
  - Business risks
  - Technological risks
  - Operational risks

A Risk Based Audit Approach
Risk-based Auditing

Gather Information and Plan;
- Knowledge of business and industry
- Prior year’s audit results
- Recent financial information
- Regulatory statutes
- Inherent risk assessments

Obtain Understanding of Internal Control;
- Control environment
- Control procedures
- Detection risk assessment
- Control risk assessment
- Equate total risk

Perform Compliance Tests;
- Identify key controls to be tested
- Perform tests on reliability, risk prevention, and adherence to organisational policies and procedures

Perform Substantive Tests;
- Analytical procedures
- Detailed tests of account balances
- Other substantive audit procedures

Conclude the Audit;
- Create recommendations
- Write audit report
Audit Planning

- Audit planning steps
  - Gain an understanding of the business’s mission, objectives, purpose and processes
  - Identify stated contents (policies, standards, guidelines, procedures, and organisation structure)
  - Evaluate risk assessment and privacy impact analysis
  - Perform a risk analysis
Audit Planning (continued)

- Conduct an internal control review
- Set the audit scope and audit objectives
- Develop the audit approach or audit strategy
- Assign personnel resources to audit and address engagement logistics

Effect of Laws and Regulations on IS Audit Planning

- Regulatory requirements
  - Adequate controls
  - Privacy
  - Responsibilities
  - Oversight and Governance
  - Protection of assets
  - Financial Management
  - Correlation to financial, operational and IT audit functions
Performing the Audit

ISACA IT Audit and Assurance Tools and Techniques

- Procedures developed by the ISACA Standards Board provide examples of possible processes an IS auditor might follow in an audit engagement
- The IS auditor should apply their own professional judgment to the specific circumstances
ISACA IT Audit and Assurance Standards Framework

- Framework for the ISACA IS Auditing Standards:
  - Standards
  - Guidelines
  - Procedures

Relationship Among Standards, Guidelines and Tools and Techniques

- **Standards**
  - Must be followed by IS auditors
- **Guidelines**
  - Provide assistance on how to implement the standards
- **Tools and Techniques**
  - Provide examples for implementing the standards
## ISACA IT Audit and Assurance Standards Framework (continued)

- S1 Audit Charter
- S2 Independence
- S3 Ethics and Standards
- S4 Competence
- S5 Planning
- S6 Performance of audit work
- S7 Reporting
- S8 Follow-up activities
- S9 Irregularities and illegal acts
- S10 IT Governance
- S11 Use of risk assessment in audit planning
- S12 Audit materiality
- S13 Using the Work of Other Experts
- S14 Audit Evidence
- S15 IT Controls
- S16 E-commerce

## Evidence

- It is a requirement that the auditor’s conclusions be based on sufficient, competent evidence:
  - Independence of the provider of the evidence
  - Qualification of the individual providing the information or evidence
  - Objectivity of the evidence
  - Timing of the evidence
Gathering Evidence

- Techniques for gathering evidence:
  - Review IS organisation structures
  - Review IS policies and procedures
  - Review IS standards
  - Review IS documentation
  - Interview appropriate personnel
  - Observe processes and employee performance

Sampling

- General approaches to audit sampling:
  - Statistical sampling
  - Non-statistical sampling
Compliance vs. Substantive Testing

- Compliance test
  - Determines whether controls are in compliance with management policies and procedures
- Substantive test
  - Tests the integrity of actual processing
- Correlation between the level of internal controls and substantive testing required
- Relationship between compliance and substantive tests

Testing Controls

- Review the system to identify controls
- Test compliance to determine whether controls are functioning.
- Evaluate the controls to determine the basis for reliance and the nature, scope and timing of substantive tests.
- Use two types of substantive tests to evaluate the validity of the data.
  - Test balance and transactions
  - Perform analytic review procedures
Integrated Auditing

- Process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity.
- Focuses on risk to the organisation (for an internal auditor)
- Focuses on the risk of providing an incorrect or misleading audit opinion (for an external auditor)

Using the Services of Other Auditors and Experts

- Considerations when using services of other auditors and experts:
  - Audit charter or contractual stipulations
  - Impact on overall and specific IS audit objectives
  - Impact on IS audit risk and professional liability
  - Independence and objectivity of other auditors and experts
Using the Services of Other Auditors and Experts (continued)

- Considerations when using services of other auditors and experts:
  - Professional competence, qualifications and experience
  - Scope of work proposed to be outsourced and approach
  - Supervisory and audit management controls
  - Method of communicating the results of audit work
  - Compliance with legal and regulatory stipulations
  - Compliance with applicable professional standards

Audit Risk

- Inherent Risk
- Control Risk
- Overall Audit Risk
- Detection Risk
Computer-assisted Audit Techniques

CAATs enable IS auditors to gather information independently

CAATs include:
- Generalised audit software (GAS)
- Utility software
- Debugging and scanning software
- Test data
- Application software tracing and mapping
- Expert systems

Computer-assisted Audit Techniques (continued)

Features of generalised audit software (GAS):
- Mathematical computations
- Stratification
- Statistical analysis
- Sequence checking
Computer-assisted Audit Techniques (continued)

Functions supported by GAS:

- File access
- File reorganisation
- Data selection
- Statistical functions
- Arithmetical functions

CAATs as a continuous online audit approach:

- Improves audit efficiency

IS auditors must:

- Develop audit techniques for use with advanced computerised systems
- Be involved in the design of advanced systems to support audit requirements
- Make greater use of automated tools
Audit Analysis and Reporting

Audit Documentation

- Audit documentation includes:
  - Planning and preparation of the audit scope and objectives
  - Description on the scoped audit area
  - Audit program
  - Audit steps performed and evidence gathered
  - Other experts used
  - Audit findings, conclusions and recommendations
Automated Work Papers

- Risk analysis
- Audit programs
- Results
- Test evidences
- Conclusions
- Reports and other complementary information

Automated Work Papers (continued)

- Minimum controls:
  - Access to work papers
  - Audit trails
  - Automated features to provide and record approvals
  - Security and integrity controls
  - Backup and restoration
  - Encryption techniques
Evaluation of Audit Strengths and Weaknesses

- Assess evidence
- Evaluate overall control structure
- Evaluate control procedures
- Assess control strengths and weaknesses

Communicating Audit Results

- Exit interview
  - Correct facts
  - Realistic recommendations
  - Implementation dates for agreed recommendations
- Presentation techniques
  - Executive summary
  - Visual presentation
Communicating Audit Results (continued)

- Audit report structure and contents
  - Introduction to the report
  - Audit findings presented in separate sections
  - The IS auditor’s overall conclusion and opinion
  - The IS auditor’s reservations with respect to the audit - audit limitations
  - Detailed audit findings and recommendations

Communicating Audit Results (continued)

- Audit recommendations may not be accepted
  - Negotiation
  - Conflict resolution
  - Explanation of results, findings and best practices or legal requirements
Management Implementation of Audit Recommendations

- Ensure that accepted recommendations are implemented as per schedule
- Auditing is an ongoing process
- Timing a follow-up

Control Self-Assessment

- A management technique
- A methodology
- In practice, a series of tools
- Can be implemented by various methods
Objectives of CSA

- Leverage the internal audit function by shifting some control monitoring responsibilities to functional areas
- Enhancement of audit responsibilities, not a replacement
- Educate management about control design and monitoring
- Empowerment of workers to assess the control environment

Benefits of CSA

- Early detection of risks
- More effective and improved internal controls
- Increased employee awareness of organisational objectives
- Highly motivated employees
- Improved audit rating process
- Reduction in control cost
- Assurance provided to stakeholders and customers
Disadvantages of CSA

- Could be mistaken as an audit function replacement
- May be regarded as an additional workload
- Failure to act on improvement suggestions could damage employee morale
- Lack of motivation may limit effectiveness in the detection of weak controls

Auditor Role in CSA

- Internal control professionals
- Assessment facilitators
Traditional vs. CSA Approach

- **Traditional Approach**
  - Assigns duties/supervises staff
  - Policy/rule driven
  - Limited employee participation
  - Narrow stakeholder focus

- **CSA Approach**
  - Empowered/accountable employees
  - Continuous improvement/learning curve
  - Extensive employee participation and training
  - Broad stakeholder focus

Continuous Auditing Vs. Continuous Monitoring

- **Continuous monitoring**
  - Provided by IS management tools
  - Based on automated procedures to meet fiduciary responsibilities

- **Continuous auditing**
  - Audit-driven
  - Completed using automated audit procedures
Continuous Auditing

Distinctive character
• Short time lapse between the facts to be audited and the collection of evidence and audit reporting

Drivers
• Better monitoring of financial issues
• Allows real-time transactions to benefit from real-time monitoring
• Prevents financial fiascoes and audit scandals
• Uses software to determine proper financial controls

Continuous Auditing (continued)

Application of continuous auditing due to:
• New information technology developments
• Increased processing capabilities
• Standards
• Artificial intelligence tools
Continuous Auditing (continued)

_advantages
- Instant capture of internal control problems
- Reduction of intrinsic audit inefficiencies

_disadvantages
- Difficulty in implementation
- High cost
- Elimination of auditors’ personal judgment and evaluation

ISACA Code of Professional Ethics

_Advantages
The Association’s Code of Professional Ethics provides guidance for the professional and personal conduct of members of ISACA and/or holders of ISACA designations.
Conclusion

Know

• Audit Planning
• Performing an Audit
• Risk as related to audit planning and performance
• Ongoing Audit techniques
• Ethics
ISACA®
Trust in, and value from, information systems

2016 CISA® Review Course

Governance and Management of IT
Exam Relevance

Ensure that the CISA candidate...

- Understands and can provide assurance that the organisation has the structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.

- The content area in this chapter will represent approximately 16% of the CISA examination (approximately 24 questions).

Agenda

- Tasks and Knowledge Statements
- Definition of Corporate Governance
- Strategic Planning and Models
- Policies, Standards and Procedures
Task Statements

- Effective governance of IT to support the organisation
- IT organisational structure
  - Strategy
  - Policies, standards, procedures
- Reporting to management
- Monitoring of controls

Task Statements (continued)

- Resource investment and management
- Contracting
- Performance measurement and reporting
- Risk management strategies
- Business continuity strategy
- Business impact analysis
Governance and Management of IT

Corporate Governance

- Ethical corporate behaviour
- Governance of IT systems and assets towards the preservation of value for all stakeholders
- Resource management
- Establishment of rules to manage and report on business risks
Governance of Enterprise IT

Comprises the body of issues addressed in considering how IT is applied within the enterprise.

Effective enterprise governance focuses on:
- Individual and group expertise
- Experience in specific areas
- Key element: alignment of business and IT

Governance of Enterprise IT cont.

Two issues:
- IT delivers value to the business
- IT risks are managed
**Information Technology Monitoring and Assurance Practices for Management**

- IT governance implies a system where all stakeholders provide input into the decision making process:
  - Board
  - Internal customers
  - Finance

**Best Practices for IT Governance**

**Strategic Alignment**
- Focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

**Value Delivery**
- Is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and improving the intrinsic value of IT.

**Resource Management**
- Is about the optimal investment in, and the proper management of, Critical IT resources: applications, information, infrastructure and people, Key issues relate to the optimisation of knowledge and infrastructure.
Best Practices for IT Governance (continued)

Risk Management
- Requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

Performance Measurement
- Tracks and monitors strategy implementation, projection completion, resource usage, process performance and services delivery, using, for example, balanced scorecards that translate into action to achieve goals measurable beyond conventional accounting.

Information Security Governance
- Focused activity with specific value drivers
  - Integrity of information
  - Continuity of services
  - Protection of information assets
- Integral part of IT governance
- Importance of information security governance
Information Security Governance

- Should be supported at the highest levels of the organisation
- IS Gov. broadens scope beyond simply protection of IT system and data - integration and overall security regardless of handling, processing, transporting, or storing.
- Protects information assets at all times, in all forms (electronic, paper, communicated), and in all locations

Information Security Governance

- Exposure to civil and legal liability, regulators
- Provide assurance of policy compliance
- Enhance business Ops continuity - lower risk: uncertainty
- Foundation for risk management, process enhanced and fast incident response procedures
- Optimise allocation of the limited security resources as well as procurement process
- Ensuring that important decisions are made on accurate data
Result of Security Governance

- Strategic link to business / Organisation Objectives
- Overall risk management
- Optimise investments
- Management of resources
- Report on performance / results
- Process integration

Strategic Planning and Models
IS Strategy

- Strategic Planning.
- Steering committee role.
- Primary strategic functions

Strategic Enterprise Architecture Plans

- Involves documenting an organisation’s IT assets in a structured manner to facilitate understanding, management and planning for IT investments
- Often involves both a current state and optimised future state representation
IT Strategy Committee

- The creation of an IT strategy committee is an industry best practice
- Committee should broaden its scope to include not only advice on strategy when assisting the board in its IT governance responsibilities, but also to focus on IT value, risks and performance

Standard IT Balanced Scorecard

- A process management evaluation technique that can be applied to the IT governance process in assessing IT functions and processes
- Method goes beyond the traditional financial evaluation
- One of the most effective means to aid the IT strategy committee and management in achieving IT and business alignment
Enterprise Architecture (continued)

The Basic Zachman Framework

<table>
<thead>
<tr>
<th></th>
<th>Data</th>
<th>Functional</th>
<th>Network</th>
<th>People</th>
<th>Process</th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Model</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems Model</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Model</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Representation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enterprise Architecture (continued)

* The Federal Enterprise Architecture (FEA) hierarchy:
  - Performance
  - Business
  - Service component
  - Technical
  - Data
Maturity and Process Improvement Models

- IDEAL model
  - Capability Maturity Model Integration (CMMI)
  - Team Software Process (TSP)
  - Personal Software Process (PSP)

IT Investment and Allocation Practices

- Financial benefits - impact on budget and finances
- Nonfinancial benefits - impact on operations or mission performance and results
Auditing IT Governance Structure and Implementation

Indicators of potential problems include:

- Unfavourable end-user attitudes
- Excessive costs
- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent hardware/software errors

Policies, Standards and Procedures
Policies and Procedures

Reflect management guidance and direction in developing controls over:

- Information systems
- Related resources
- IS department processes

Policies

- High level documents
- Must be clear and concise
- Set tone for organisation as a whole (top down)
- Lower-level policies - defined by individual divisions and departments
Policies (continued)

- Information Security Policy
  - Defines information security, overall objectives and scope
  - Statement of management intent
  - Framework for setting control objectives including risk management
  - Defines responsibilities for information security management
  - Acceptable Use Policy

Procedures

- Procedures are detailed documents that describe the steps a person must follow when undertaking an activity:
  - Define and document implementation policies
  - Must be derived from the parent policy
  - Must implement the spirit (intent) of the policy statement
  - Must be written in a clear and concise manner
Standards

- Audits measure compliance with standards of:
  - Operational procedures
  - Best practices
  - Consistency of performance

Risk Management
Risk Management Process

- IT risk management needs to operate at multiple levels including:
  - The operational level
  - The project level
  - The strategic level

Risk Analysis Methods

- Qualitative
- Semi quantitative
- Quantitative
  - Probability and expectancy
  - Single loss expectancy
  - Annual loss expectancy method
Risk Mitigation

Eliminate  Avoid

Accept  Mitigate

Transfer

Resource Management
Organisation of the IT Function

- The auditor must assess whether the IT department is correctly:
  - Funded
  - Aligned with business needs
  - Managed
  - Staffed (skills)

IS Roles and Responsibilities

- Systems development manager
- Project management
- Service Desk (help desk)
- End user
- End user support manager
- Data management
- Quality assurance manager
- Information security manager
IS Roles and Responsibilities (continued)

- Vendor and outsourcer management
- Infrastructure operations and maintenance
- Media management
- Data entry
- Systems administration
- Security administration
- Quality assurance
- Database administration

IS Roles and Responsibilities (continued)

- Systems analyst
- Security architect
- Applications development and maintenance
- Infrastructure development and maintenance
- Network management
Segregation of Duties Within IS

- Avoids possibility of errors or misappropriations
- Discourages fraudulent acts
- Limits access to data

Segregation of Duties Controls

- Control measures to enforce segregation of duties include:
  - Transaction authorisation
  - Custody of assets
  - Access to data
  - Authorisation forms
  - User authorisation tables
Segregation of Duties Controls (continued)

- Compensating controls for lack of segregation of duties include:
  - Audit trails
  - Reconciliation
  - Exception reporting
  - Transaction logs
  - Supervisory reviews
  - Independent reviews

Human Resource Management

- Hiring
- Employee handbook
- Promotion policies
- Training
- Scheduling and time reporting
- Employee performance evaluations
- Required vacations
- Termination policies
Sourcing Practices

- Sourcing practices relate to the way an organisation obtains the IS function required to support the business.
- Organisations can perform all IS functions in-house or outsource all functions across the globe.
- Sourcing strategy should consider each IS function and determine which approach (insourcing or outsourcing) allows the IS function to meet the organisation’s goals.

Management of IT Functional Operations
Organisational Change Management

What is change management?
- Managing changes to the organisation’s:
  - Projects
  - Systems
  - Technology
  - Configurations

Identify and apply technology improvements at the infrastructure and application level

Change Management (continued)

- All changes must be documented, approved and tested
- All changes must be performed correctly and monitored for successful execution
- Changes must not degrade system security or performance
Quality Management

- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- Service management
- Security
- Human resource management
- General administration

Performance Optimisation

- Performance measures indicate the quality of the IT program
  - Measures should be set to evaluate services critical to business success
- There are generally five ways to use performance measures:
  1. Measure products/services
  2. Manage products/services
  3. Ensure accountability
  4. Make budget decisions
  5. Optimise performance
Reviewing Documentation

The following documents should be reviewed:

- IT strategies, plans and budgets
- Security policy documentation
- Organisation/functional charts
- Job descriptions
- Steering committee reports
- System development and program change procedures
- Operations procedures
- Human resource manuals
- Quality assurance procedures

Reviewing Contractual Commitments

There are various phases to computer hardware, software and IS service contracts, including:

- Development of contract requirements and service levels
- Contract bidding process
- Contract selection process
- Contract acceptance
- Contract maintenance
- Contract compliance
Business Continuity Planning

- Business continuity planning (BCP) is a process designed to reduce the organisation’s business risk
- A BCP is much more than just a plan for the information systems
IS Business Continuity Planning

- IS processing is of strategic importance
  - Critical component of overall BCP
  - Most key business processes depend on the availability of key systems and infrastructure components

Disasters and Other Disruptive Events

- Disasters are disruptions that cause critical information resources to be inoperative for a period of time
- Good BCP will take into account impacts on IS processing facilities
Business Continuity Policy

🌟 Defines the extent and scope of business continuity for both internal and external stakeholders

🌟 Should be proactive
Business Continuity Planning Incident Management

- All types of incidents should be categorised
  - Negligible
  - Minor
  - Major
  - Crisis

Business Impact Analysis

- Critical step in developing the business continuity plan

- Three main questions to consider during BIA phase:
  1. What are the different business processes?
  2. What are the critical information resources related to an organisation’s critical business processes?
  3. What is the critical recovery time period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered?
Business Impact Analysis (continued)

- What is the system’s risk ranking?
  - Critical
  - Vital
  - Sensitive
  - Non-sensitive

Development of Business Continuity Plans

- Factors to consider when developing the plans
  - Pre-disaster readiness covering incident response management to address all relevant incidents affecting business processes
  - Evacuation procedures
  - Procedures for declaring a disaster (escalation procedures)
  - Circumstances under which a disaster should be declared
Development of Business Continuity Plans

- Factors to consider when developing the plans
  - The clear identification of the responsibilities in the plan
  - The clear identification of the persons responsible for each function in the plan
  - The clear identification of contract information
  - The step-by-step explanation of the recovery process
  - The clear identification of the various resources required for recovery and continued operation of the organisation

Other Issues in Plan Development

- Management and user involvement is vital to the success of BCP
  - Essential to the identification of critical systems, recovery times and resources
  - Involvement from support services, business operations and information processing support
- Entire organisation needs to be considered for BCP
## Components of a Business Continuity Plan

- A business continuity plan may consist of more than one plan document
  - Continuity of operations plan (COOP)
  - Disaster recovery plan (DRP)
  - Business resumption plan
  - Continuity of support plan / IT contingency plan
  - Crisis communications plan
  - Incident response plan
  - Transportation plan
  - Occupant emergency plan (OEP)
  - Evacuation and emergency relocation plan

## Components of a Business Continuity Plan (continued)

- Components of the plan
  - Key decision-making personnel
  - Backup of required supplies
  - Insurance
Insurance

- Insurance
  - IS equipment and facilities
  - Media (software) reconstruction
  - Extra expense
  - Business interruption
  - Valuable papers and records
  - Errors and omissions
  - Fidelity coverage
  - Media transportation

Plan Testing

- Schedule testing at a time that will minimise disruptions to normal operations
- Test must simulate actual processing conditions
- Test execution:
  - Documentation of results
  - Results analysis
  - Recovery / continuity plan maintenance
Summary of Business Continuity

- Business continuity plan must:
  - Be based on the long-range IT plan
  - Comply with the overall business continuity strategy

Summary of Business Continuity and Disaster Recovery (continued)

- Process for developing and maintaining the BCP/DRP
  - Conduct risk assessment
  - Prepare business impact analysis
  - Choose appropriate controls and measures for recovering IT components to support the critical business processes
  - Develop the detailed plan for recovering IS facilities (DRP).
  - Develop a detailed plan for the critical business functions to continue to operate at an acceptable level (BCP).
  - Test the plans
  - Maintain the plans as the business changes and systems develop.
Auditing Business Continuity

- Understand and evaluate business continuity strategy
- Evaluate plans for accuracy and adequacy
- Verify plan effectiveness
- Evaluate offsite storage
- Evaluate ability of IS and user personnel to respond effectively
- Ensure plan maintenance is in place
- Evaluate readability of business continuity manuals and procedures

Reviewing the Business Continuity Plan

- IS auditors should verify that the plan is up to date including:
  - Currency of documents
  - Effectiveness of documents
  - Interview personnel for appropriateness and completeness of plan
Evaluation of Prior Test Results

IS auditors must review the test results to:

• Determine whether corrective actions are in the plan
• Evaluate thoroughness and accuracy
• Determine problem trends and resolution of problems

Evaluation of Offsite Storage

An IS auditor must:

• Evaluate presence, synchronisation and currency of media and documentation
• Perform a detailed inventory review
• Review all documentation
• Evaluate availability of facility
Interviewing Key Personnel

- Key personnel must have an understanding of their responsibilities
- Current detailed documentation must be kept

Evaluation of Security at Offsite Facility

- An IS auditor must:
  - Evaluate the physical and environmental access controls
  - Examine the equipment for current inspection and calibration tags
Reviewing Alternative Processing Contract

- An IS auditor should obtain a copy of the contract with the vendor
- The contract should be reviewed against a number of guidelines
  - Contract is clear and understandable
  - Organisation’s agreement with regulations

Reviewing Insurance Coverage

- Insurance coverage must reflect actual cost of recovery
- Coverage of the following must be reviewed for adequacy
  - Media damage
  - Business interruption
  - Equipment replacement
  - Business continuity processing
End of Domain
ISACA®
Trust in, and value from, information systems

2016 CISA® Review Course
Chapter 3
Information Systems Acquisition, Development and Implementation
Exam Relevance

Ensure that the CISA candidate...

• Understands and can provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the enterprise’s strategies and objectives

• The content area in this chapter will represent approximately 18% of the CISA examination

(approximately 27 questions)

Agenda

• Learning Objectives
• Program and Project Management
• Systems Development Models
• Types of Specialised Business Applications
• Acquisition
• Change Control
Learning Objectives

- Evaluate Business Case for IT project approval
  - Feasibility, meets business objectives
- Evaluate project management practices and controls
  - Cost-effective, meets business objectives
- Conduct project reviews
  - On schedule, budget, deliverables, documentation

Learning Objectives cont.

- Ensure controls are built into systems during requirements, acquisition, development, and testing phases
- Evaluate readiness of the system for implementation and migration into production
- Conduct post-implementation reviews to ensure project and business objectives are met
Program and Project Management

Portfolio/Program Management

- A program is a group of projects and time-bound tasks that are closely linked together through common objectives, a common budget, intertwined schedules and strategies.
- Programs have a limited time frame (start and end date) and organisational boundaries.
Portfolio/Program Management (continued)

- The objectives of project portfolio management are:
  - Optimisation of the results of the project portfolio
  - Prioritising and scheduling projects
  - Resource coordination (internal and external)
  - Knowledge transfer throughout the projects

Business Case Development and Approval

- A business case:
  - Provides the information required for an organisation to decide whether a project should proceed
  - Is normally derived from a feasibility study as part of project planning
  - Should be of sufficient detail to describe the justification for setting up and continuing a project
Benefits Realisation Techniques

- Benefits realisation requires:
  - Describing benefits management or benefits realisation
  - Assigning a measure and target
  - Establishing a tracking/measuring regime
  - Documenting the assumption
  - Establishing key responsibilities for realisation
  - Validating the benefits predicted in the business
  - Planning the benefit that is to be realised

General IT Project Aspects

- IS projects may be initiated from any part of an organisation
- A project is always a time-bound effort
- Project management should be a business process of a project-oriented organisation
- The complexity of project management requires a careful and explicit design of the project management process
Project Context and Environment

- A project context can be divided into a time and social context. The following must be taken into account:
  - Importance of the project in the organisation
  - Connection between the organisation’s strategy and the project
  - Relationship between the project and other projects
  - Connection between the project to the underlying business case

Project Organisational Forms

- Three major forms of organisational alignment for project management are:
  - Influence project organisation
  - Pure project organisation
  - Matrix project organisation
Project Communication

- Depending on the size and complexity of the project and the affected parties, communication may be achieved by:
  - One-on-one meetings
  - Kick-off meetings
  - Project start workshops
  - A combination of the three

Project Objectives

- A project needs clearly defined results that are specific, measurable, achievable, relevant and time-bound (SMART)
- A commonly accepted approach to define project objectives is to begin with an object breakdown structure (OBS)
- After the OBS has been compiled, a work breakdown structure (WBS) is designed
Roles and Responsibilities of Groups and Individuals

- Senior management
- User management
- Project steering committee
- Project sponsor
- Systems development management
- Project manager
- Systems development project team
- User project team
- Security officer
- Quality assurance

Project Management Practices

- Project management is bound by the iron triangle
  - Schedule
  - Resources
  - Scope

- Changing any one element will invariably change the other two
Project Planning

The project manager needs to determine:

- The various tasks that need to be performed to produce the expected business application system
- The sequence or the order in which these tasks need to be performed
- The duration or the time window for each task
- The priority of each task
- The IT resources that are available and required to perform these tasks
- Budget or costing for each of these tasks
- Source and means of funding

Project Planning (continued)

- Software size estimation
- Lines of source code
- Function point analysis
  - FPA feature points
  - Cost budgets
  - Software cost estimation
- Scheduling and establishing the time frame
  - Critical path methodology
    - Gantt Chart
    - PERT
    - Time box management
General Project Management

- Involves automated techniques to handle proposals and cost estimations, and to monitor, predict and report on performance with recommended action items.

- Many of these techniques are provided as decision support systems (DSS) for planning and controlling project resources.

Project Controlling

- Includes management of:
  - Scope
  - Resource usage
  - Risk
  - Inventory
  - Assess
  - Mitigate
  - Discover
  - Review & evaluate
Project Risk

The CISA must review the project for risks that the project will not deliver the expected benefits:

- Scope creep
- Lack of skilled resources
- Inadequate requirements definition
- Inadequate testing
- Push to production without sufficient allotted time

Closing a Project

When closing a project, there may still be some issues that need to be resolved, ownership of which needs to be assigned.

The project sponsor should be satisfied that the system produced is acceptable and ready for delivery.

Custody of contracts may need to be assigned, and documentation archived or passed on to those who will need it.
Business Application Development

The implementation process for business applications, commonly referred to as an SDLC, begins when an individual application is initiated as a result of one or more of the following situations:

- A new opportunity that relates to a new or existing business process
- A problem that relates to an existing business process
- A new opportunity that will enable the organisation to take advantage of technology
- A problem with the current technology
Traditional SDLC Approach

- Also referred to as the waterfall technique, this life cycle approach is the oldest and most widely used for developing business applications.
- Based on a systematic, sequential approach to software development that begins with a feasibility study and progresses through requirements definition, design, development, implementation and post implementation.

Traditional SDLC Approach (continued)

- Some of the problems encountered with this approach include:
  - Unanticipated events
  - Difficulty in obtaining an explicit set of requirements from the user
  - Managing requirements and convincing the user about the undue or unwarranted requirements in the system functionality
  - The necessity of user patience
  - A changing business environment that alters or changes the user’s requirements before they are delivered.
Traditional SDLC Approach (continued)

- Feasibility
- Requirements
- Design
- Implement
- Configuration
- Selection Development
- Post-Implementation

Requirements Definition

- Need to understand business requirements
  - May involve helping the business to understand their needs
  - Trace business requirements to systems requirements
  - Justify systems solutions based on stated business requirements
Business Process Reengineering and Process Change Projects

<table>
<thead>
<tr>
<th>Generic Process Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Control</td>
</tr>
<tr>
<td>- Process Owner</td>
</tr>
<tr>
<td>- Process Goal</td>
</tr>
<tr>
<td>- Process Parameters</td>
</tr>
<tr>
<td>(Quality, KPIs, etc.)</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Process</td>
</tr>
<tr>
<td>(Defined) Input</td>
</tr>
<tr>
<td>Subprocesses or Activities</td>
</tr>
<tr>
<td>(Defined) Output</td>
</tr>
<tr>
<td>Process Enabler</td>
</tr>
<tr>
<td>- Resources</td>
</tr>
<tr>
<td>- Roles</td>
</tr>
</tbody>
</table>

Business Process Reengineering and Process Change Projects (continued)

*BPR methods and techniques*

- Benchmarking process

© Firebrand Training Ltd
ISACA CISA Certification | Certified Information Systems Auditor Courseware version 5
Risks Associated with Software Development

- Business risk relating to the likelihood that the new system may not meet the users’ business needs, requirements and expectations
- Potential risks that can occur when designing and developing software systems:
  - Within the project
  - With suppliers
  - Within the organisation
  - With the external environment

Use of Structured Analysis, Design and Development Techniques

- Closely associated with the traditional, classic SDLC approach
- Techniques provide a framework for representing the data and process components of an application using various graphical notations at different levels of abstraction, until it reaches the abstraction level that enables programmers to code the system
Alternative Development Methods

Many new software development approaches have emerged.

Traditional waterfall model is being replaced along with some revolutionary thinking.

IS auditing may encounter the following.

- Incremental
- Evolutionary

Iterative

Spiral

Agile Development

Agile development refers to a family of similar development processes that espouse a non-traditional way of developing complex systems.

Agile development processes have a number of common characteristics, including:

- The use of small, time-boxed subprojects or iterations
- Re-planning the project at the end of each iteration
- Relatively greater reliance on tacit knowledge
- Heavy influence on mechanisms to effectively disseminate tacit knowledge and promote teamwork
- A change in the role of the project manager
Agile Development

- Image available


Prototyping

- The process of creating a system through controlled trial and error procedures to reduce the level of risks in developing the system
- Reduces the time to deploy systems primarily by using faster development tools such as fourth-generation techniques
- Potential risk is that the finished system will have poor controls
- Change control often becomes more complicated
Rapid Application Development

- Concept Definition
- Functional Design
- Development
- Deployment

Other Alternative Development Methods

- Data-Oriented (DOSD)
- Object-Oriented (OOSD)
- Component-Based (DCOME, COBRA, RMI, MTS, MJB).
- Web Based (XML, SOAP)
- Reverse engineering
Computer-aided Software Engineering

- Case involves automated tools: Upper, Middle, Lower.
- Available for mainframe and mini/micro computers.
- Enforce uniform approach to system developer, enable storage & document retrieval, automate system design data.
- Auditor may even use case tool him/herself.

Fourth-generation Languages

- Common characteristics of 4GLs include:
  - Nonprocedural language
  - Environmental independence (portability)
  - Software facilities
  - Programmer workbench concepts
  - Simple language subsets
- 4GLs are classified as:
  - Query and report generators
  - Embedded database 4GLs
  - Relational database 4GLs
  - Application generators
Types of Specialised Business Applications

Electronic Commerce

- E-commerce risks:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication and non-repudiation
  - Power shift to customers

- It is important to take into consideration the importance of security issues that extend beyond confidentiality objectives
Electronic Data Interchange

The benefits associated with the adoption of EDI include:

- Less paperwork
- Fewer errors during the exchange of information
- Improved information flow, database-to-database and company-to-company
- No unnecessary rekeying of data
- Fewer delays in communication
- Improved invoicing and payment processes

Electronic Mail

At the most basic level, the e-mail process can be divided into two principal components:

- Mail servers, which are hosts that deliver, forward and store mail
- Clients, which interface with users and allow users to read, compose, send and store e-mail messages
Electronic Banking

- Banks should have a risk management process to enable them to identify, measure, monitor and control their technology risk exposure.
- Risk management of new technologies has three essential elements:
  - Risk management is the responsibility of the board of directors and senior management.
  - Implementing technology is the responsibility of IT senior management members.
  - Measuring and monitoring risk is the responsibility of members of operational management.

Electronic Finance

- Advantages of e-finance to consumers include:
  - Lower costs
  - Increased breadth and quality
  - Widening access to financial services
  - A-synchrony (time-decoupled)
  - A-topy (location-decoupled)
Electronic Funds Transfer

- Electronic funds transfer (EFT) is the exchange of money via telecommunications without currency actually changing hands
- Allows parties to move money from one account to another, replacing traditional check writing and cash collection procedures
- Usually function via an internal bank transfer from one party’s account to another or via a clearinghouse network

Automated Teller Machine

- Recommended internal control guidelines for ATMs include:
  - Written policies and procedures covering personnel, security controls, operations, settlement, balancing, etc.
  - Procedures for PIN issuance and protection during storage
  - Procedures for the security of PINs during delivery
  - Controls over plastic card procurement
  - Controls and audit trails of the transactions that have been made at the ATM
Artificial Intelligence and Expert Systems

Artificial intelligence is the study and application of the principles by which:

- Knowledge is acquired and used
- Goals are generated and achieved
- Information is communicated
- Collaboration is achieved
- Concepts are formed
- Languages are developed

Business Intelligence

Business intelligence (BI) is a broad field of IT that encompasses the collection and dissemination of information to assist decision making and assess organisational performance.

Some typical areas in which BI is applied include:

- Process cost, efficiency and quality
- Customer satisfaction with product and service offerings
- Customer profitability
- Staff and business unit achievement of KPIs
- Risk management
A decision support system (DSS) is an interactive system that provides the user with easy access to decision models and data from a wide range of sources, to support semi-structured decision-making tasks typically for business purposes.

A principle of DSS design is to concentrate less on efficiency and more on effectiveness. A DSS is often developed with a specific decision or well-defined class of decisions to solve. Frameworks are generalisations about a field that help put many specific cases and ideas into perspective:

- G. Gorry-M.S. Morton framework
- Sprague-Carson framework
Prototyping is the most popular approach to DSS design and development

It is difficult to implement a DSS because of its discretionary nature

Developers should be prepared for eight implementation risk factors:

- Non-existent or unwilling users
- Multiple users or implementers
- Disappearing users, implementers or maintainers
- Inability to specify purpose or usage patterns in advance
- Inability to predict and cushion impact on all parties
- Lack or loss of support
- Lack of experience with similar systems
- Technical problems and cost-effectiveness issues
The DSS designer and user should use broad evaluation criteria, including:

- Traditional cost-benefit analysis
- Procedural changes, more alternatives examined, less time consumer in making the decision
- Evidence of improvement in decision making
- Changes in the decision process

Acquisition
Infrastructure Development / Acquisition Practices

- Analysis of present infrastructure leads to new design, techniques, procedures, training.
- Under umbrella of business continuity, legacy hw/sw, data conversion: Translation, 24 x 7 availability.
- Goals: Reduce costs, increase profitability, improve functionality, minimised impact, confidentiality- integrity- availability, afield, progressive migration and implementation

Project Phases of Physical Architecture Analysis

1. Review of existing architecture
2. Analysis and design
3. Craft functional requirements
4. Functional requirements
5. Online final functional requirements
6. Proof of concept

Vendor selection

Architecture-workshop 1
Architecture-workshop 2
Presentation and discussion of functional requirements
Architecture-workshop 3
Delivery of Prototype

© Firebrand Training Ltd
ISACA CISA Certification | Certified Information Systems Auditor Courseware version 5
Hardware Acquisition

- Organisation type
- Requirement for data processing.
- Hardware requirements.
- System software application.
- Support system.
- Adaptability needs.
- Constraint.
- Conversion needs.

System Software Acquisition

- Business, technical, functional, collaborative needs.
- Security and reliability.
- Cost and benefits.
- Obsolescence and risk.
- System Compatibility.
- Resource allocation.
- Training and personnel requirements.
- Need for scalability.
- Impact on present infrastructure.
An IS auditor’s tasks in system development, acquisition and maintenance include:

- Determine the main components, objectives and user requirements of the system
- Determine and rank the major risks to, and exposures of, the system
- Identify controls to mitigate the risks to, and exposures of, the system
- Monitor the system development process
- Participate in post implementation reviews
- Test system maintenance procedures
- Evaluate the system maintenance process

Auditing Systems Development Acquisition

1. Feasibility study
2. Requirements definition
3. Software acquisition Process
4. Design & Development
5. Testing
6. Implementation and review
7. Post-Implementation
System Software Change Control Procedures

- Change management
  - RFC documents
  - Testing and auditing
  - Emergency changes
  - Unauthorised change control
- Configuration management

Application Controls
Application Controls

Application controls are controls over input, processing and output functions. They include methods for ensuring that:

- Only complete, accurate and valid data are entered and updated in a computer system
- Processing accomplishes the correct task
- Processing results meet expectations
- Data are maintained

Input/Origination Controls

- Input authorisation
- Batch controls and balancing
- Error reporting and handling
Processing Procedures and Controls

- Data validation and editing procedures
- Processing controls
- Data file control procedures

Output Controls

- Output controls provide assurance that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner.
Types of Output Controls

Output controls include:

- Logging and storage of negotiable, sensitive and critical forms in a secure place
- Computer generation of negotiable instruments, forms and signatures
- Report distribution
- Balancing and reconciling
- Output error handling
- Output report retention
- Verification of receipt of reports

Business Process Control Assurance

Specific matters to consider in business process control assurance are:

- Process maps
- Process controls
- Assessing business risks within the process
- Benchmarking with best practices
- Roles and responsibilities
- Activities and tasks
- Data restrictions
Auditing Application Controls

- Data integrity testing
  - Online Transaction Processing System
  - The ACID principle:
    - Atomicity
    - Consistency
    - Isolation
    - Durability
- Continuous Online audit

Application Testing

- Reasonableness checks
- Range checks (in range and out of range values)
- Stress testing
- Regression testing
- Parallel testing
- Functionality testing
- Security assurance testing
Precautions Regarding Testing

- Do not use sensitive production data
- Do not test in production
- Do not use production file names
- Ensure that all tests are completed
- Document the results of all tests for follow-up

System Change Procedures and the Program Migration Process

- An IS auditor should consider the following:
  - The use of a methodology for authorising, prioritising and tracking system change requests from the user
  - Document emergency change procedures in the operations manuals
  - Ensure that change control is a formal procedure for the user and the development groups
  - Whether the change control log ensures all changes shown were resolved
  - User satisfaction with the turnaround of change requests
  - Adequacy of the security access restrictions over production source and executable modules
System Change Procedures and the Program Migration Process (continued)

For a selection of changes on the change control log:

- Determine whether changes to requirements resulted in appropriate change-development documents
- Determine whether changes were made as documented
- Determine whether current documentation reflects the changed environment
- Evaluate the adequacy of the procedures in place for testing system changes
- Review evidence to ensure that procedures are carried out as prescribed by organisational standards
- Review the procedures established for ensuring executable and source code integrity

End of Chapter Three
ISACA®

Trust in, and value from, information systems

2016 CISA Review Course

Information Systems Operations, Maintenance and Service Management
Exam Relevance

Ensure that the CISA candidate...

- Understands and can provide assurance to users as well as management that the expected level of IT service will be delivered, per expectations derived from the organisation’s business objectives.

- The content area in this chapter will represent approximately 20% of the CISA examination

(approximately 40 questions)

Agenda

- Information Systems Operations
- Information Systems Hardware
- IS Architecture and Software
- IS Network Infrastructure
- Auditing Infrastructure and Operations
- Disaster Recovery Planning
Information Systems Operations

IT Service Management Frameworks

- A set of ideas or facts that provide support for the implementation of service management
- ITSM
- ITIL
- ISO20000-1:2011
- IT Service Delivery & support
- Tools to monitor effectiveness & efficiency of IT services
  - Exception reports
  - System & application logs
  - Operator problem reports
  - Operator work schedule
Information Systems Operations

* IS Operations
  - Job scheduling
  - Jobs that must be run
  - Sequence of job execution
  - Conditions that cause program execution

Information Systems Operations

* Incident & Problem Management
  - Incident handling process
  - Critical process within ITSM
  - Problem Management
  - Detection, documentation, control, resolution & reporting of abnormal conditions
Information Systems Operations

- Support / Help Desk
  - Common support functions
  - Fig 4.7 page 260
- Change Management Process
  - Covered in Domain 3

Information Systems Operations

- Release Management
  - Major releases
  - Minor software releases
  - Emergency software releases
  - Planning a release involves 8 steps
  - Difference between change management & release management
An asset is something of either tangible or intangible value that is worth protecting.

COBIT 5

- Manage IT assets through their life cycle to make sure their use delivers value at optimal cost.
Information Systems Hardware

Computer hardware components & architectures

- Processing components
- I/O components
- Common enterprise back-end devices
  - Print servers
  - File servers
- Types of computers
  - Application servers
  - Web servers
  - Proxy servers
  - Database servers
  - Appliances
- USB
  - Memory cards / flash drives
Information Systems Hardware

🌟 Computer hardware components & architectures

- Risks include
  - Viruses and other malicious software
  - Data theft
  - Data & media loss
  - Corruption of data
  - Loss of confidentiality

Information Systems Hardware

🌟 Computer hardware components & architectures

- Controls include
  - Encryption
  - Granular Control
  - Security personnel education
  - “Lock desktop” policy enforcement
  - Antivirus policy
  - Use of secure devices only
  - Inclusion of return-to-owner information
Information Systems Hardware

**Computer hardware components & architectures**

- Radio Frequency Identification
  - Tag
    - Microchip & Antenna
  - Power modes
    - Passive tags
    - Active tags
- Used in asset management, tracking, authentication, matching, process control, access control, SCM
- Risks
  - Business process, BI, privacy, externality risks
- Controls
  - Management, Operational, Technical

**Hardware Maintenance Programme**

- Requirements vary based on complexity & performance workloads
- Auditors should ensure
  - Formal maintenance plans have been developed, approved & are being followed
  - Maintenance costs are within budget and not excessive
  - Budget overruns may indicate lack of adherence to maintenance procedures
Information Systems Hardware

Hardware Monitoring Procedures

- Typical procedures & reports for monitoring effective & efficient use of hardware include:
  - Availability reports
  - Hardware error reports
  - Asset management reports
  - Utilisation reports

Information Systems Hardware

Capacity Management

- CPU utilization (processing power)
- Computer storage utilization
- Telecommunications, LAN & WAN bandwidth utilization
- I/O channel utilization
- Number of users
- New technologies
- New applications
- Service level agreements (SLAs)
- Vendor performance
Information Systems Operations

IS operations are in charge of the daily support of an organisation’s IS hardware and software environment.

IS operations include:
- Management of IS operations
- Infrastructure support including computer operations
- Technical support / help desk
- Information security management

Management of IS Operations

Operations management functions include:
- Resource allocation
- Standards and procedures
- IS operation processes monitoring
IT Service Management

- Service levels are auditing through review of:
  - Exception reports
  - System and application logs
  - Operator problem reports
  - Operator work schedules

Infrastructure Operations

- Audit
  - Scheduling
  - Race conditions
  - Maintenance windows
  - Job scheduling software
  - Mutual exclusivity
  - Concurrent operations and resource contention
Monitoring Use of Resources

- Process of incident handling
  - Is it followed....
  - Are lessons learned
  - Documented...

- Problem management
  - What is the mean time to clear trouble conditions

- Detection, documentation, control, resolution and reporting of abnormal conditions

IS Architecture and Software
IS Architecture and Software

- Operating systems
  - Software control features or parameters
- Access control software
- Data communications software
- Data management
- Database management system (DBMS)
- Tape and disk management system
- Utility programs
- Software licensing issues

IS Architecture and Software

- Operating Systems
  - Defines user interfaces
  - Permits users to share hardware
  - Permits users to share data
  - Inform users of any error
  - Permits recovery from system error
  - Communicates completion of a process
  - Allows system file management
  - Allows system accounting management
Operating Systems, (continued)

- Software control features or parameters
- Data management
- Resource management
- Job management
- Priority setting

Access control software

- Designed to prevent:
  - Unauthorised access to data
  - Unauthorised use of systems functions and programs
  - Unauthorised updates/changes to data
IS Architecture and Software

- **Data Communications Software**
  - Used to transmit messages or data from one point to another
  - Interfaces with the operating system, application programs, telecommunications systems, network control system

IS Architecture and Software

- **Data Management**
  - File Organisation
  - Sequential
  - Direct random access
IS Architecture and Software

Database Management Systems

- DBMS architecture
- Detailed DBMS metadata architecture
- Data dictionary / directory system (DD / DS)
- Database structure
- Database controls

Example of a database

- Referential and Entity Integrity
- View-based access control (most users cannot see author’s real name just the pseudonym)

<table>
<thead>
<tr>
<th>Author ID</th>
<th>P- Last Name</th>
<th>P- First Name</th>
<th>Real Last Name</th>
<th>Real First Name</th>
<th>State</th>
<th>Town</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Twain</td>
<td>Mark</td>
<td>Clemens</td>
<td>Samuel</td>
<td>Mi</td>
<td>Biloxi</td>
<td>Joe</td>
</tr>
<tr>
<td>2</td>
<td>Herriot</td>
<td>James</td>
<td>Krant</td>
<td>Ian</td>
<td>Yk</td>
<td>Durham</td>
<td>Pete</td>
</tr>
<tr>
<td>3</td>
<td>Grisham</td>
<td>John</td>
<td>Grisham</td>
<td>John</td>
<td>FL</td>
<td>Orlando</td>
<td>Alan</td>
</tr>
</tbody>
</table>
IS Architecture and Software

Tape and Disk Management Systems

- Tracks and lists tape / disk resources needed for data centre processing
- Minimizes computer operator time and errors
- Improve space efficiency by consolidating fragmented free spaces
- Provide inventory control over tapes, identification of offsite rotation of backup media and security features to control tape access

IS Architecture and Software

Utility programs

- 5 categories of functional use:
  - Understanding application systems
  - Assessing or testing data quality
  - Testing a program’s ability to function correctly and maintain data integrity
  - Assisting in faster program development
  - Improving operational efficiency
IS Architecture and Software

Software licensing issues

- Documented policies and procedures that guard against unauthorized use or copying of software
- Listing of all standard, used and licensed application and system software
- Centralizing control and automated distribution and the installation of software
- Requiring that all PCs be diskless workstations and access applications from a secured LAN
- Regularly scanning user PCs

Digital Rights Management

- DRM removes usage control from the person in possession of digital content & puts it in the hands of a computer program
- Prevents copying or modifying of data by unauthorised users
Network Infrastructure

- Telecommunications links for networks can be:
  - Analog
  - Digital

- Methods for transmitting signals over telecommunication links are:
  - Copper
  - Fibre
  - Coaxial
  - Radio Frequency
Enterprise Network Architectures

Today’s networks are part of a large, centrally-managed, inter-networked architecture solution high-speed local- and wide-area computer networks serving organisations’ distributed computing environments.

Types of Networks

- Personal area networks (PANs)
- Local area networks (LANs)
- Wide area networks (WANS)
- Metropolitan area networks (MANs)
- Storage area networks (SANs)
Network Services

- E-mail services
- Print services
- Remote access services
- Directory services
- Network management
- Dynamic Host Configuration Protocol (DHCP)
- DNS

Network Standards and Protocols

- Critical success factors:
  - Interoperability
  - Availability
  - Flexibility
  - Maintainability
OSI Architecture

ISO / OSI
- Is a proof of a concept model composed of seven layers, each specifying particular specialised tasks or functions

Objective
- To provide a set of open system standards for equipment manufacturers and to provide a benchmark to compare different communication systems

OSI Architecture (continued)

Functions of the layers of the ISO / OSI Model
- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer
Application of the OSI Model in Network Architectures (continued)

Network Architectures

© Firebrand Training Ltd
ISACA CISA Certification | Certified Information Systems Auditor Courseware version 5
Network Components

- Repeaters
- Hubs
- Bridges
- Switches
- Routers

Communications Technologies

- Message switching
- Packet switching
- Circuit switching
- Virtual circuits
  - PVC
- Dial-up services
Communications Technology (continued)

- Point to point - leased lines
- X.25
- Frame Relay
- Integrated services digital network (ISDN)
- Asynchronous transfer mode
- Multiprotocol label switching
- Digital subscriber lines
- Virtual Private Networks

Wireless Networking

- Wireless networks
- Wireless wide area network (WWAN)
  - Microwave, Optical
- Wireless local area network (WLAN)
  - 802.11
- Wireless personal area network (WPAN)
  - 802.15 Bluetooth
- Wireless ad hoc networks
- Wireless application protocol (WAP)
Risks Associated with Wireless Communications

- Wireless access: exposures
  - Interception of sensitive information
  - Loss or theft of devices
  - Misuse of devices
  - Loss of data contained in devices
  - Distraction caused by devices
  - Wireless user authentication
  - File security
  - Wireless encryption
  - Interoperability
  - Use of wireless subnets
  - Translation point

Internet Technologies

- TCP / IP Internet world wide web services
  - URL
  - Common gateway scripts
  - Cookie
  - Applets
  - Servlets
  - Bookmark
Auditing Infrastructure and Operations

Auditing of Network Management

- Network administration and control
  - Network performance metrics
  - Capacity
  - Errors
  - Network management issues
Auditing of Applications Management

- Applications in a networked environment
  - Client-server technology
  - Middleware
  - Cloud
  - Virtual
  - Software as a Service
  - Service Oriented architecture

Hardware Reviews

- Audits of Hardware include:
  - Acquisition process
  - Configuration
  - Maintenance / upgrades
  - Operational procedures
  - Monitoring
Operating System Reviews

- Audits of Operating Systems include:
  - Patch management
  - Configuration - hardening
  - Access controls

Database Reviews

- Audits of Databases include:
  - Schemas
  - Efficiency of processing
  - Security
    - Views
    - Updates
  - Backups
  - Access controls
Network Infrastructure and Implementation Reviews

🌟 Review controls over network equipment
- Physical controls
- Protected cabling - conduit
- Locked equipment rooms
- Environmental controls
- Server Rooms
- Access control
- Fire detection and suppression

Network Infrastructure and Implementation Reviews

🌟 Logical security controls
- Network User and Administrator Access & Passwords
- Network Access Change Requests
- Test Plans
- Security Reports
- Performance and monitoring
Physical Security Audits

Physical Controls
- Access control
- Lock and Key management
- Positive pressurization
- Contaminant-free air
- Humidity controls
- Power supply
- UPS load and maintenance

Access Controls Review

Logical Security Control: Questions to Consider:
- Are users assigned unique passwords?
- Are users required to change the passwords on a periodic basis?
- Are passwords encrypted and not displayed on the computer screen when entered?
- Is network user access based on written authorisation and given on a need-to-know basis and based on the individual’s responsibilities?
Access Controls Review (continued)

Logical Security Control: Questions to Consider:
- Are network workstations automatically disabled after a short period of inactivity?
- Is remote access monitored and secure?
- Are all login attempts to the system logged?
- Are all activities by administrators logged?

Scheduling Reviews

Areas to Review:
- Regularly scheduled applications
- Input deadlines
- Data preparation time
- Estimated processing time
- Output deadlines
- Procedures for collecting, reporting and analysing key performance indicators
- Are the items included in SLAs?
- Are the items functioning according to the SLAs?
Scheduling Reviews; Questions to Consider

- Job schedule reviews;
  - Have critical applications been identified and granted highest priority
  - Is schedule of rush/rerun jobs consistent with their assigned priority?
  - Do scheduling procedures facilitate optimal use of computer resources while meeting services requirements?
  - Do operators record jobs that are completed, to be processed and the required job completion codes?

Auditing Job Scheduling

- Daily Job Schedule;
  - Are the number of personnel assigned to each shift adequate to support the workload?
  - Are operations procedures and schedules being followed
  - Do the operators record any critical activity and alert next shift to any outstanding issues
Job Scheduling Reviews

- Exception handling logs;
  - Do operators require written or electronic approval for exceptions?
  - Are all exceptions documented?
  - Are error codes recorded
  - Are exception and error logs reviewed for further action

Personnel Reviews

- Personnel;
  - Does the operations and administration staff have adequate training and skills
  - Is management providing proper oversight for operations staff
  - Is separation of duties enforced
Disaster Recovery Planning
BCP/DRP Audits

Auditing of Business Continuity Plans

- Is the plan reasonable
  - Does the plan reflect business priorities
  - Does Management support the plan
- Is the Business Impact Analysis (BIA) current
- Are regular tests being performed
- Are lessons learned being applied
- Is the plan kept up to date
Recovery Point Objective and Recovery Time Objective

- **Recovery Point Objective (RPO)**
  - Based on acceptable data loss
  - Indicates the most current state of data that can be recovered

- **Recovery Time Objective (RTO)**
  - Based on acceptable downtime
  - Indicates the point in time at which the business plans to resume sustainable service levels after a disaster

Business Continuity Strategies

- Additional parameters important in defining recovery strategies
  - Interruption window
  - Service delivery objective (SDO)
  - Maximum tolerable outages
Recovery Strategies

A recovery strategy is a combination of preventive, detective and corrective measures.

The selection of a recovery strategy would depend upon:
- The criticality of the business process and the applications supporting the processes
- Cost
- Time required to recover
- Security

Recovery Alternatives

Types of offsite backup facilities
- Cold sites
- Mobile sites
- Warm sites
- Reciprocal agreements
- Hot sites
- Mirrored sites
- Reciprocal agreements
Audit of Third Party Recovery Agreements

Provisions for use of third-party sites should cover:

- Configurations
- Disaster declaration
- Access
- Priority
- Availability
- Speed of availability
- Subscribers per site and area
- Preference
- Insurance
- Usage period
- Communications
- Warranties
- Audit
- Testing
- Reliability
- Security

Organisation and Assignment of Responsibilities

Have recovery teams been set up to:

- Retrieve critical and vital data from offsite storage
- Install and test systems software and applications at the systems recovery site
- Acquire and install hardware at the system recovery site
- Operate the system recovery site
Team Responsibilities

- Manage the disaster
  - Rerouting communications traffic
  - Re-establish the local area user/system network
  - Transport users to the recovery facility
  - Restore databases, software and data
  - Supply necessary office goods, i.e., special forms, paper

Backup and Restoration

- Offsite library controls
- Security and control of offsite facilities
- Media and documentation backup
- Periodic backup procedures
- Frequency of Rotation
- Types of Media and Documentation Rotated
- Backup Schemes
- Method of Rotation
End of Domain
ISACA®
Trust in, and value from, information systems

2016 Firebrand CISA® Review Course
Chapter 5 - Protection of Information Assets
Exam Relevance

Ensure that the CISA candidate...

- “Understands and can provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.”

- The content area in this chapter will represent approximately 25% of the CISA examination (approximately 38 questions)

Course Agenda

- Learning Objectives
- Information Security Management
- Access Controls
- Equipment and Network Security
- Encryption
- Malware
- Incident Handling and Evidence
- Physical and Environmental Controls
Chapter 5 Task Statements

- Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices
- Evaluate the design, implementation and monitoring of system and logical security controls
- Verify the confidentiality, integrity and availability of information and information systems
- Evaluate the design, implementation and monitoring of the data classification processes and procedures

Chapter 5 Task Statements (continued)

- Evaluate physical access and environmental controls to determine whether information assets are adequately safeguarded
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets
  - Backup media
  - Offsite storage
  - Hard copy/print data
  - Electronic data
Knowledge Areas

The CISA candidate is expected to be familiar with auditing the controls related to:

• Security Awareness
• Incident handling
• Identification, Authentication and Authorisation
• Hardware and Software-based security controls

Knowledge Areas (continued)

The CISA candidate is expected to be familiar with auditing the controls related to:

• Virtualization
• Network security
• Internet protocols and security
• System attacks and Malware
• Intrusion detection, vulnerability scanning
• Data leakage
• Encryption and public key infrastructure
• Social networking risks
Knowledge Areas (continued)

The CISA candidate is expected to be familiar with auditing the controls related to:

- Mobile and wireless security
- Voice communications
- Evidence preservation (forensics)
- Data classification
- Physical and environmental security

Information Security Management
Importance of Information Security Management

- Security objectives to meet organisation’s business requirements include:
  - Ensure the availability, integrity and confidentiality of information and information systems
  - Ensure compliance with laws, regulations and standards

Key Elements of Information Security Management

- Key elements of information security management:
  - Senior management commitment and support
  - Policies and procedures
  - Organisation
  - Security awareness and education
  - Monitoring and compliance
  - Incident handling and response
Critical Success Factors to Information Security Management

- Strong commitment and support by the senior management on security training
- Professional risk-based approach must be used systematically to identify sensitive and critical resources

Inventory and Classification of Information Assets

- The inventory record of each information asset should include:
  - Identification of assets
  - Relative value of assets to the organisation
  - Location (where the asset is located)
  - Security / risk classification
  - Asset group
  - Owner
  - Designated custodian
Privacy Management Issues and the Role of IS Auditors

- Pinpoint the nature of personally identifiable information (pii) associated with business processes:
  - Identify identifiable information (pii) associated with business processes
  - Document the collection, use, disclosure and destruction of personally identifiable information
  - Ensure that accountability for privacy issues exists
  - Set the foundation for informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk

Privacy Management Issues and the Role of IS Auditors (continued)

Compliance with privacy policy and laws

- Identify and understand legal requirements regarding privacy from laws, regulations and contract agreements
- Check whether personal data are correctly managed in respect to these requirements
- Verify that the correct security measures are adopted
- Review management’s privacy policy to ascertain that it takes into consideration the requirement of applicable privacy laws and regulations.
Social Media Risks

- Inappropriate sharing of information
  - Organisational activity
  - Staffing issues
  - Privacy-related sensitive data
- Installation of vulnerable applications

Access Controls
System Access Permission

- Who has access rights and to what?
- What is the level of access to be granted?
- Who is responsible for determining the access rights and access levels?
- What approvals are needed for access?

Mandatory and Discretionary Access Controls

- Mandatory
  - Enforces corporate security policy
  - Compares sensitivity of information resources
- Discretionary
  - Enforces data owner-defined sharing of information resources
IAAA

Identification
- Method to distinguish each entity in a unique manner that is accessing resources

Authentication
- Validate, verify or prove the identity

Authorisation
- Rights, permissions, privileges granted to an authenticated entity

Accounting (Audit) - track all activity

Authentication

Knowledge
- Password, passphrase

Ownership / possession
- Smartcard, token, key fob

Characteristic
- Biometrics
Authorisation

- Need to know
- Least privilege
- Mutual exclusivity
- Dual control
- Separation of duties
- Time limited (hours of work etc.)

Authorisation Issues

- Access restrictions at the file level include:
  - Read, inquiry or copy only
  - Write, create, update or delete only
  - Execute only
  - A combination of the above
Challenges with Identity Management

- Many changes to systems and users
- Many types of users - employees, customers, guests, managers, regulators
- Audit concerns
  - Unused IDs
  - Misconfigured IDs
  - Failure to follow procedures
  - Group IDs

Identification and Authentication

- I&A common vulnerabilities:
  - Weak authentication methods
  - Lack of confidentiality and integrity for the stored authentication information
  - Lack of encryption for authentication and protection of information transmitted over a network
  - User’s lack of knowledge on the risks associated with sharing passwords, security tokens, etc.
Logical Access Exposures

Technical exposures include:

- Data leakage
- Wire tapping
- Trojan horses / backdoors
- Viruses
- Worms
- Logic bombs
- Denial-of-service attacks
- Computer shutdown
- War driving
- Piggybacking
- Trap doors
- Asynchronous attacks
- Rounding down
- Salami technique

Paths of Logical Access

General points of entry:

- Network connectivity
- Remote access
- Operator console
- Online workstations or terminals
Logical Access Control Software

- Prevent unauthorised access and modification to an organisation’s sensitive data and use of system critical functions
- General operating and/or application systems access control functions include the following:
  - Create or change user profiles
  - Assign user identification and authentication
  - Apply user logon limitation rules
  - Notification concerning proper use and access prior to initial login
  - Create individual accountability and auditability by logging user activities. Establish rules for access to specific information resources (e.g., system-level application resources and data)
  - Log events
  - Report capabilities

Logical Access Control Software (continued)

- Database and/or application-level access control functions include:
  - Create or change data files and database profiles
  - Verify user authorisation at the application and transaction levels
  - Verify user authorisation within the application
  - Verify user authorisation at the field level for changes within a database
  - Verify subsystem authorisation for the user at the file level
  - Log database/data communications access activities for monitoring access violations
Auditing Logical Access

When evaluating logical access controls the IS auditor should:

- Identify sensitive systems and data
- Document and evaluate controls over potential access
- Test controls over access paths to determine whether they are functioning and effective
- Evaluate the access control environment to determine if the control objectives are achieved
- Evaluate the security environment to assess its adequacy

Access Control Lists

Access control lists (ACLs) provide a register of:

- Users who have permission to use a particular system resource
- The types of access permitted
Centralised versus Decentralised Access

- Logical access security administration:
  - Centralised environment
  - Decentralised environment

- Advantages of conducting security in a decentralised environment:
  - Security controls are monitored frequently
  - Security administration is onsite at the distributed location
  - Security issues resolved in a timely manner

Decentralised Access Risks

- Risks associated with distributed responsibility for security administration:
  - Local standards might be implemented rather than those required
  - Levels of security management might be below what can be maintained by central administration
  - Unavailability of management checks and audits
Single Sign-on (SSO)

- Single sign-on (SSO)
  - Consolidating access functions for multiple systems into a single centralised administrative function
  - A single sign-on interfaces with:
    - Client-server and distributed systems
    - Mainframe systems
    - Network security including remote access mechanisms

Single Sign-on Advantages

- Single sign-on (SSO) advantages:
  - Elimination of multiple user IDs and passwords
  - May select a stronger password
  - It improves an administrator’s ability to centrally manage users’ accounts and authorisations
  - Reduces administrative overhead
  - Greater access consistency between systems
  - It reduces the time taken by users to log into multiple applications and platforms
Single Sign-on Disadvantages

- Single sign-on (SSO) disadvantages:
  - May not support legacy applications or all operating environments
  - The costs associated with SSO development can be significant
  - The centralised nature of SSO presents the possibility of a single point of failure and total compromise of an organisation’s information assets

Familiarisation with the Organisation’s IT Environment

- Every layer of a system has to be reviewed for security controls including:
  - The network
  - Operating system platform
  - Applications software
  - Database
  - Physical and environmental security
Remote Access

Remote access security:

Today’s organisations require remote access connectivity to their information resources for different types of users such as employees, vendors, consultants, business partners and customer representatives.

- Consolidated
- Monitored
- Policies
- Appropriate access levels
- Encrypted

Remote Access Security

Remote access security risks include:

- Denial of service
- Malicious third parties
- Misconfigured communications software
- Misconfigured devices on the corporate computing infrastructure
- Host systems not secured appropriately
- Physical security issues on remote users’ computers
Auditing Remote Access

- Assess remote access points of entry
  - Test dial-up access controls
  - Test the logical controls
  - Evaluate remote access approaches for cost-effectiveness, risk and business requirements

Auditing Remote Access (continued)

- Audit Internet points of presence:
  - E-mail
  - Marketing
  - Sales channel / electronic commerce
  - Channel of deliver for goods / services
  - Information gathering
Logging All System Access

Audit logging and monitoring system access:

• Provides management an audit trail to monitor activities of a suspicious nature, such as a hacker attempting brute force attacks on a privileged logon ID
• Record all activity for future investigation

Equipment and Network Security
Security of Portable Media

- Use of approved portable devices
  - PDAs
  - IPADs, IPODs, and similar units

Security and Audit Issues:
  - Sensitive data stored on unsecured devices
  - Loss, theft, insecure configuration
  - Passwords, encryption

Mobile Device Security

- Access issues with mobile technology:
  - Control use via policy
  - Restrict use of portable drives, memory
  - Disable USB access
  - Encrypt all data transported or saved by these devices
Storing, Retrieving, Transporting and Disposing of Confidential Information

Policies required for:

- Backup files of databases
- Databases
- Disposal of media previously used to hold confidential information
- Management of equipment sent for offsite maintenance
- Public agencies and organisations concerned with sensitive, critical or confidential information
- E-token electronic keys
- Storage records

Concerns Associated with Storage Media

Preserving information during shipment or storage:

- Protect from direct sunlight, liquids, dust, magnetic fields
- Encryption
- Labelling
- Tracking
Network Infrastructure Security

Communication network controls:
• Employ skilled administration staff
• Separation of duties
• Restrict administrator level access
• Record all administrator level activity
• Review audit trails detect any unauthorised network operations activities

Network Infrastructure Security (Continued)

Communication network controls (continued)
• Create and enforce operational procedures
• Monitor unauthorised access or activity by administrators or other staff
• Ensure fast response time to trouble tickets
• Monitor for system efficiency
• Identify all assets connecting to the network - people, processes and equipment
• Use data encryption to protect sensitive messages from disclosure during transmission
LAN Security Issues

The IS auditor should identify and document:

- LAN topology and network design
- Segmentation
- LAN administrator / LAN ownership
- Functions performed by the LAN admin
- Distinct groups of LAN users
- Applications used on the LAN
- Procedures and standards relating to network design, support, naming conventions and data security

Client-server Security

- Control techniques in place
- Securing access to data or application
- Use of network monitoring devices
- Data encryption techniques
- Authentication systems
- Use of application level access control programs
- Protection of end devices
Wireless Security Threats

- Unauthorised equipment
- Misconfigured equipment
  - WEP, WPA, WPA2
- Radio frequency management
- Unauthorised access
- Interference and denial of service

Wireless Security Threats (continued)

- Malicious access to WLANs:
  - War driving
  - War walking
  - War chalking
  - Passive attacks
  - Sniffing
Audit Log Analysis Tools

- Tools for audit trails (logs) analysis:
  - Audit reduction tools
  - Trends/variance-detection tools
  - Attack signature-detection tools

Internet Threats and Security

- Active attacks:
  - Brute-force attack
  - Masquerading
  - Packet replay
  - Phishing
  - Message modification
  - Unauthorised access through the Internet or web-based services

- Denial of service
- Penetration attacks
- E-mail spamming
- E-mail spoofing
- Web Application attack
- SQL Injection
- Cross Site Scripting
- Buffer overflows
Causes of Internet Attacks

- Freely available tools and techniques
- Lack of security awareness and training
- Exploitation of security vulnerabilities
- Poor Configuration of network equipment
- Lack of encryption

Firewalls

- Firewall security systems
- Firewall general features
- Firewall types
  - Router packet filtering
  - Application firewall systems
  - Stateful inspection
  - Proxies
Firewall Issues

- Firewall issues
  - A false sense of security
  - The circumvention of firewall
  - Misconfigured firewalls
  - Monitoring activities may not occur on a regular basis
  - Firewall policies

Network Security Architecture

- Network Segmentation
  - Firewalls
  - Gateways
  - VLANs
  - Screened-host firewall
  - Dual-homed firewall
  - Demilitarized zone (DMZ)
Honeypots and Honeynets

- Provide a distraction for hackers
- May present a real environment to attack (high interaction systems)
- Record all activity
- Learn hacking methods and techniques

Intrusion Detection and Prevention Systems

- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Host, network or application based
IDS / IPS Components

- Sensors that are responsible for collecting data
- Analysers that receive input from sensors and determine intrusive activity
- An administration console
- A user interface
- IDS / IPS types include:
  - Signature-based
  - Statistical-based
  - Neural networks

IDS / IPS Features

- Intrusion detection
- Gathering evidence on intrusive activity
- Automated response
- Security monitoring
- Interface with system tools
- Security policy management
Voice-Over IP (VoIP)

- VoIP security issues:
  - Inherent poor security
  - Internet architecture does not provide the same physical wire security as the phone lines (shared lines versus private lines)

- The key to securing VoIP
  - Security mechanisms such as those deployed in data networks (e.g., firewalls, encryption) to provide security
  - Proper configuration of equipment

Techniques for Testing Security

- Vulnerability Scanning
- Penetration testing
- Internal versus external
- Enumerate and attempt to exploit system vulnerabilities
- Web applications
- Operating systems
- Physical
Auditing Network Infrastructure Security

- Review network diagrams and implementation
- Evaluate compliance with applicable security policies, standards, and procedures
- Ensure network connections are secure and properly monitored and managed
- Identify possible attacks and misuse
- Review service level agreements (SLAs)
- Ensure backups are being done and tested
**Encryption Definition**

- Altering data in storage or transit so that it cannot be understood by unauthorised personnel
- Converts a plaintext message into a form of ciphertext using a key known only to authorised personnel
- Substitution
- Transposition

**Encryption**

- Key elements of encryption systems
  - Encryption algorithm
  - Encryption key
  - Key length
- Private key cryptographic systems
- Public key cryptographic systems
Symmetric Encryption

- Use the same (shared) key to both encrypt and decrypt a message

Characteristics

- Fast, Confidentiality, good for bulk message and streaming media encryption

Examples:

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Asymmetric Algorithms

- Mathematically related key pair
  - Private key kept private by owner
  - Public key can be distributed freely
  - May use certificates to distribute public keys (PKI to be seen later)

- Benefits
  - Confidentiality, access control, non-repudiation, authenticity, integrity

- Disadvantages
  - Slow

- Examples - RSA, Diffie-Hellman, Elliptic Curve (ECC)
Hashing Algorithms

- Used for message integrity
  - Calculates a digest of the message
  - Can be validated by the receiver to ensure the message was not changed in transit or storage
- Examples: MD5, SHA-1, SHA256

Digital Signatures

- Digital signatures:
  - Data integrity
  - Authentication
  - Nonrepudiation
  - Replay protection
- Created by signing a hash of a message with the private key of the sender
Digital Envelope

Digital envelope:
- Used to send encrypted information and the relevant key along with it.
- The message to be sent, can be encrypted by using either:
  - Asymmetric key
  - Symmetric key

Public Key Infrastructure (PKI)

- Digital certificates
- Certificate authority (CA)
- Registration authority (RA)
- Certificate revocation list (CRL)
- Certification practice statement (CPS)
Uses of Encryption in Communications

- Use of encryption in OSI protocols:
  - Secure sockets layer (SSL)
  - Secure Hypertext Transfer Protocol (S/HTTP)
  - IP security
  - SSH
  - Secure multipurpose Internet mail extensions (S/MIME)
  - PCI-DSS (payment card industry)

Auditing Encryption Implementations

- Key management
  - Storage
  - Key history and retention
  - Changing keys
  - Strong keys
  - Performance
  - User training
Malware

Viruses

- Various types of viruses. Attack:
  - Executable program files
  - The file directory system, which tracks the location of all the computer’s files
  - Boot and system areas, which are needed to start the computer
  - Data files
## Viruses Protection

- Policies
- Education
- Patch management
- Procedural controls
- Technical controls
- Anti-virus software implementation strategies

## Other Forms of Malware

- Worms
- Trojan Horses
- Logic Bombs
- Spyware / Adware
- Keystroke Loggers
- Botnets / Zombies
Incident Handling and Evidence

Security Incident Handling and Response

- Planning and preparation
- Detection
- Initiation
- Recording
- Evaluation
- Containment
- Eradication
- Escalation
- Response
- Recovery
- Closure
- Reporting
- Post incident review
- Lessons learned
Evidence Handling

- Obtain all evidence associated with an incident
- Chain of Custody
  - Protection from alteration / unauthorised access
  - Documented
  - Secure copies
  - Bit level images of media

Physical and Environmental Controls
Physical Access Issues and Exposures

- Unauthorised entry
- Damage, vandalism or theft to equipment or documents
- Copying or viewing of sensitive or copyrighted information or intellectual property
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources
- Blackmail
- Embezzlement

Possible perpetrators include employees who are:
- Disgruntled
- On strike
- Threatened by disciplinary action or dismissal
- Addicted to a substance or gambling
- Experiencing financial or emotional problems
- Notified of their termination
### Physical Access Controls

<table>
<thead>
<tr>
<th>Control Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bolting door locks</td>
</tr>
<tr>
<td>Combination door locks (cipher locks)</td>
</tr>
<tr>
<td>Electronic door locks</td>
</tr>
<tr>
<td>Biometric door locks</td>
</tr>
<tr>
<td>Manual logging</td>
</tr>
<tr>
<td>Electronic logging</td>
</tr>
<tr>
<td>Identification badges (photo IDs)</td>
</tr>
<tr>
<td>Video cameras</td>
</tr>
<tr>
<td>Security guards</td>
</tr>
<tr>
<td>Controlled visitor access</td>
</tr>
<tr>
<td>Bonded personnel</td>
</tr>
<tr>
<td>Deadman doors</td>
</tr>
<tr>
<td>Not advertising the location of sensitive facilities</td>
</tr>
<tr>
<td>Computer workstation locks</td>
</tr>
<tr>
<td>Controlled single entry point</td>
</tr>
<tr>
<td>Alarm system</td>
</tr>
<tr>
<td>Secured report / document distribution cart</td>
</tr>
<tr>
<td>Windows</td>
</tr>
</tbody>
</table>

### Controls for Environmental Exposures

<table>
<thead>
<tr>
<th>Control Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm control panels</td>
</tr>
<tr>
<td>Water detectors</td>
</tr>
<tr>
<td>Handheld fire extinguishers</td>
</tr>
<tr>
<td>Manual fire alarms</td>
</tr>
<tr>
<td>Smoke detectors</td>
</tr>
<tr>
<td>Fire suppression systems</td>
</tr>
<tr>
<td>Strategically locating the computer room</td>
</tr>
<tr>
<td>Regular inspection by fire department</td>
</tr>
</tbody>
</table>
Controls for Environmental Exposures (continued)

- Fireproof walls, floors and ceilings of the computer room
- Electrical surge protectors
- Uninterruptible power supply / generator
- Emergency power-off switch
- Power supply leads from two substations

Controls for Environmental Exposures (continued)

- Wiring placed in electrical panels and conduit
- Restricted activity within secure areas
- Access, equipment, cameras, phones
- Fire-resistant building materials
- Documented and tested emergency evacuation plans
Electrical Problems

Power failures:
- Total failure (blackout)
- Severely reduced voltage (brownout)
- Sags, spikes and surges
- Electromagnetic interference (EMI)

Auditing Physical Access

- Touring the information processing facility (IPF)
- Testing of physical safeguards
  - Locks, fire equipment, access control procedures
- Regular tests of backup power systems
Mobile Computing Controls

- Mobile Device Vulnerabilities, Threats and Risks - fig 5.24
- Device registration
- Tagging
- Physical security
- Data storage
- Virus detection and control
- Encryption
- Compliance
- Approval
- Acceptable use policy

Mobile Computing Controls (continued)

- Due care
- Awareness training
- Network authentication, authorisation & accounting
- Secure transmission
- Standard mobile device applications
- Geolocation tracking
- Remote wipe and lock
- BYOD agreements
- Secure remote support
Peer-to-peer Computing

- Distributed architecture where tasks or workloads are shared between peers
- Used almost exclusively for file sharing
- P2P computing threats, vulnerabilities, risks & controls - fig. 5.28

Cloud Computing

- Anything-as-a-service
- Multiple models
  - Private
  - Public
  - Community
  - Hybrid
- Risks & Controls - fig. 5.29
Data Leakage

- DLP
  - Data at rest
  - Data in motion
  - Data in use (endpoint)
  - Policy creation & management
  - Directory services integration
  - Workflow management
  - Backup & restore
  - Reporting

DLP Risks, Limitations & Considerations

- Improperly tuned network DLP modules
- Excessive reporting & false positives
- Encryption
- Graphics
Practice Question

1 Which of the following BEST provides access control to data being processed on a local server?
1. Logging all access to sensitive information
2. Using strong passwords for sensitive transactions
3. Deploying software that restricts access to authorised staff
4. Restricting system access to business hours

Practice Question

2 An organisation is proposing to install a single sign-on facility giving access to all systems. The organisation should be aware that:
1. Disclosure of a password would grant maximum unauthorised access.
2. User access rights would be restricted by the additional security parameters.
3. The security administrator’s workload would increase.
4. Systems may require different levels of access control
Practice Question

3 Which of the following is the MOST effective antivirus control?

1. Scanning e-mail attachments on the mail server
2. Use of virtual environments
3. Disabling USB ports
4. An online antivirus scan with up-to-date virus definitions