Your fastest way to learn. Why wait?
FIREBRAND

ISACA

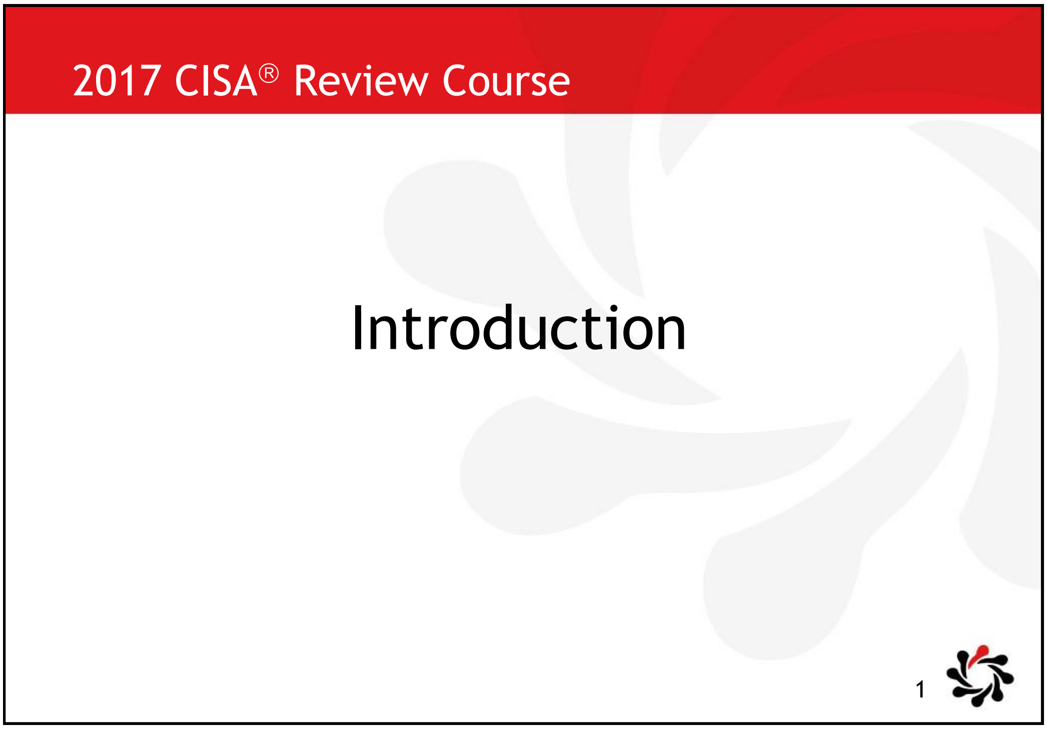
CISA Certification

Certified Information Systems Auditor Courseware

Courseware version 6.1

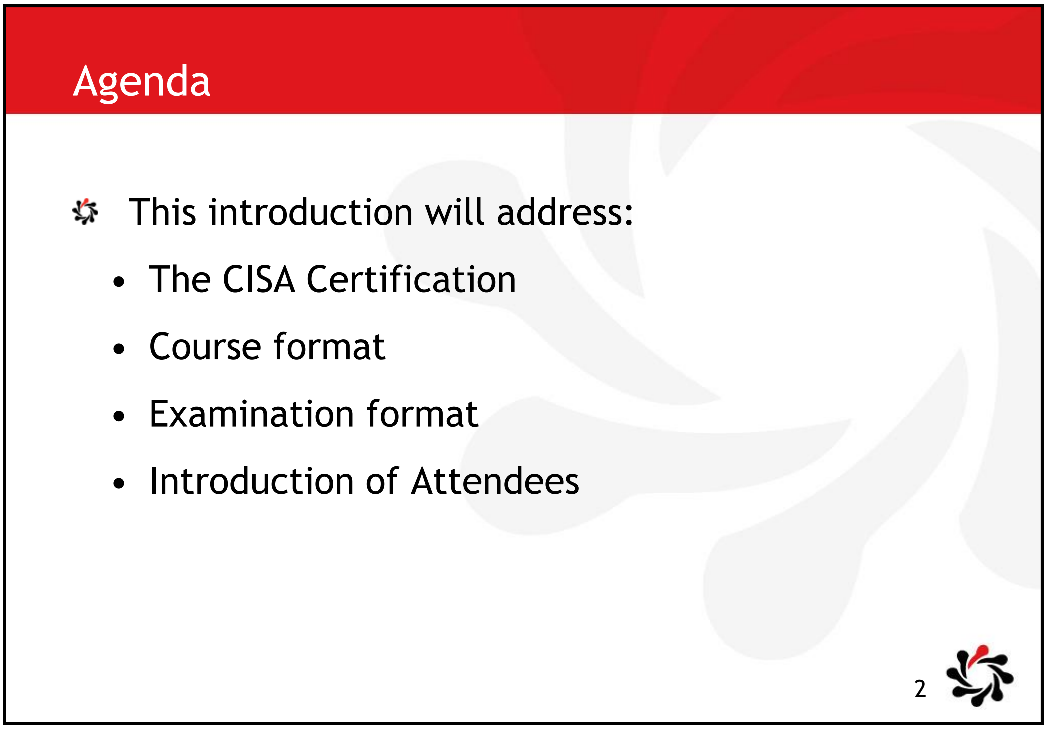
Kit Code: K-115-01

www.firebrandtraining.co.uk



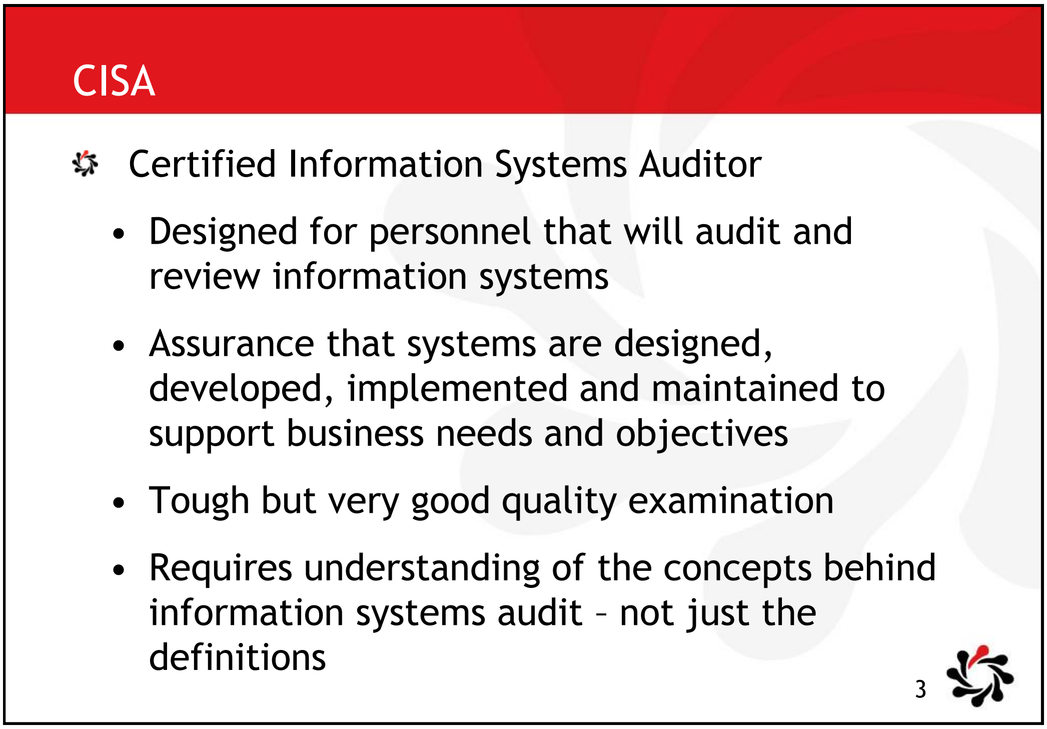
2017 CISA® Review Course

Introduction



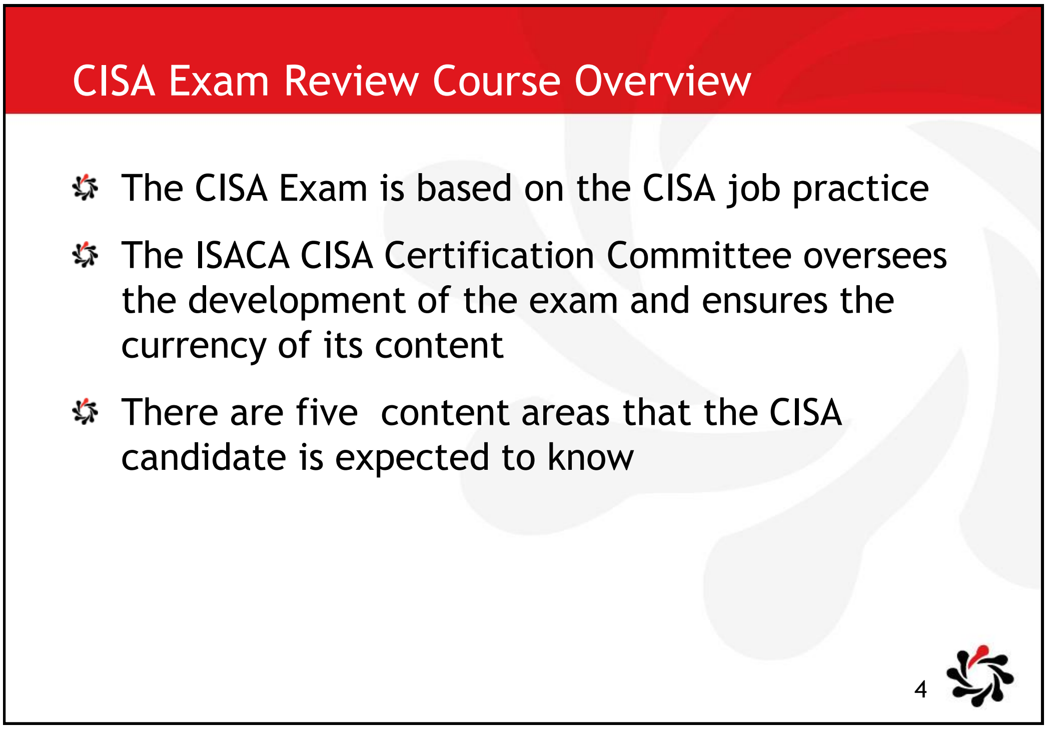
Agenda

- This introduction will address:
  - The CISA Certification
  - Course format
  - Examination format
  - Introduction of Attendees



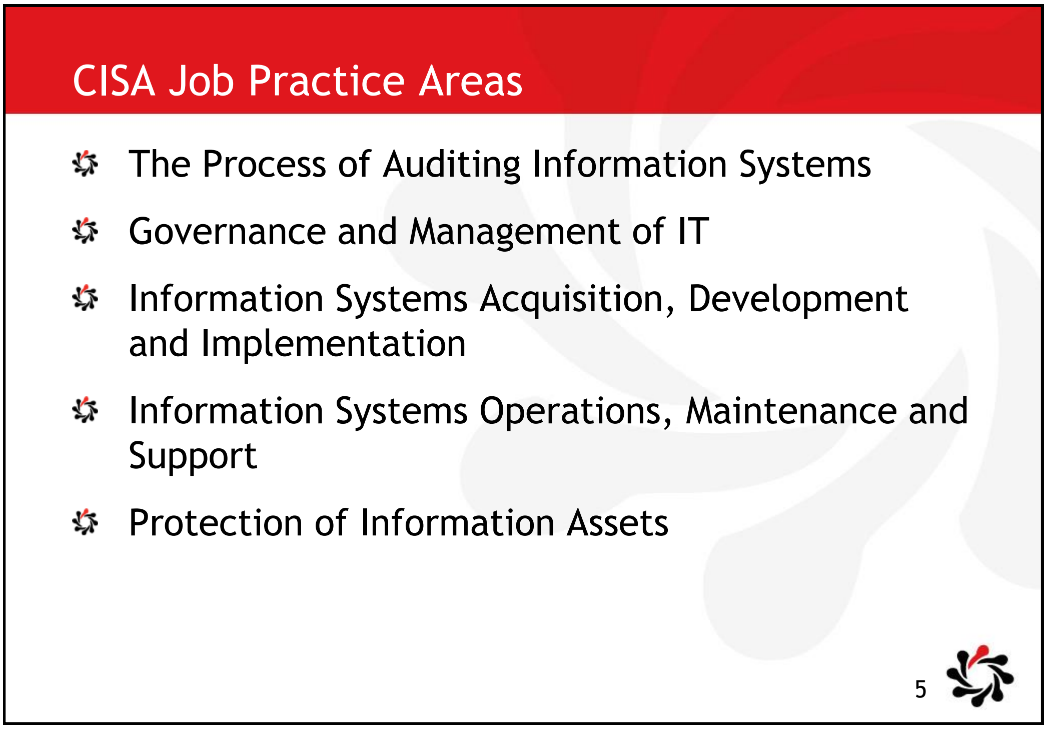
CISA

- 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



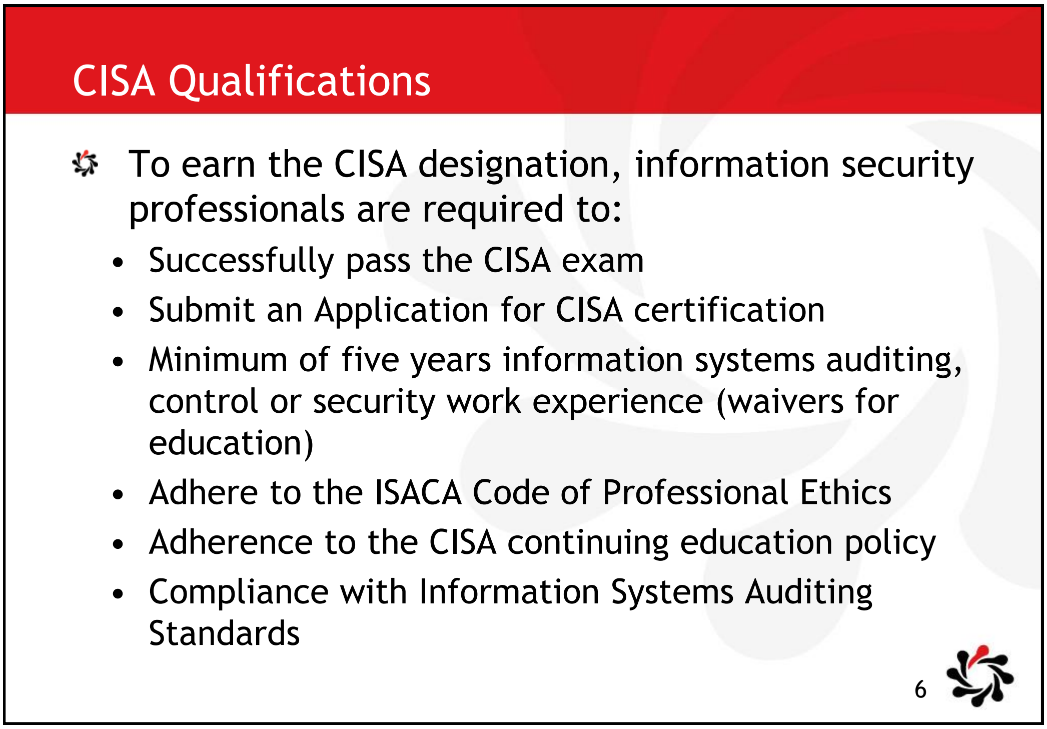
CISA Exam Review Course Overview

- 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



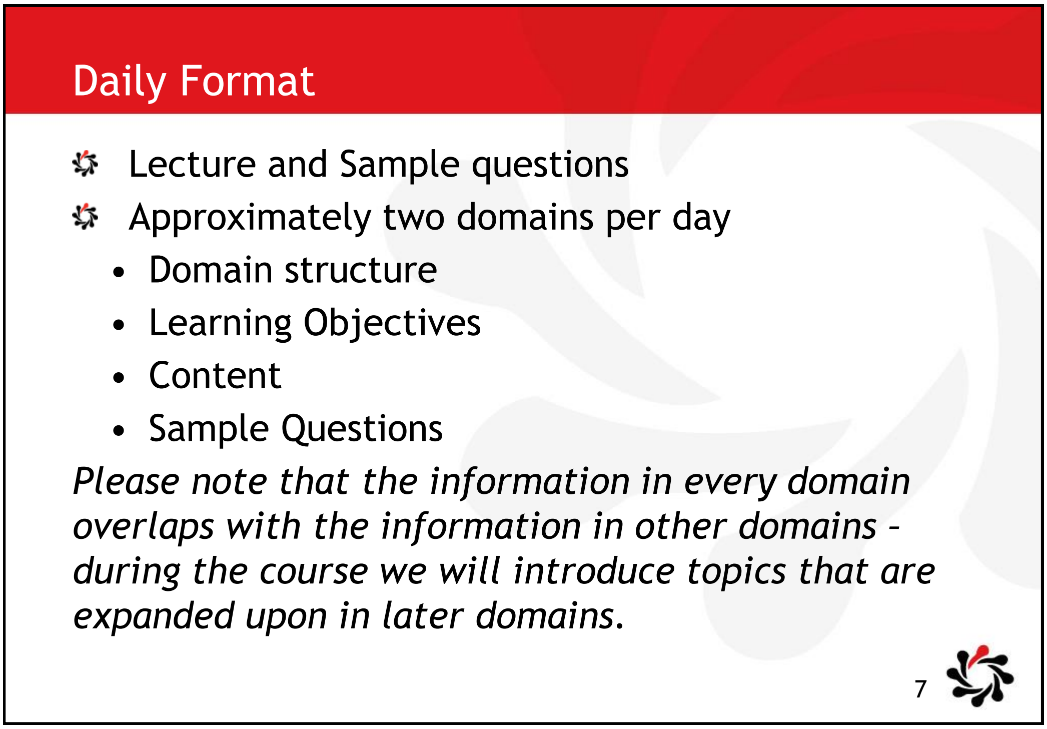
CISA Job Practice Areas

- 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

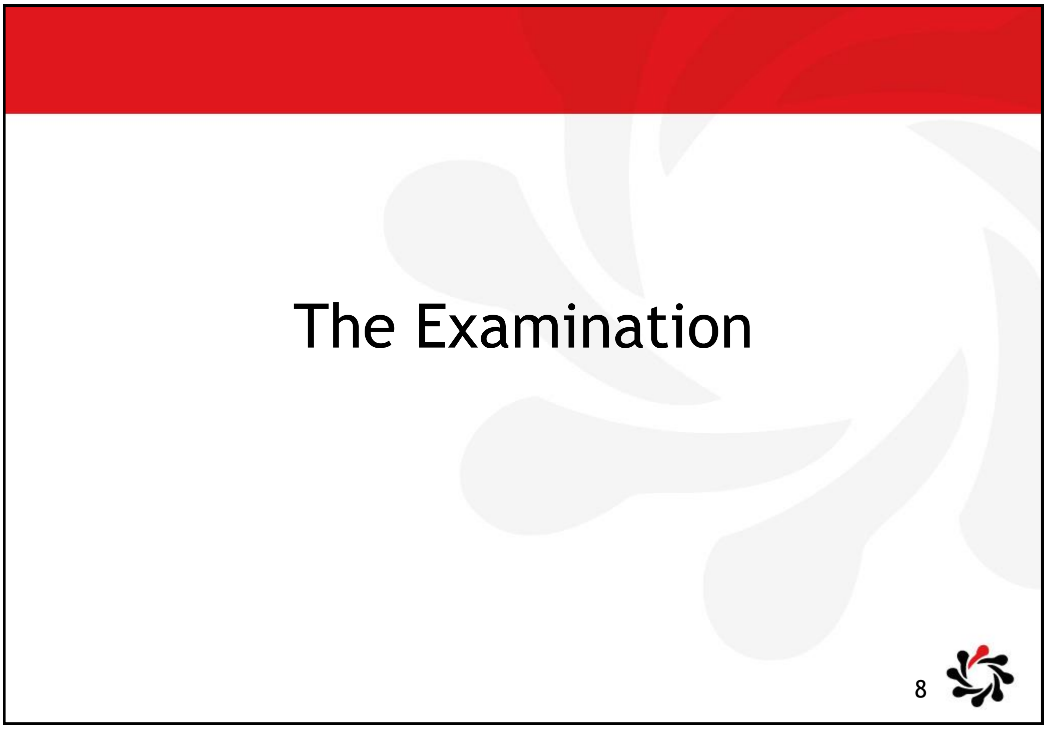
- To earn the CISA designation, information security professionals are required to:
  - Successfully pass the CISA exam
  - Submit an Application for CISA certification
  - Minimum of five years information systems auditing, control or security work experience (waivers for education)
  - Adhere to the 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.



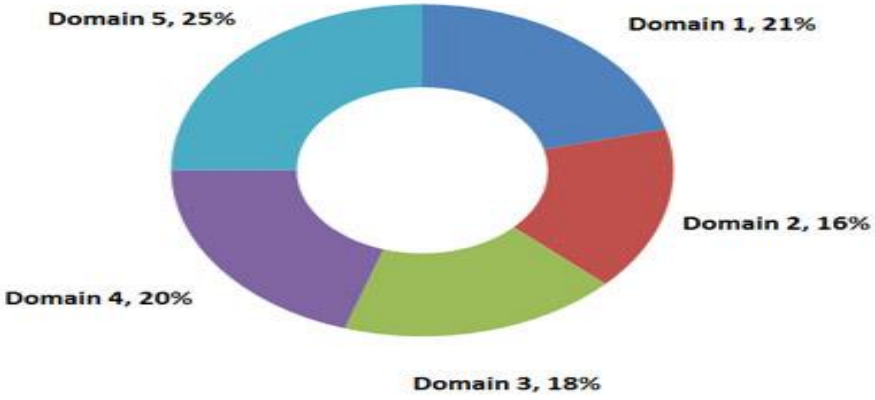
The Examination

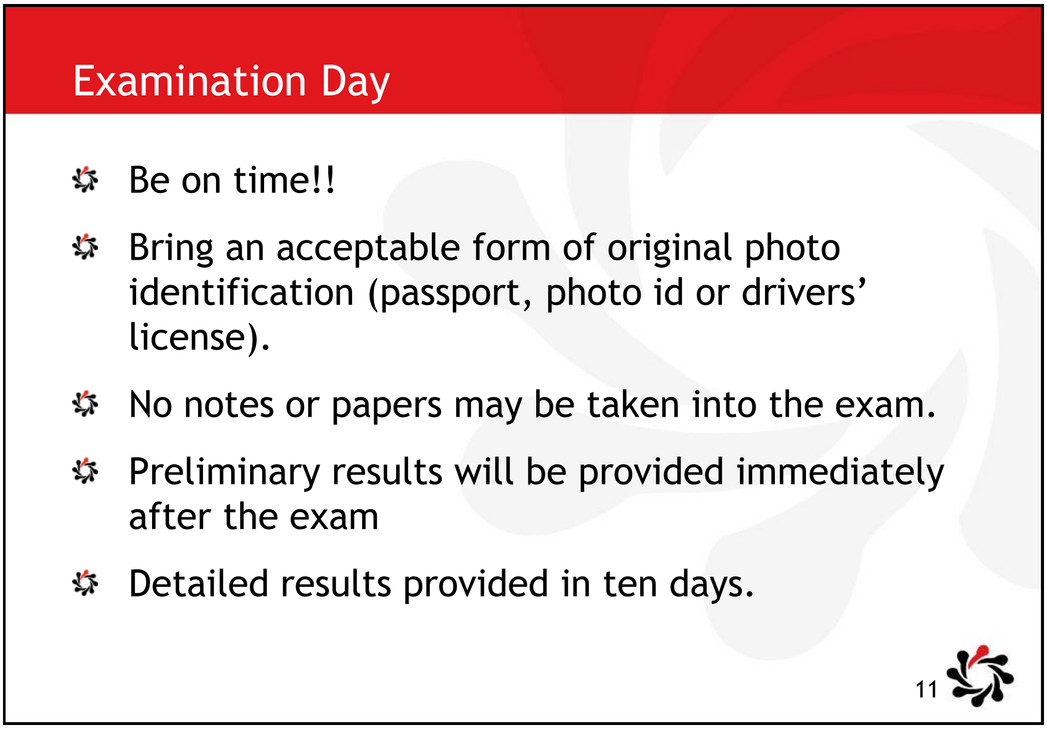
Description of the Exam

- The exam consists of 150 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
  - The 2017 examination content is the same as the 2016 examination

Examination Job Practice Areas

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

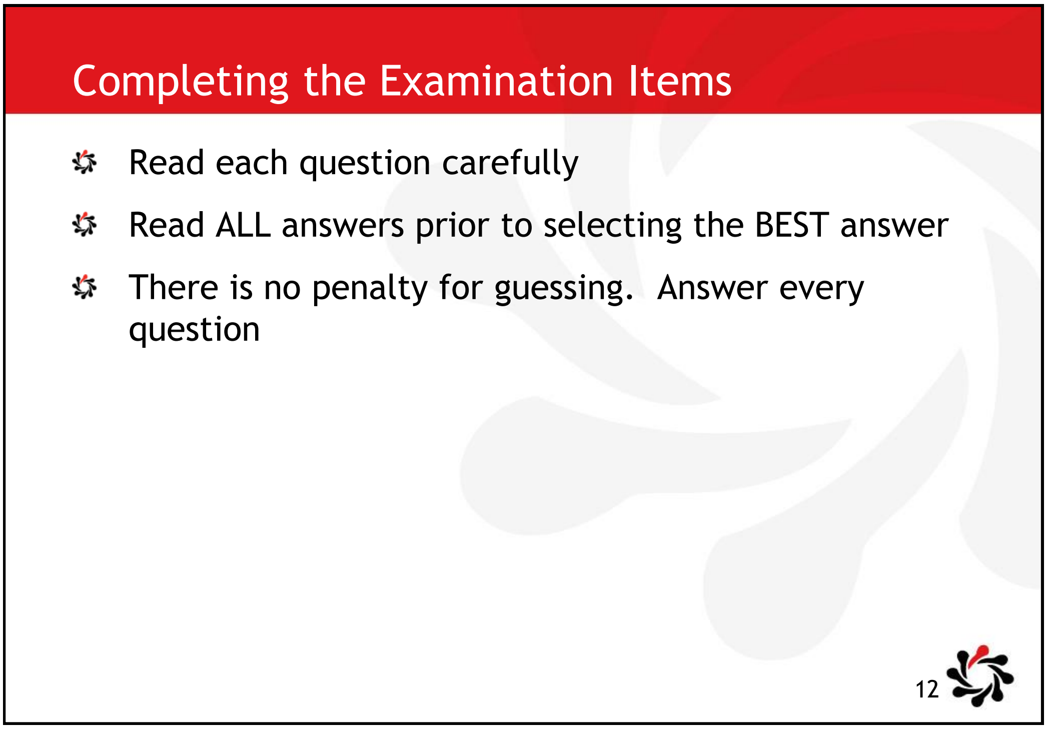




Examination Day

- Be on time!!
- Bring an acceptable form of original photo identification (passport, photo id or drivers' license).
- No notes or papers may be taken into the exam.
- Preliminary results will be provided immediately after the exam
- Detailed results provided in ten days.

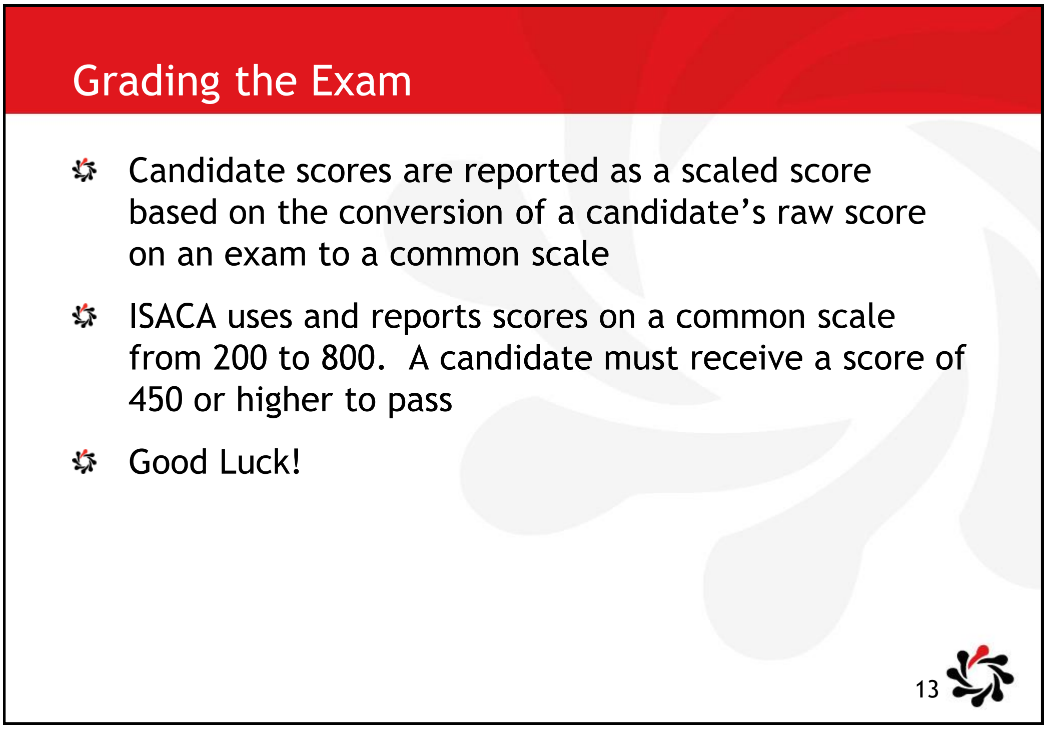
11



Completing the Examination Items

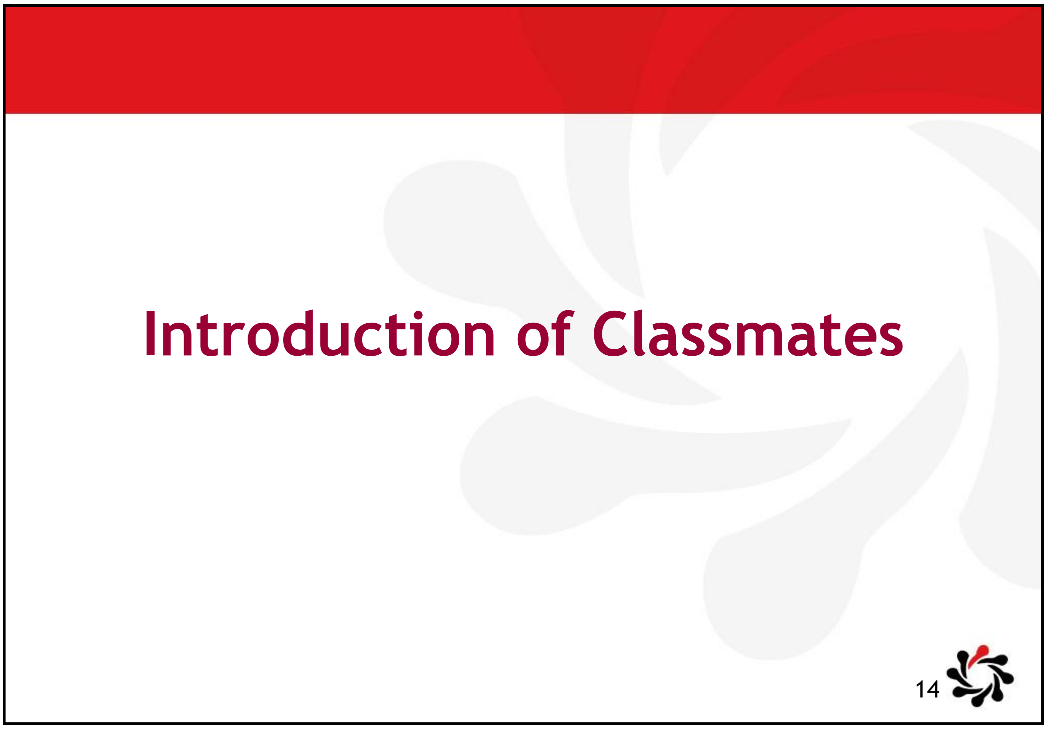
- Read each question carefully
- Read ALL answers prior to selecting the BEST answer
- There is no penalty for guessing. Answer every question

12

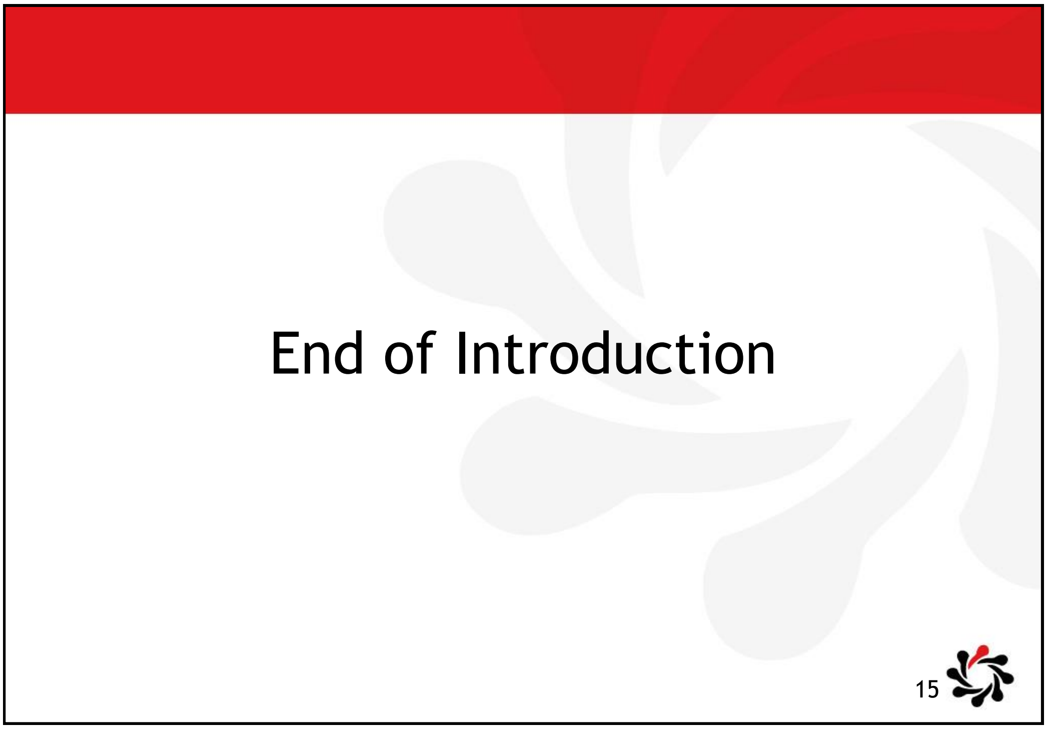


Grading the Exam

- 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
- Good Luck!

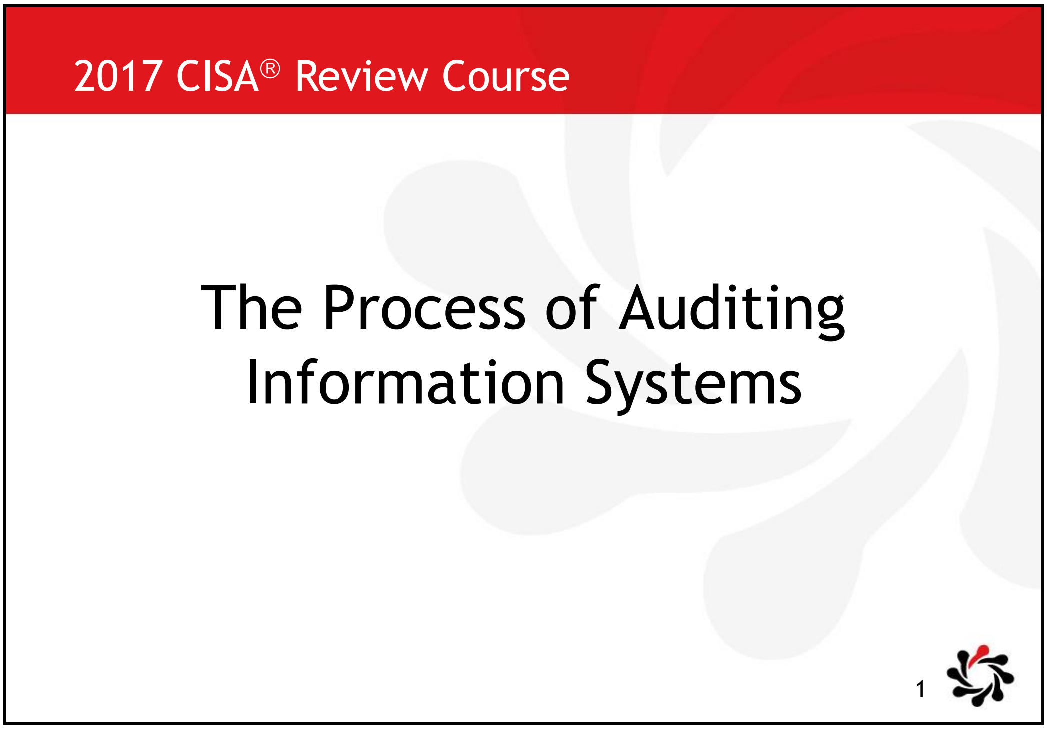


Introduction of Classmates



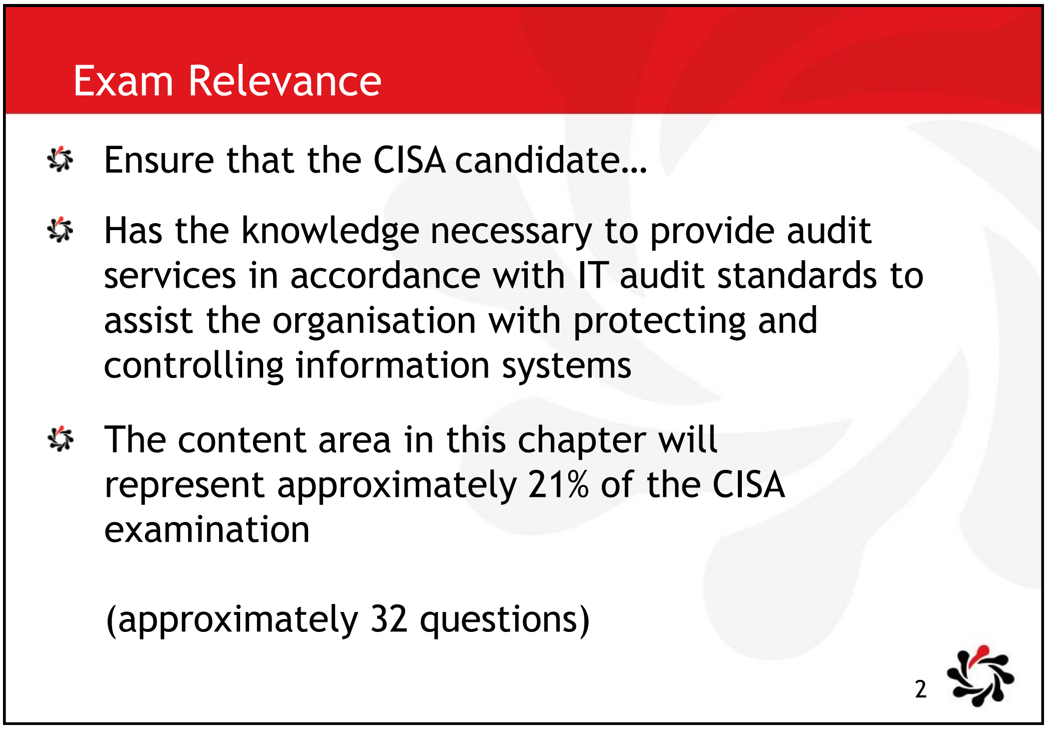
End of Introduction

15



2017 CISA® Review Course

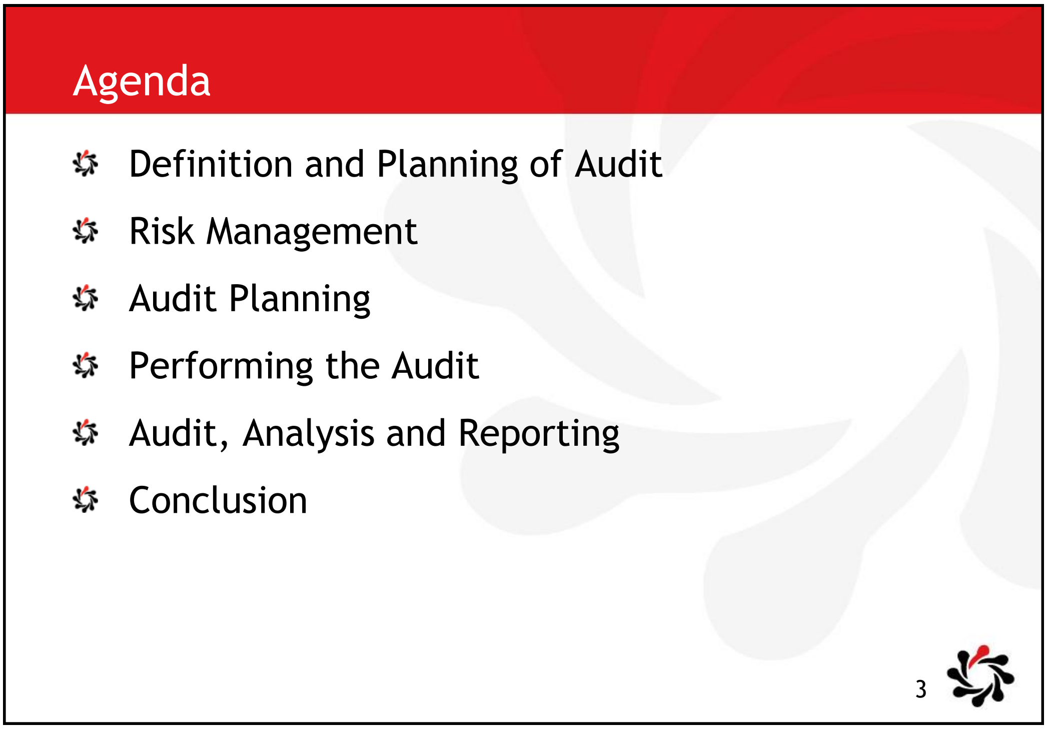
The Process of Auditing Information Systems



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

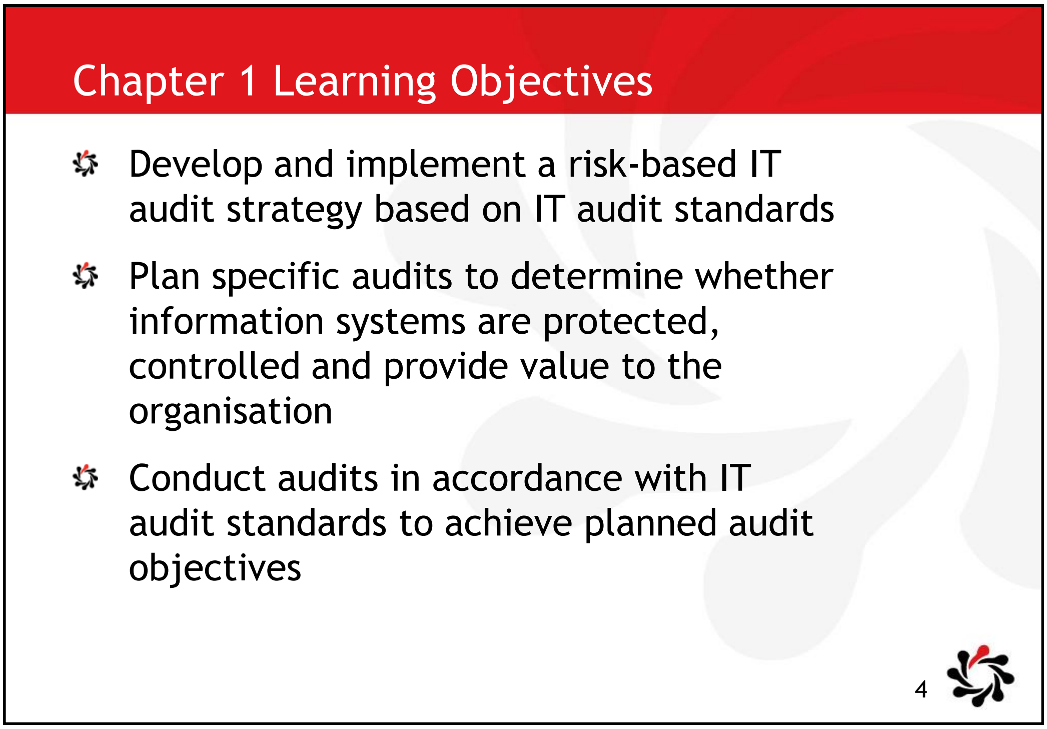
  (approximately 32 questions)



Agenda

- Definition and Planning of Audit
- Risk Management
- Audit Planning
- Performing the Audit
- Audit, Analysis and Reporting
- Conclusion

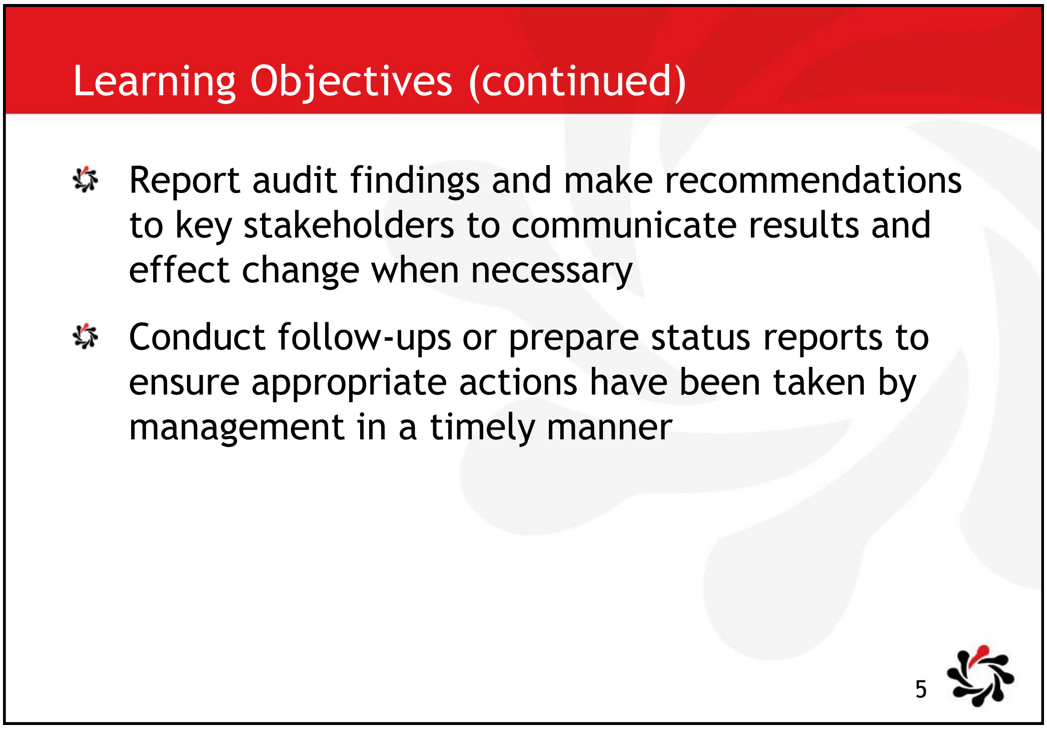
3



Chapter 1 Learning Objectives

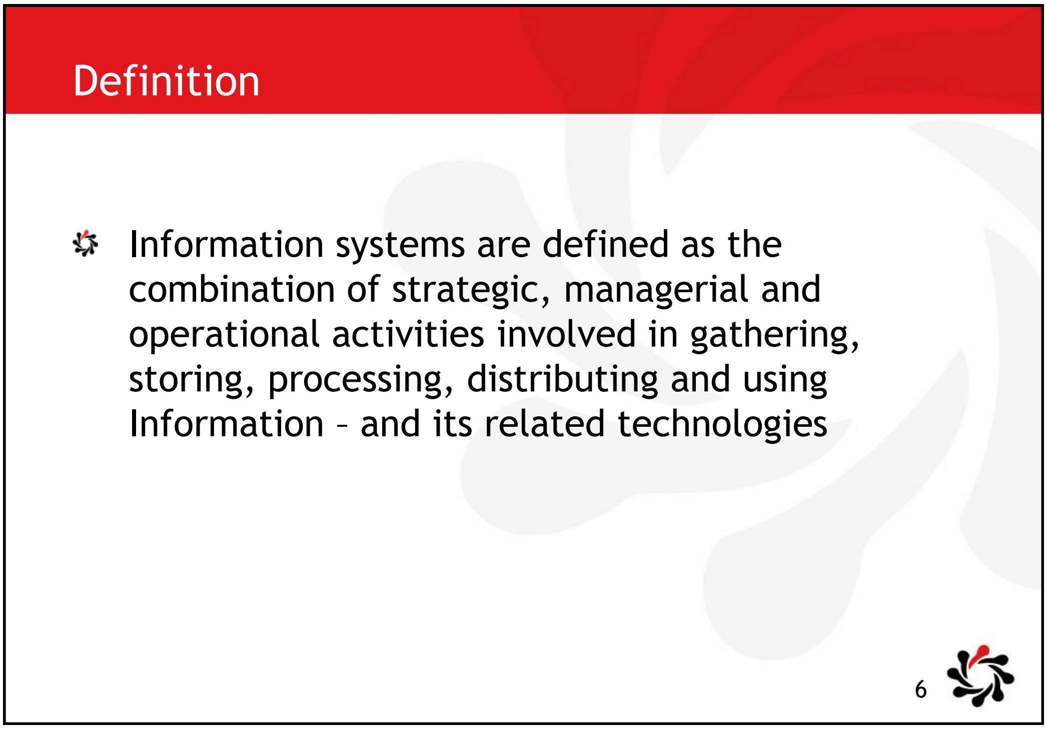
- Develop and implement a risk-based IT audit strategy based on IT audit standards
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organisation
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives

4



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



Definition

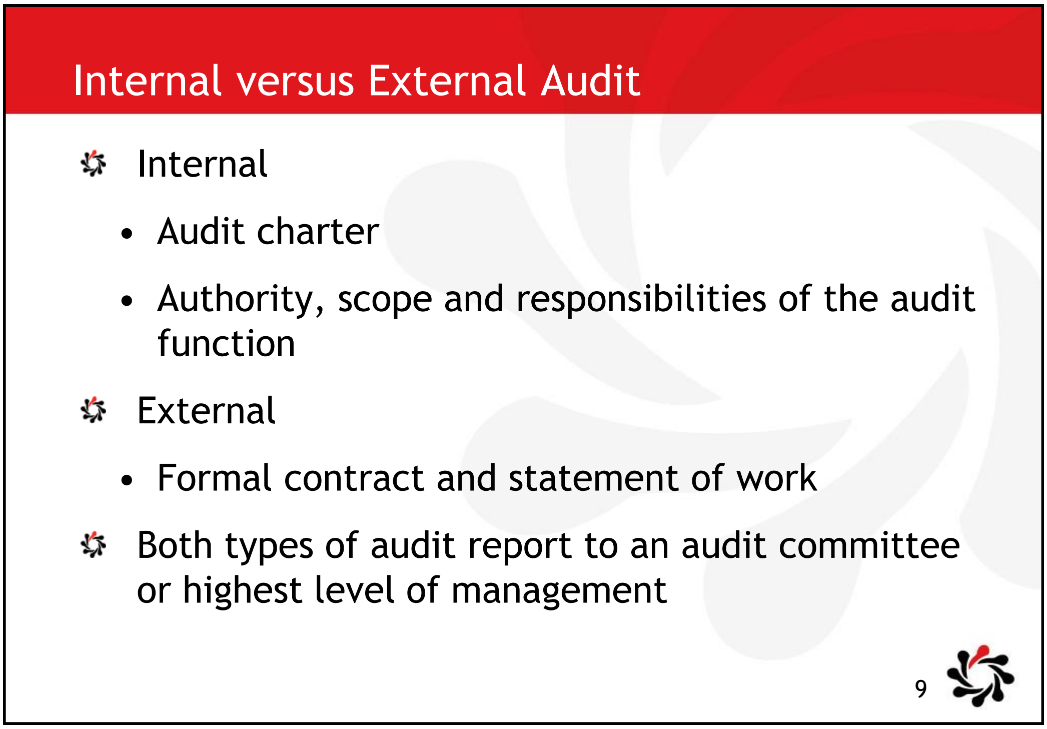
- Information systems are defined as the combination of strategic, managerial and operational activities involved in gathering, storing, processing, distributing and using Information – and its related technologies

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.

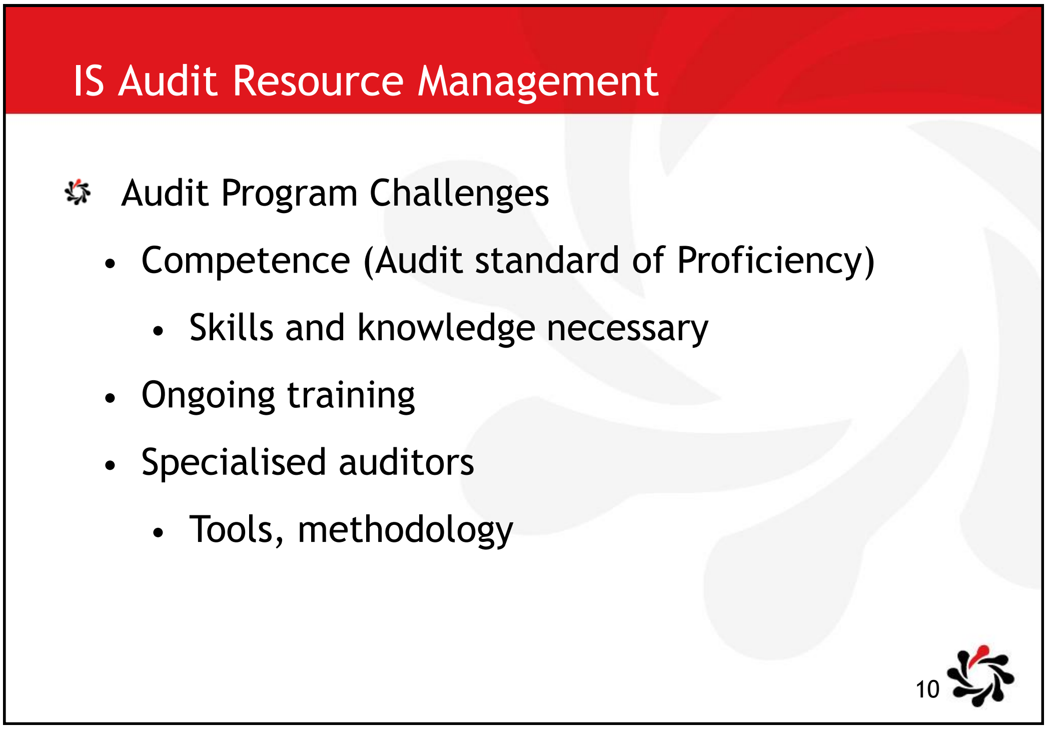
IS Audit

- IS Audit is the formal examination, interview and/or testing of information systems to determine whether:
  - Information systems are in compliance with applicable laws, regulations, contracts and/or industry guidelines
  - IS data and information have appropriate levels of confidentiality, integrity and availability
  - IS operations are being accomplished efficiently and effectiveness targets are being met



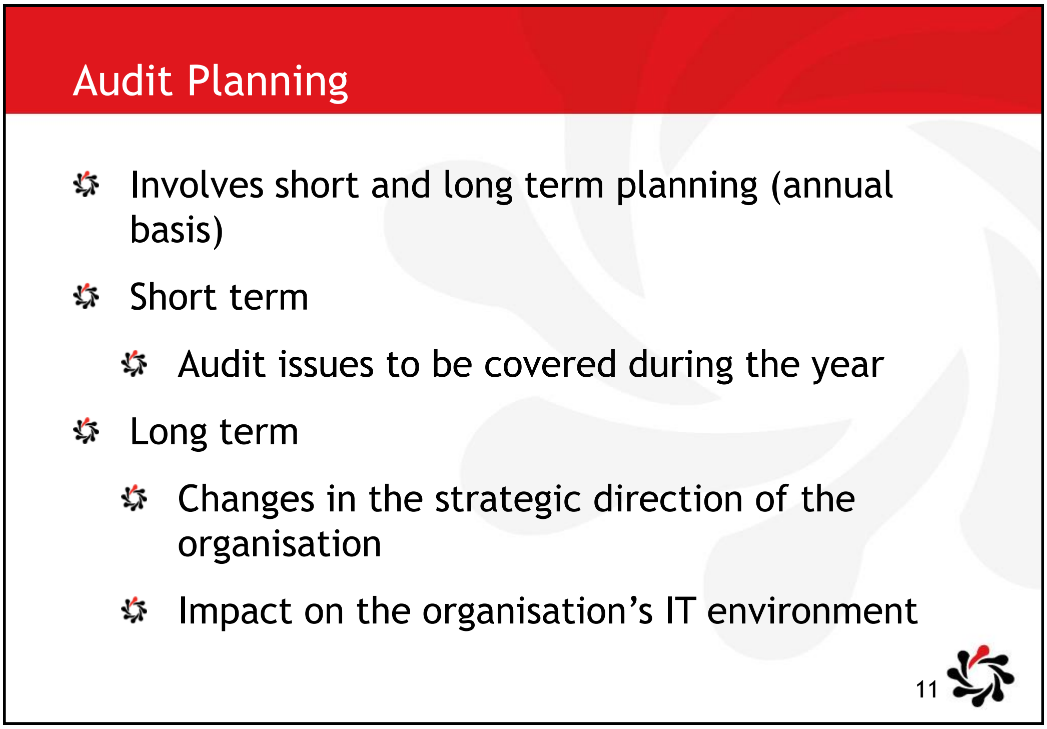
Internal versus External Audit

- Internal
  - Audit charter
  - Authority, scope and responsibilities of the audit function
- External
  - Formal contract and statement of work
- Both types of audit report to an audit committee or highest level of management



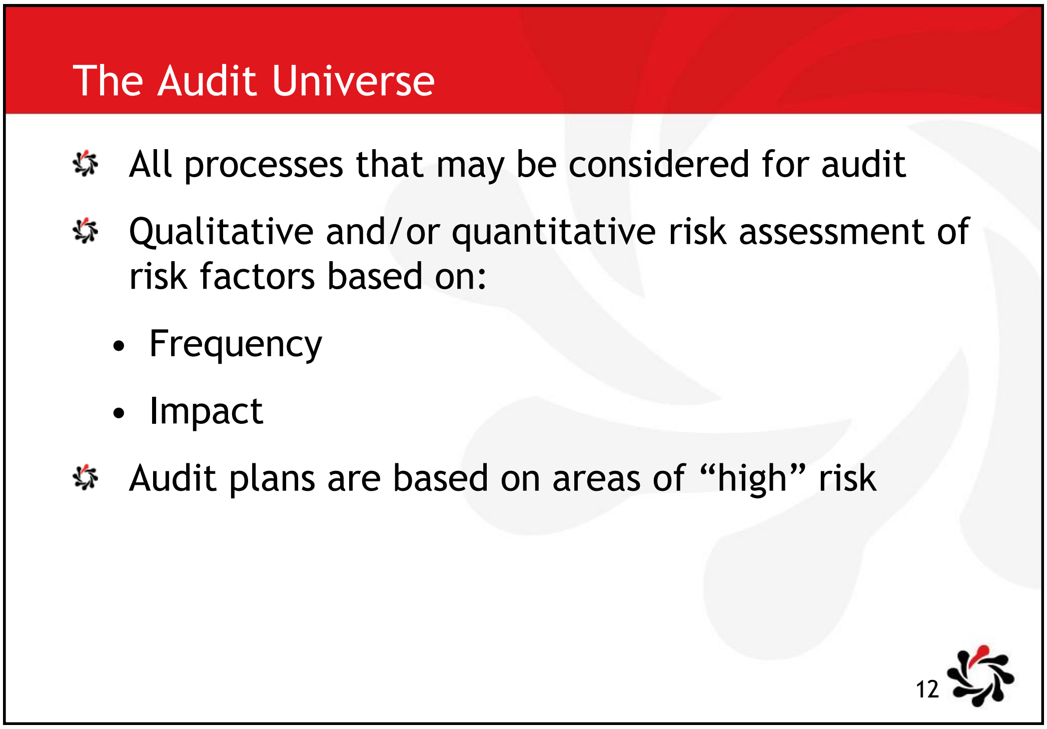
IS Audit Resource Management

- Audit Program Challenges
  - Competence (Audit standard of Proficiency)
    - Skills and knowledge necessary
  - Ongoing training
  - Specialised auditors
    - Tools, methodology



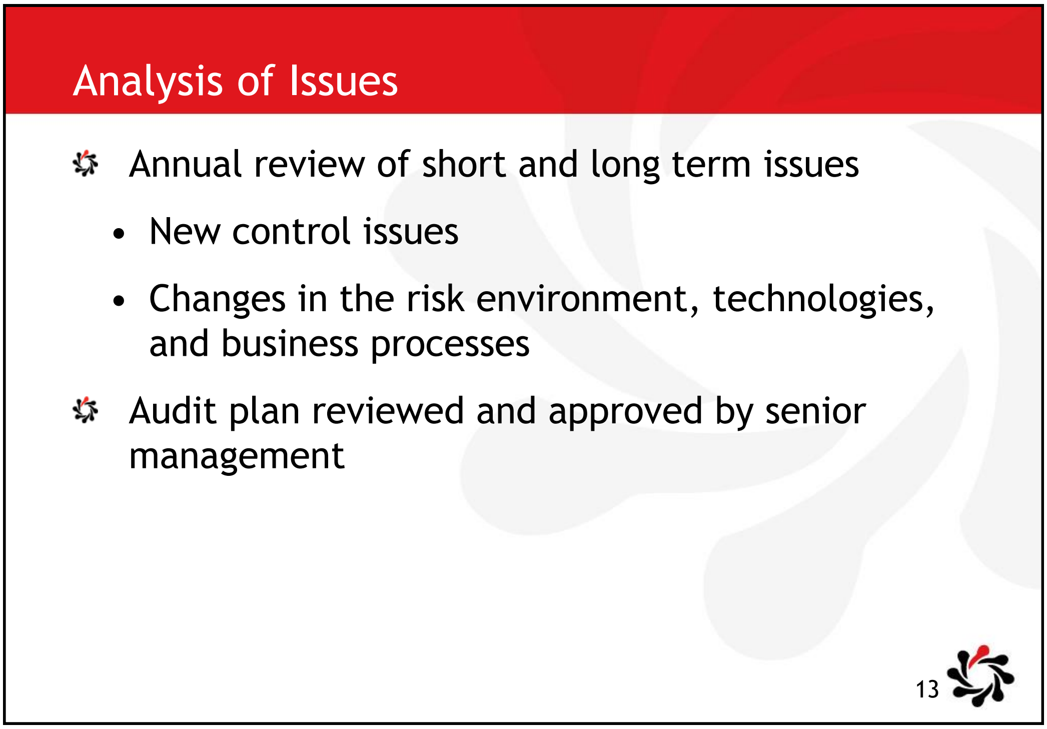
Audit Planning

- Involves short and long term planning (annual basis)
- Short term
  - Audit issues to be covered during the year
- Long term
  - Changes in the strategic direction of the organisation
  - Impact on the organisation’s IT environment



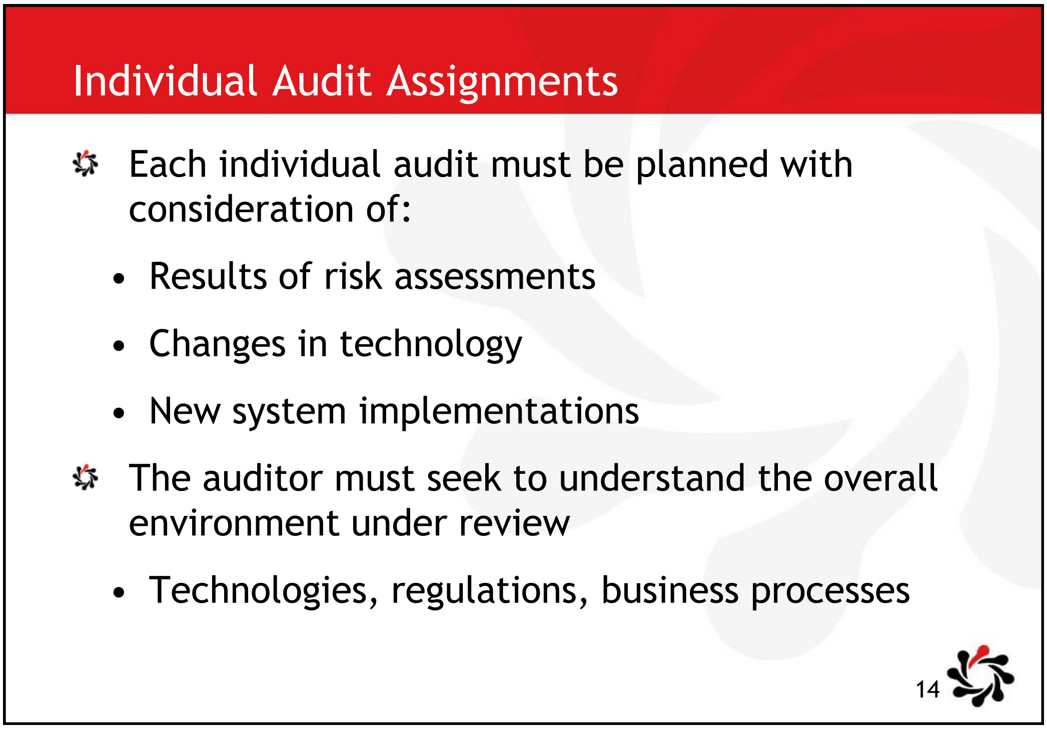
The Audit Universe

- All processes that may be considered for audit
- Qualitative and/or quantitative risk assessment of risk factors based on:
  - Frequency
  - Impact
- Audit plans are based on areas of “high” risk



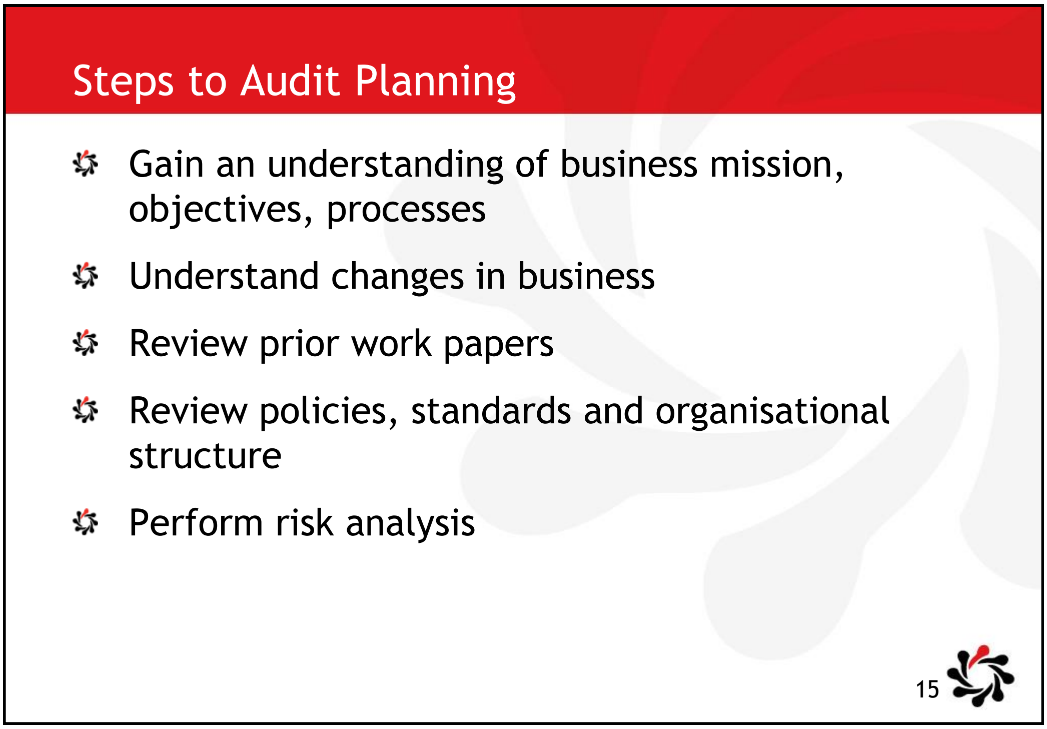
Analysis of Issues

- Annual review of short and long term issues
  - New control issues
  - Changes in the risk environment, technologies, and business processes
- Audit plan reviewed and approved by senior management



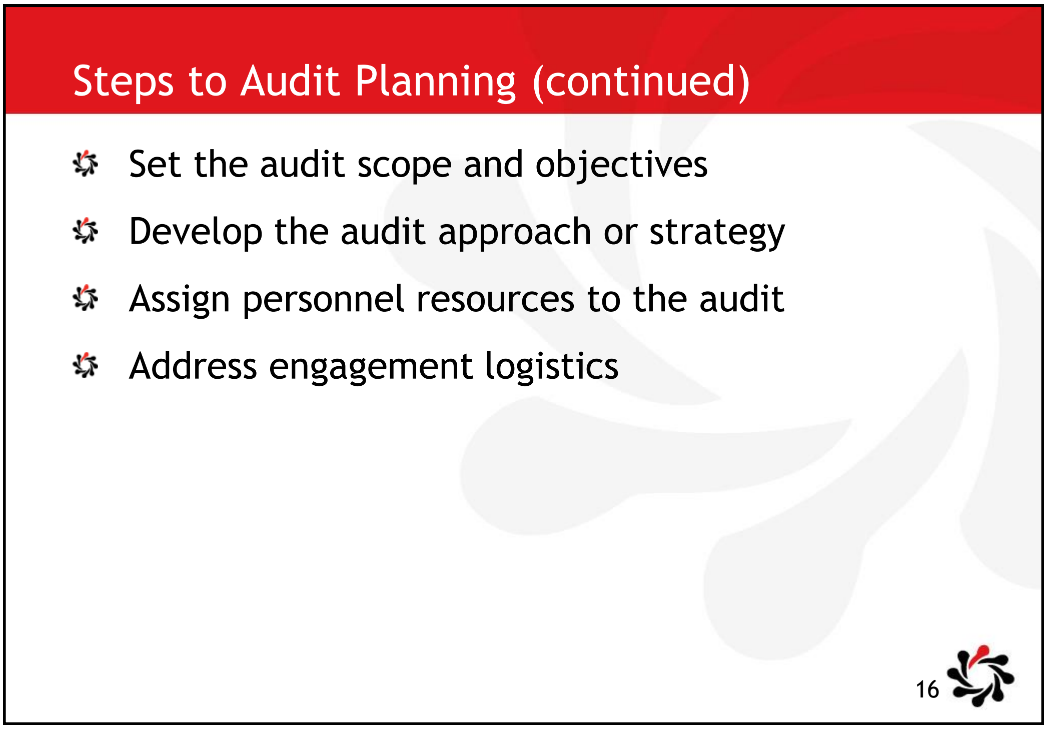
Individual Audit Assignments

- Each individual audit must be planned with consideration of:
  - Results of risk assessments
  - Changes in technology
  - New system implementations
- The auditor must seek to understand the overall environment under review
  - Technologies, regulations, business processes



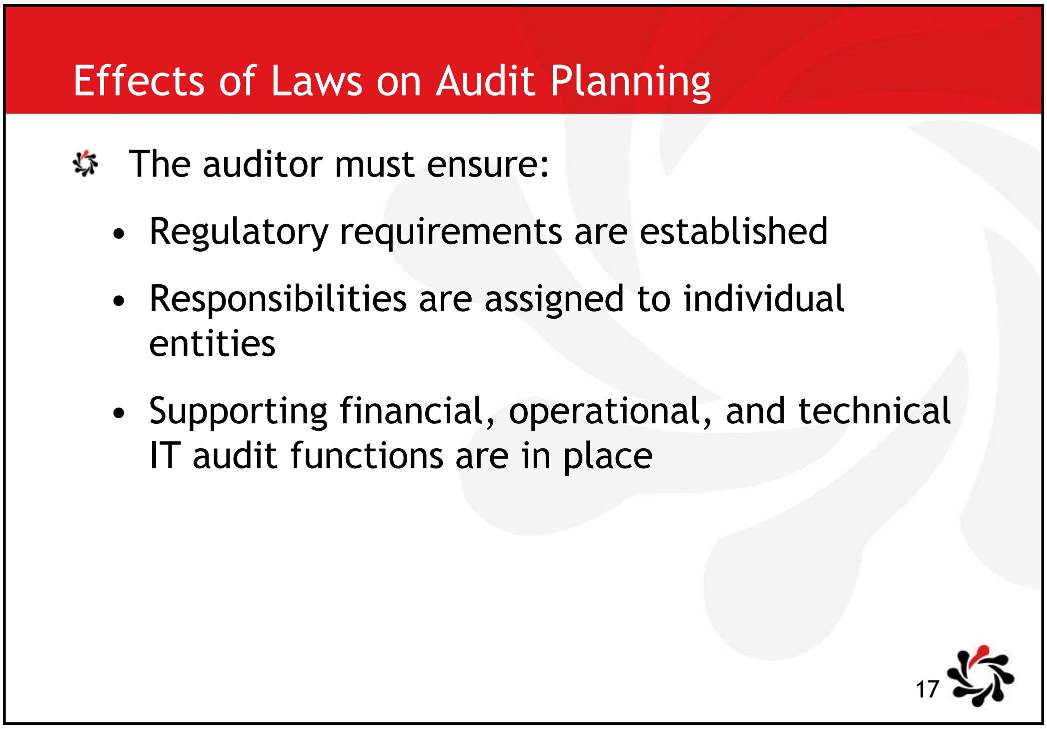
Steps to Audit Planning

- Gain an understanding of business mission, objectives, processes
- Understand changes in business
- Review prior work papers
- Review policies, standards and organisational structure
- Perform risk analysis



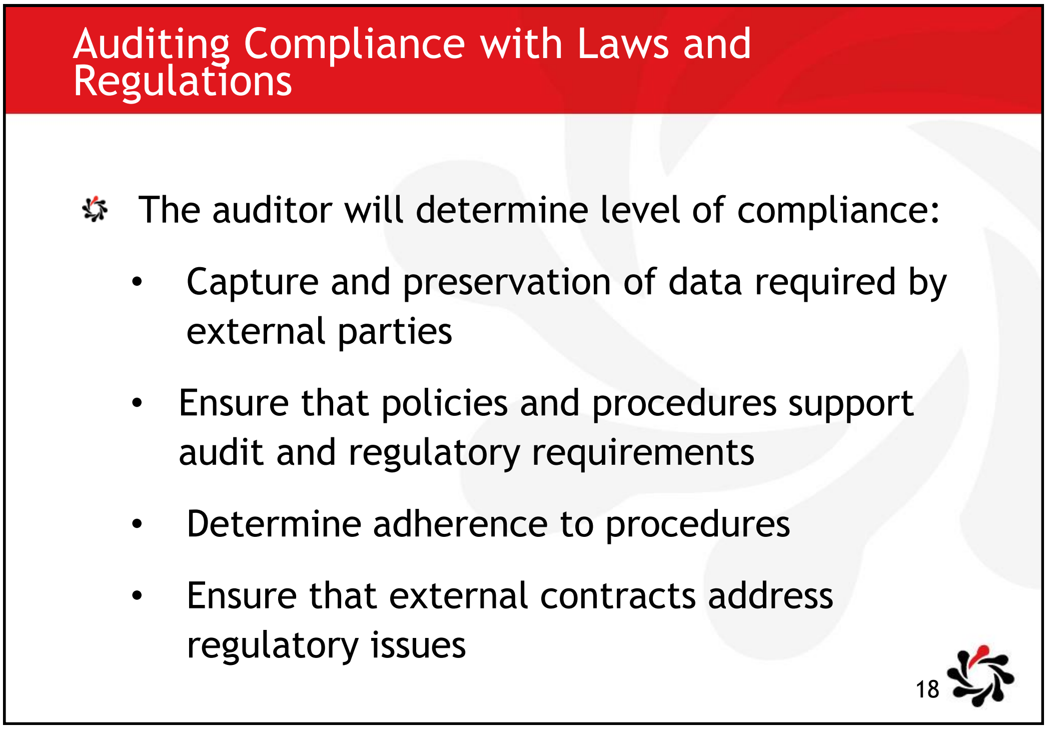
Steps to Audit Planning (continued)

- Set the audit scope and objectives
- Develop the audit approach or strategy
- Assign personnel resources to the audit
- Address engagement logistics



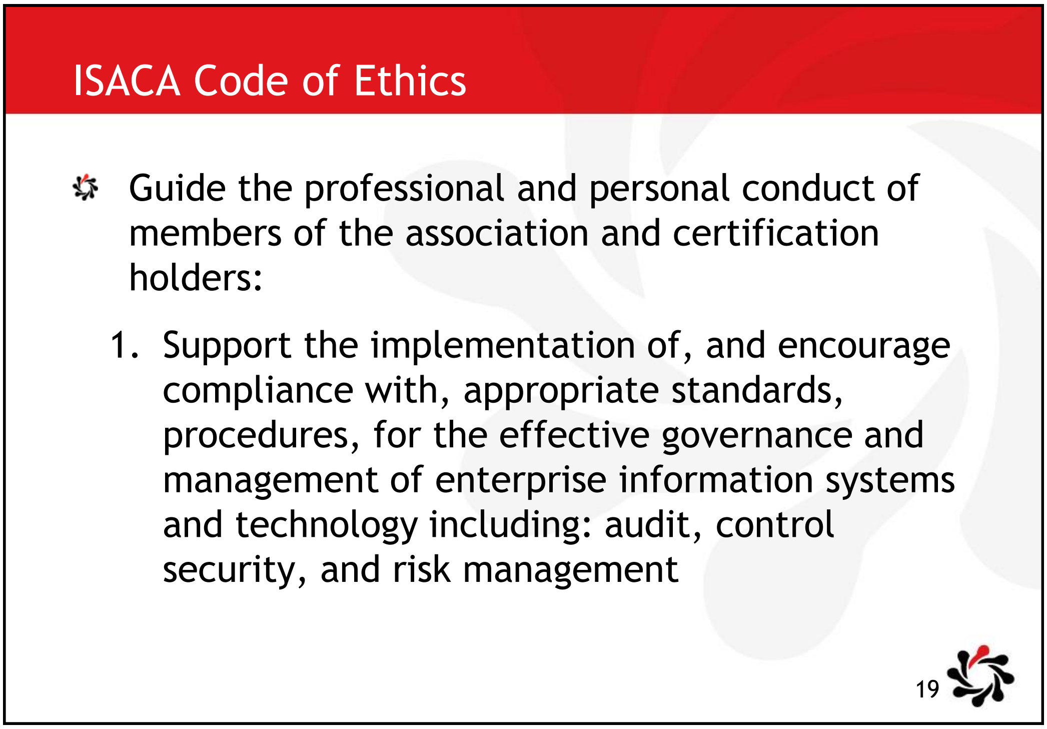
Effects of Laws on Audit Planning

- The auditor must ensure:
  - Regulatory requirements are established
  - Responsibilities are assigned to individual entities
  - Supporting financial, operational, and technical IT audit functions are in place



Auditing Compliance with Laws and Regulations

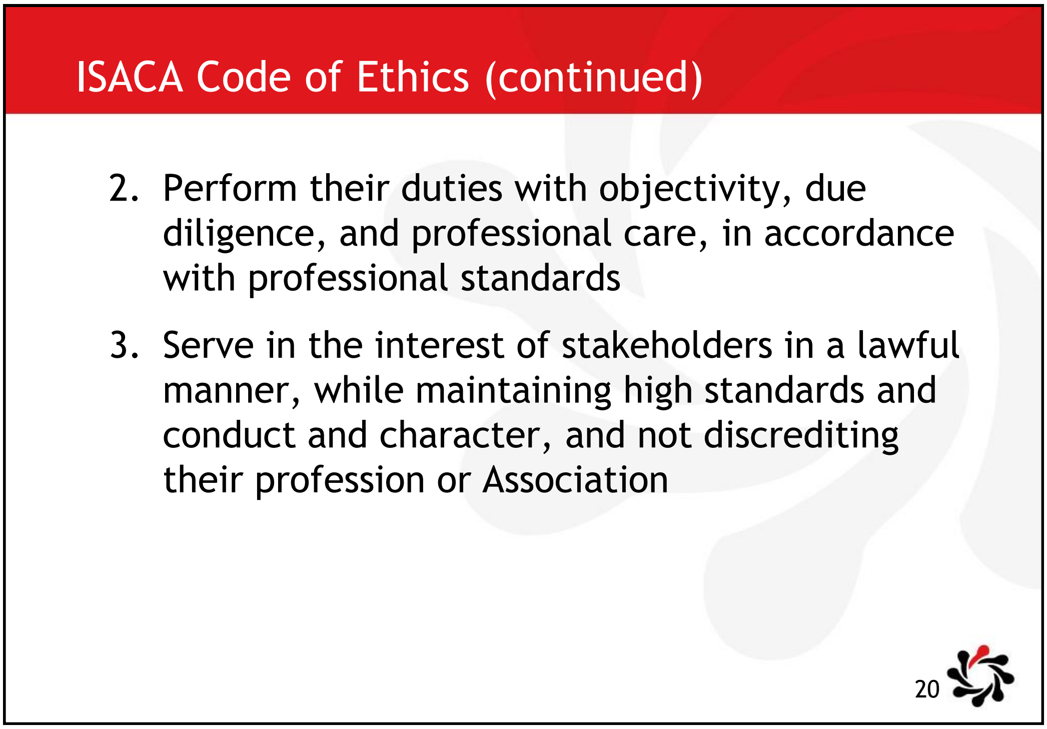
- The auditor will determine level of compliance:
  - Capture and preservation of data required by external parties
  - Ensure that policies and procedures support audit and regulatory requirements
  - Determine adherence to procedures
  - Ensure that external contracts address regulatory issues



ISACA Code of Ethics

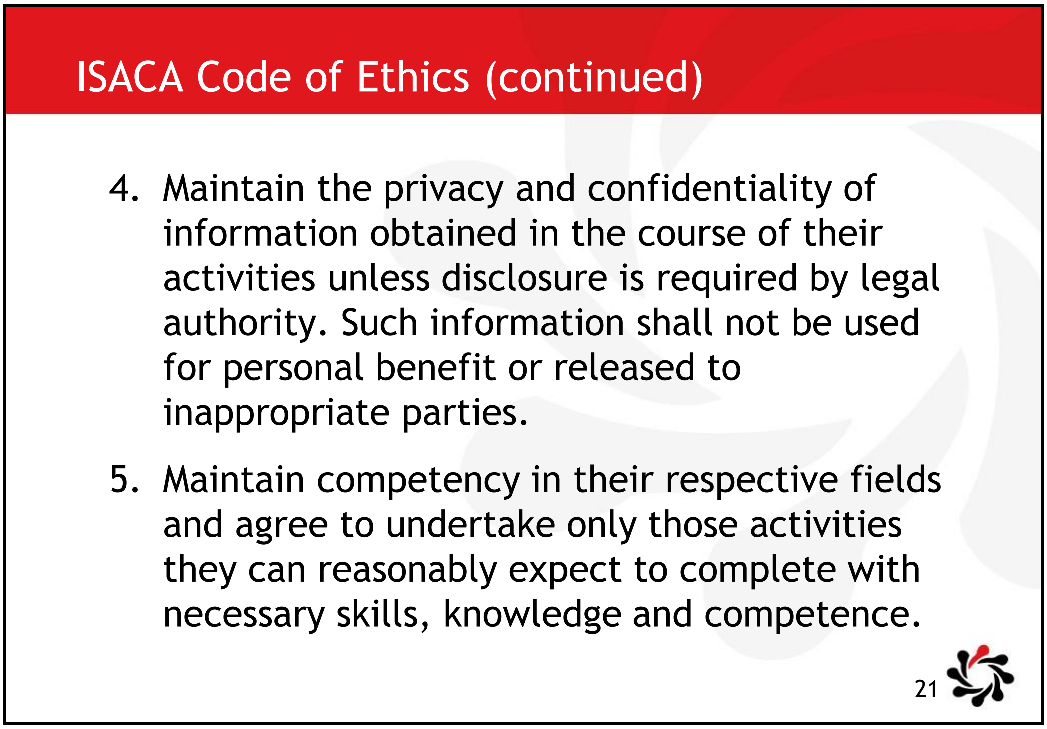
- Guide the professional and personal conduct of members of the association and certification holders:

  1. Support the implementation of, and encourage compliance with, appropriate standards, procedures, for the effective governance and management of enterprise information systems and technology including: audit, control security, and risk management



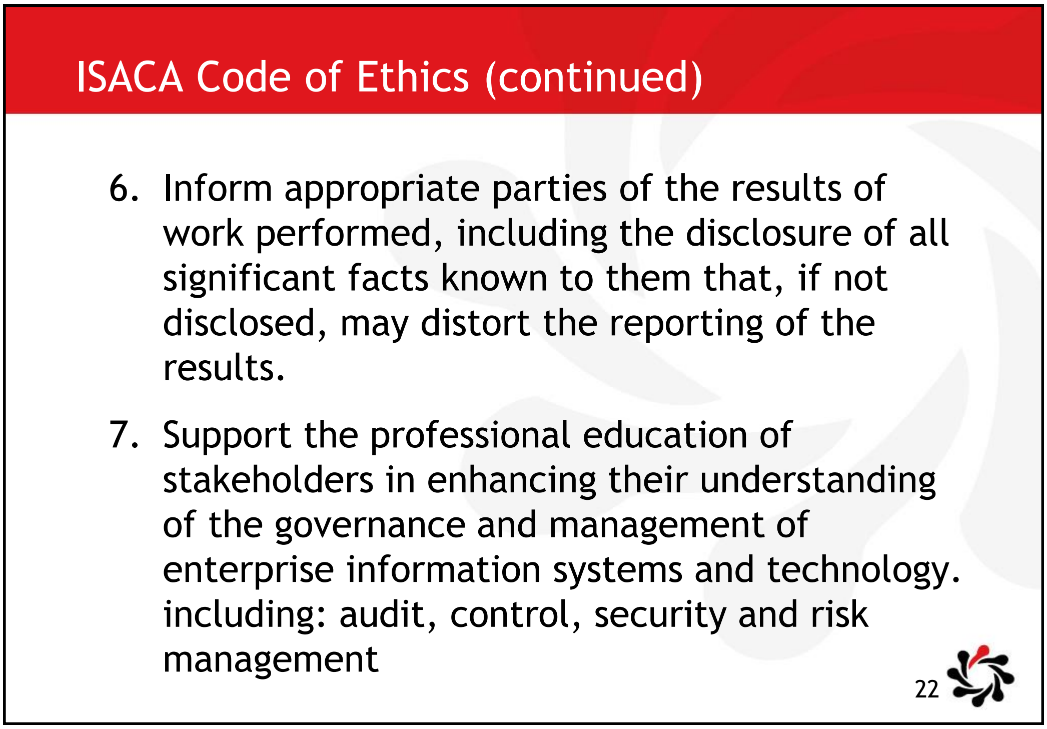
ISACA Code of Ethics (continued)

2. Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards and conduct and character, and not discrediting their profession or Association



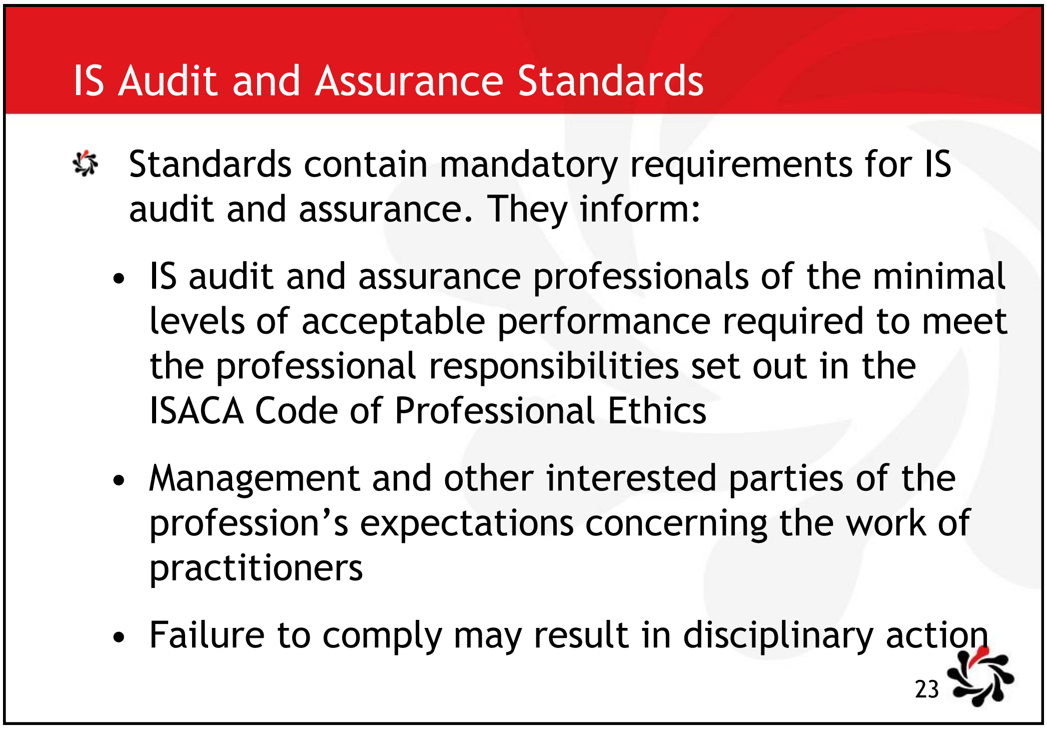
ISACA Code of Ethics (continued)

4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with necessary skills, knowledge and competence.



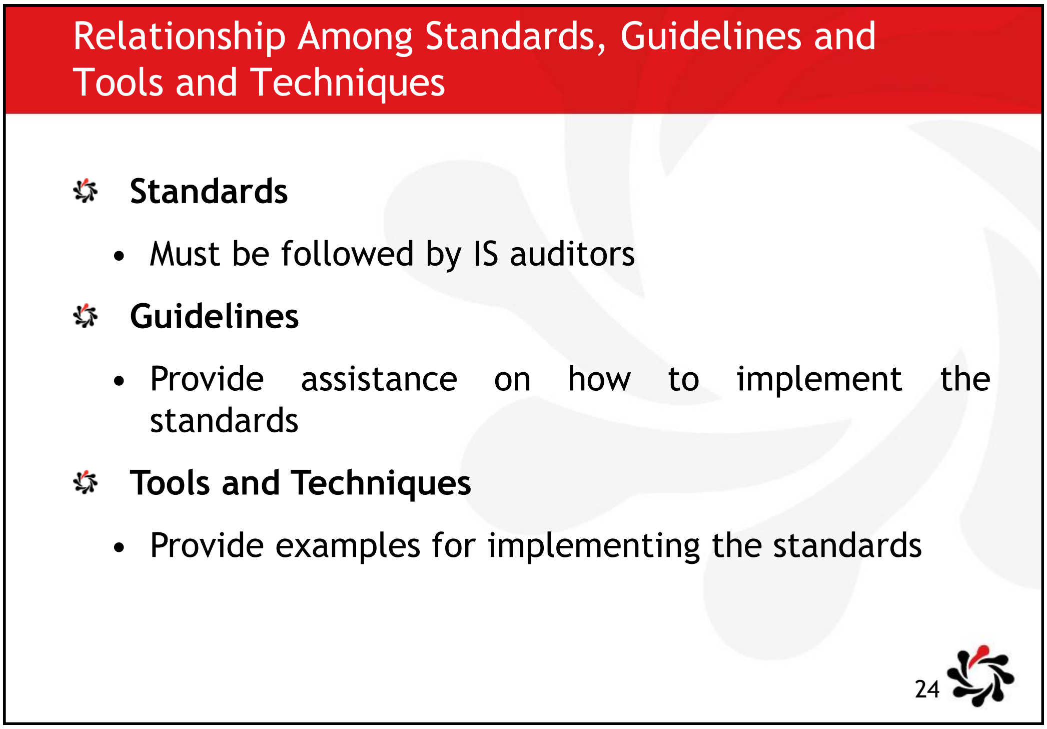
ISACA Code of Ethics (continued)

6. Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology. including: audit, control, security and risk management



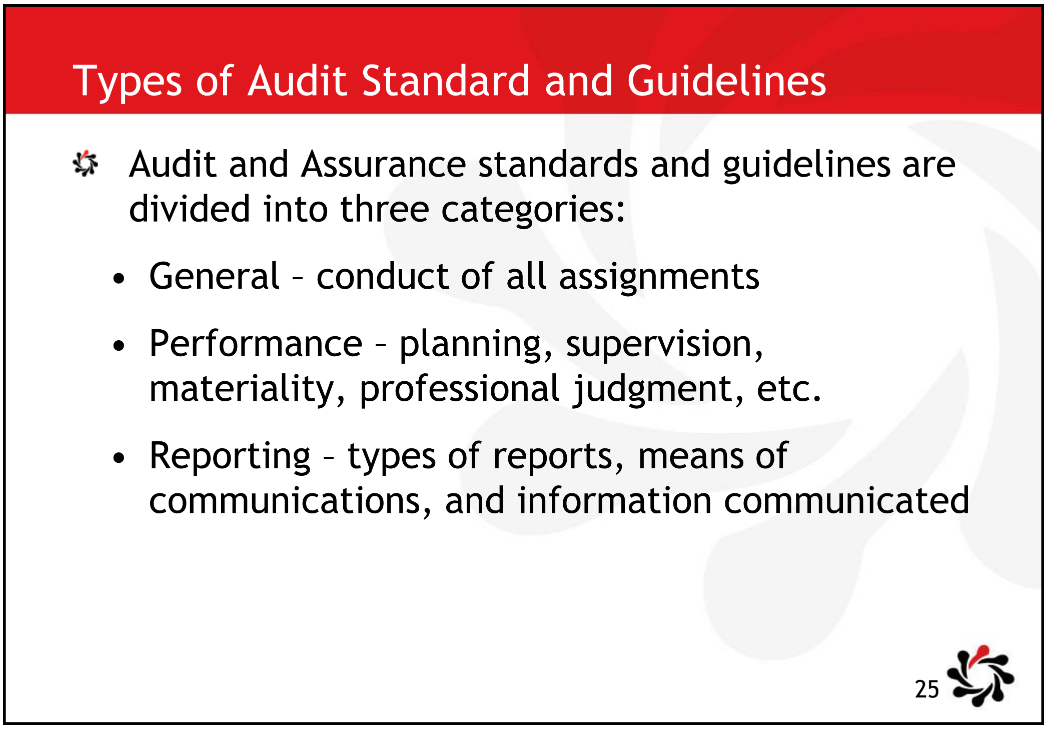
IS Audit and Assurance Standards

- Standards contain mandatory requirements for IS audit and assurance. They inform:
  - IS audit and assurance professionals of the minimal levels of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession’s expectations concerning the work of practitioners
  - Failure to comply may result in disciplinary action



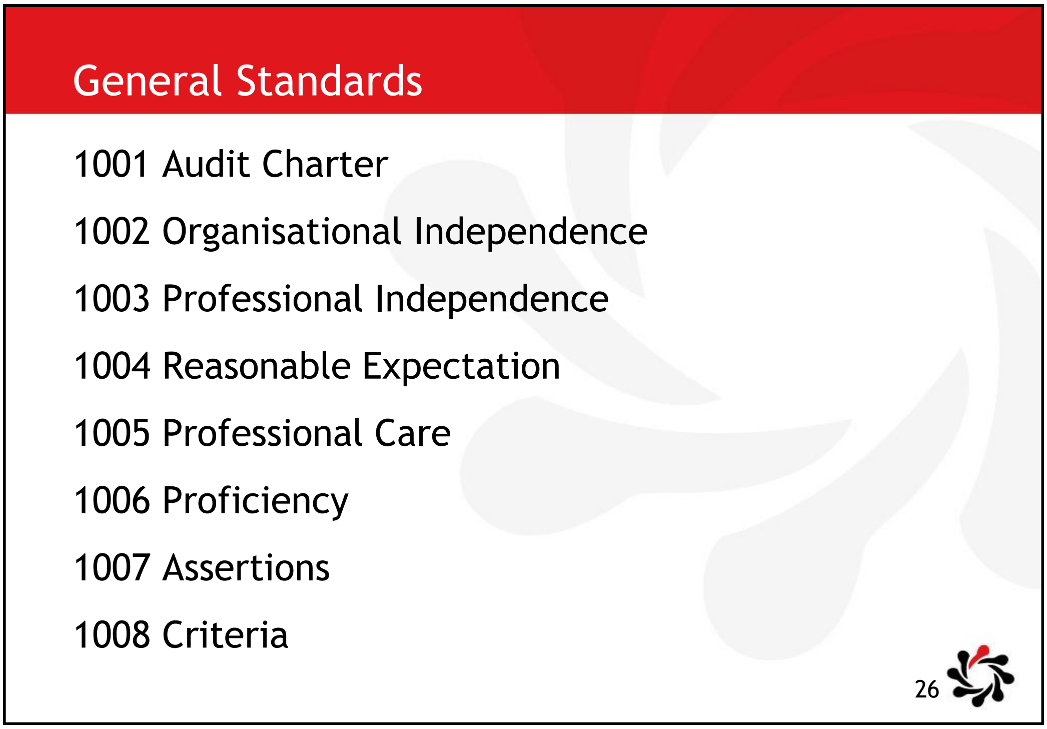
Relationship Among Standards, Guidelines and Tools and Techniques

- **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



Types of Audit Standard and Guidelines

- Audit and Assurance standards and guidelines are divided into three categories:
  - General – conduct of all assignments
  - Performance – planning, supervision, materiality, professional judgment, etc.
  - Reporting – types of reports, means of communications, and information communicated



General Standards

1001 Audit Charter

1002 Organisational Independence

1003 Professional Independence

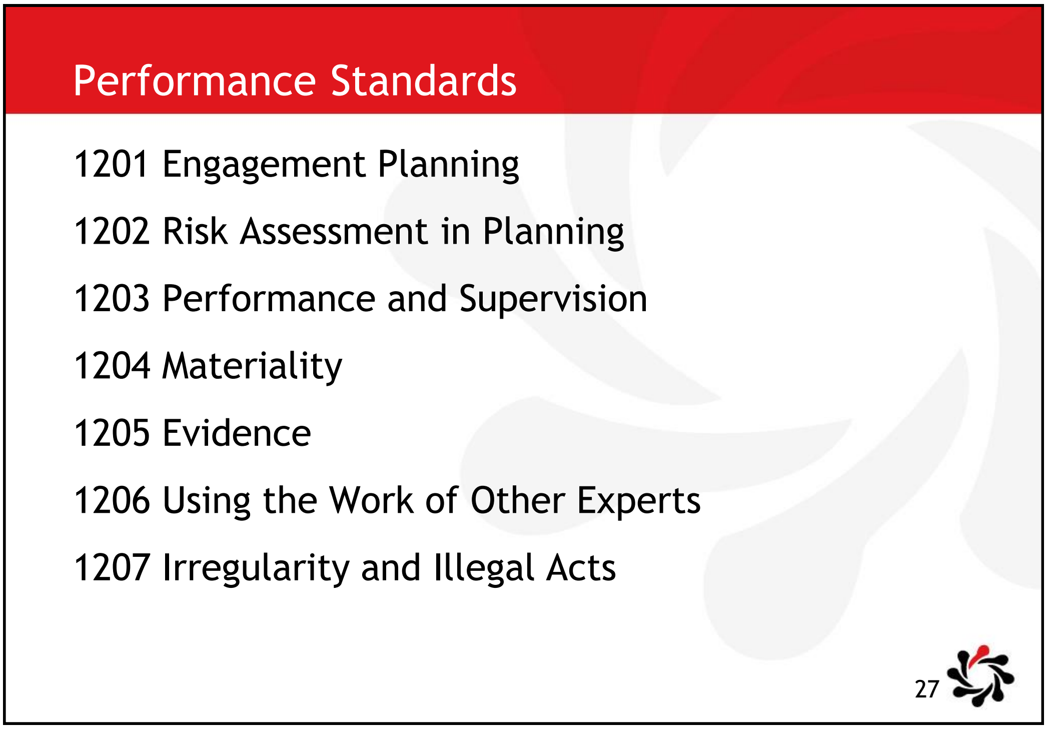
1004 Reasonable Expectation

1005 Professional Care

1006 Proficiency

1007 Assertions

1008 Criteria



Performance Standards

1201 Engagement Planning

1202 Risk Assessment in Planning

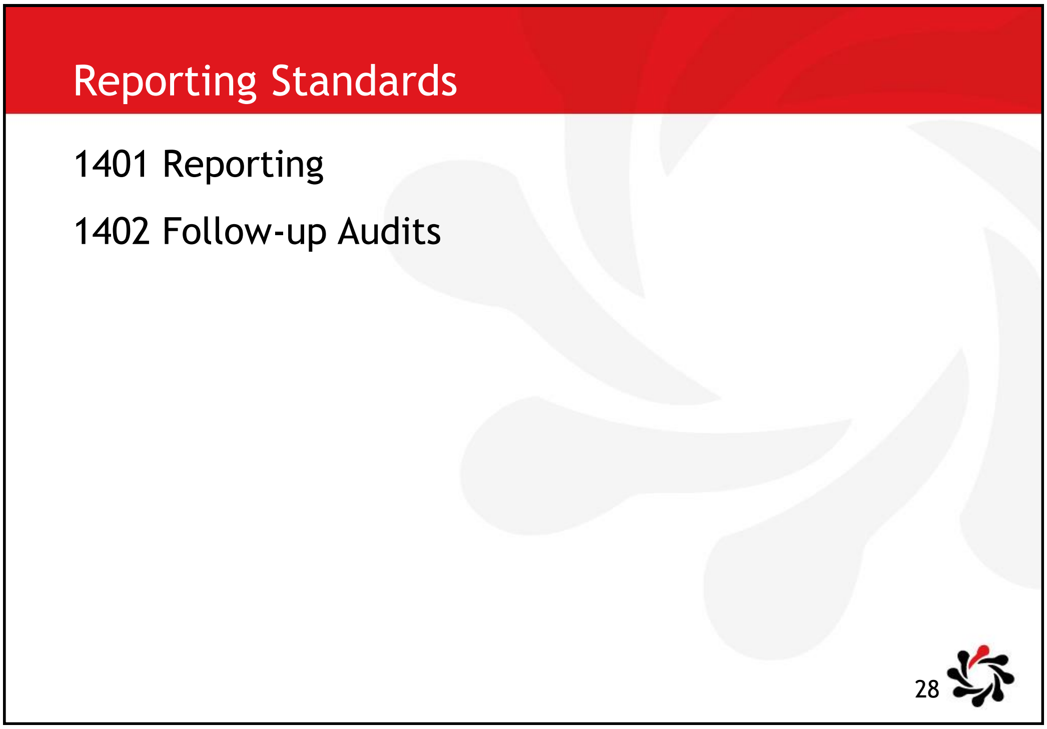
1203 Performance and Supervision

1204 Materiality

1205 Evidence

1206 Using the Work of Other Experts

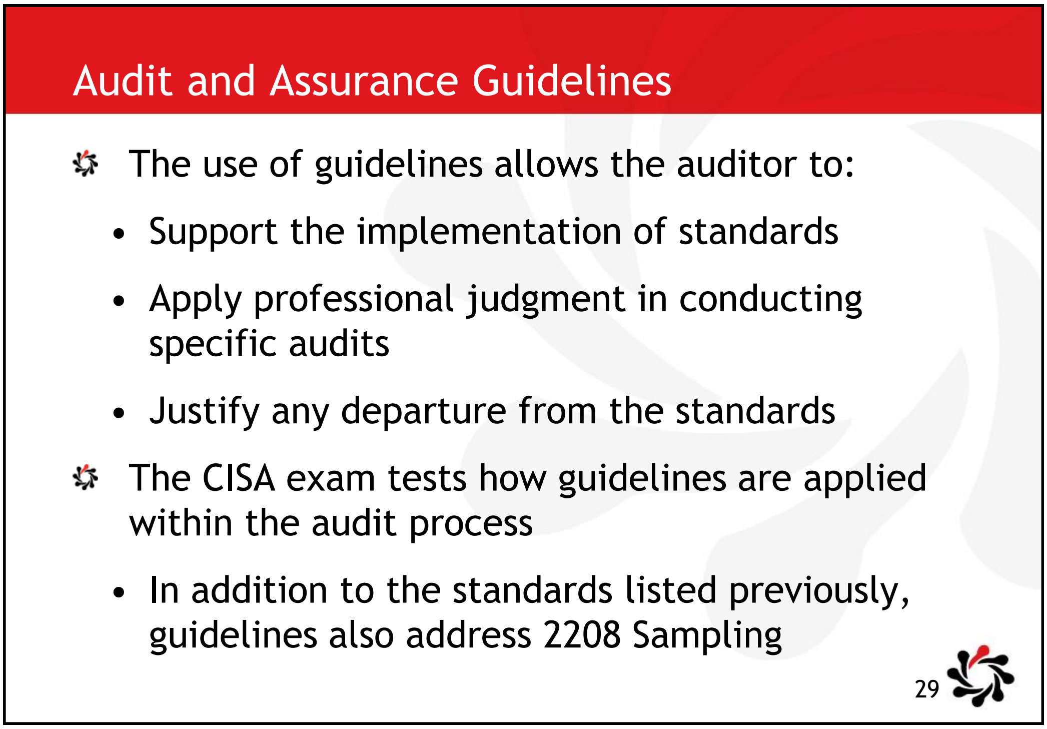
1207 Irregularity and Illegal Acts



Reporting Standards

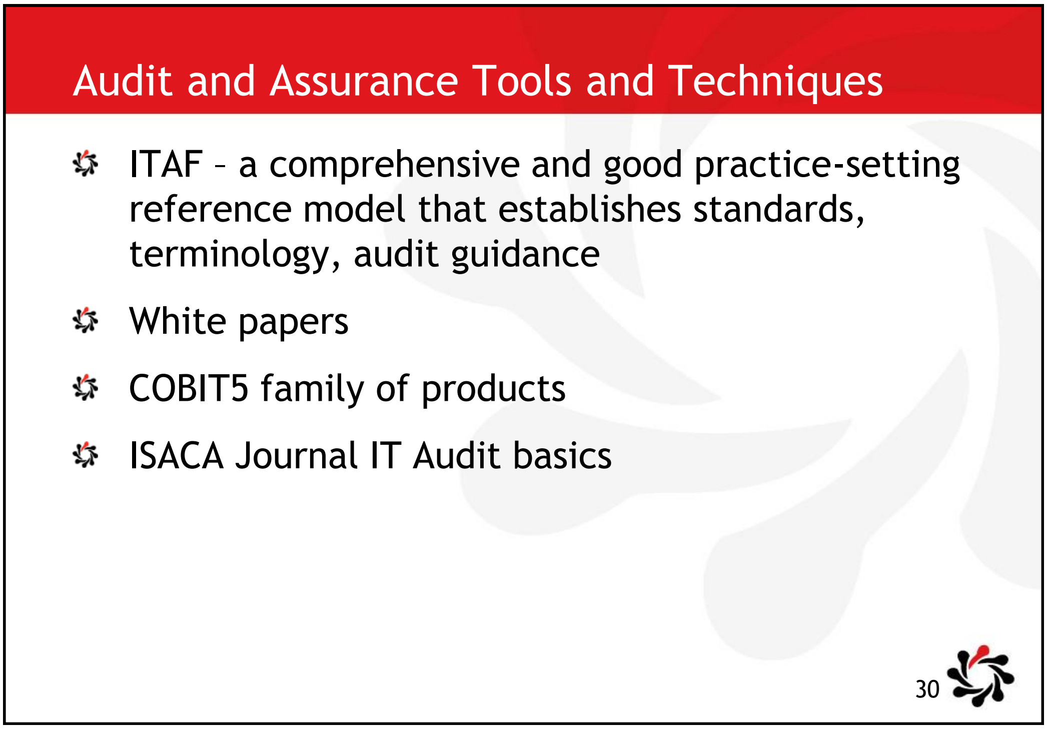
1401 Reporting

1402 Follow-up Audits



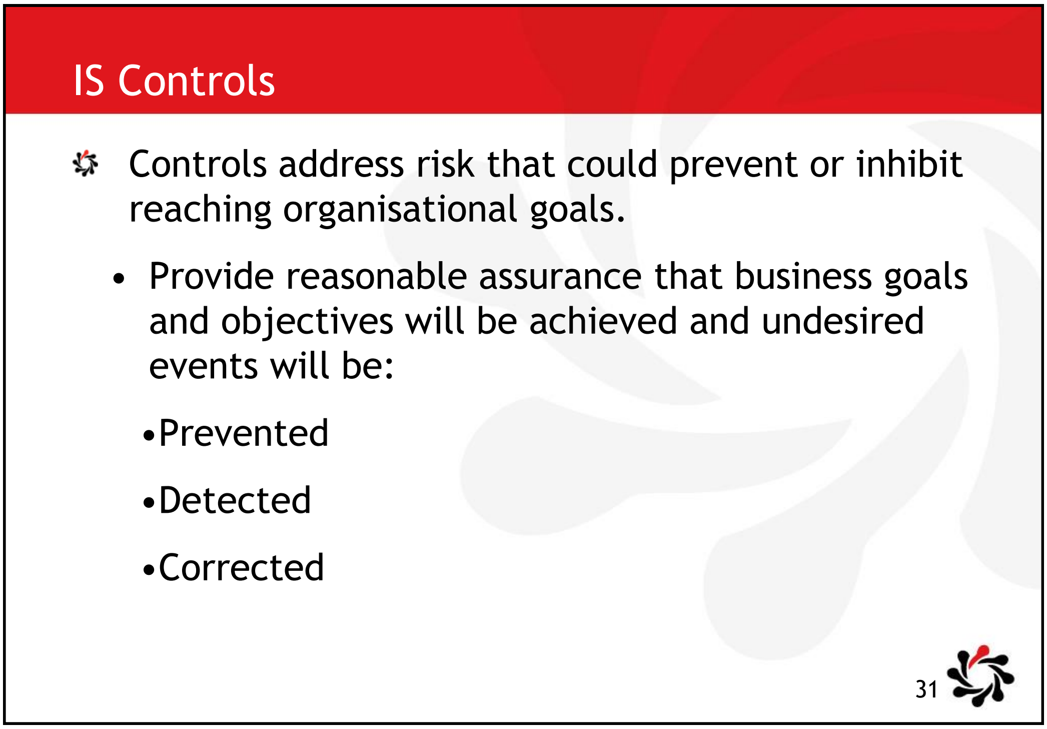
Audit and Assurance Guidelines

- The use of guidelines allows the auditor to:
  - Support the implementation of standards
  - Apply professional judgment in conducting specific audits
  - Justify any departure from the standards
- The CISA exam tests how guidelines are applied within the audit process
  - In addition to the standards listed previously, guidelines also address 2208 Sampling



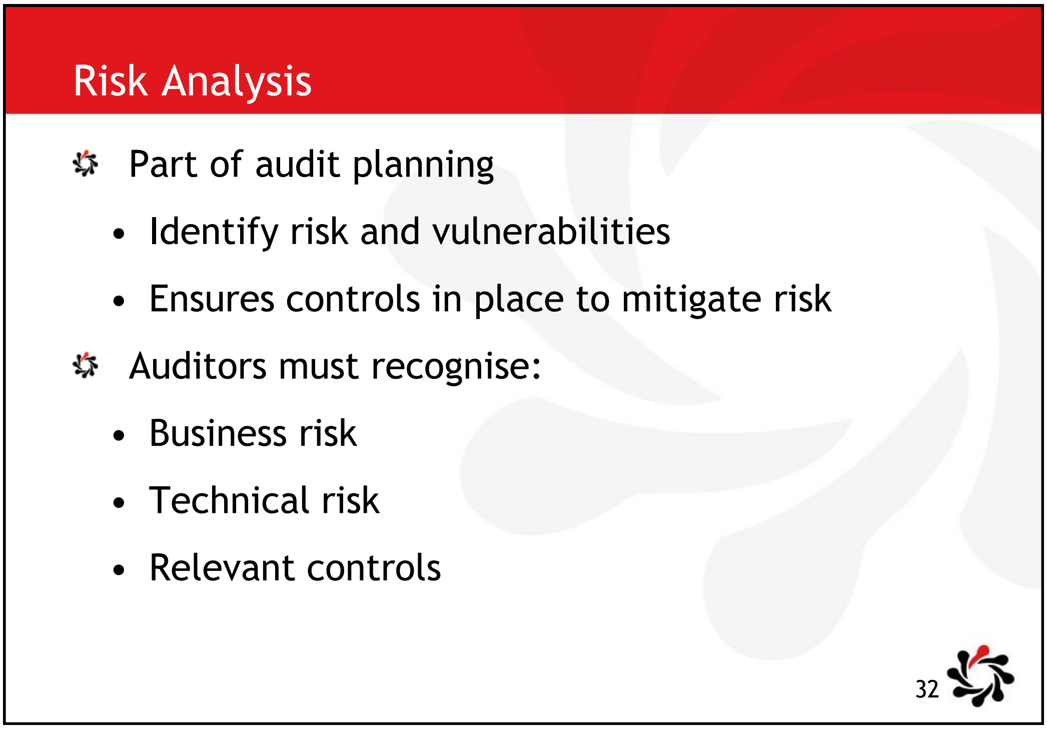
Audit and Assurance Tools and Techniques

- ITAF – a comprehensive and good practice-setting reference model that establishes standards, terminology, audit guidance
- White papers
- COBIT5 family of products
- ISACA Journal IT Audit basics



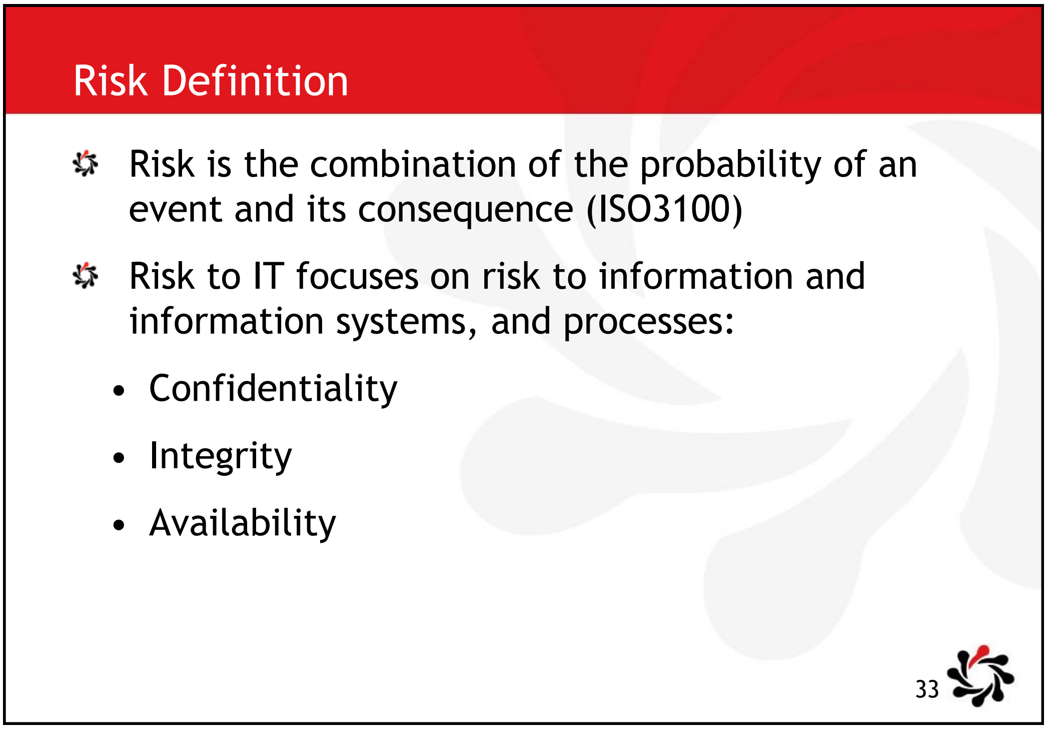
IS Controls

- Controls address risk that could prevent or inhibit reaching organisational goals.
  - Provide reasonable assurance that business goals and objectives will be achieved and undesired events will be:
    - Prevented
    - Detected
    - Corrected



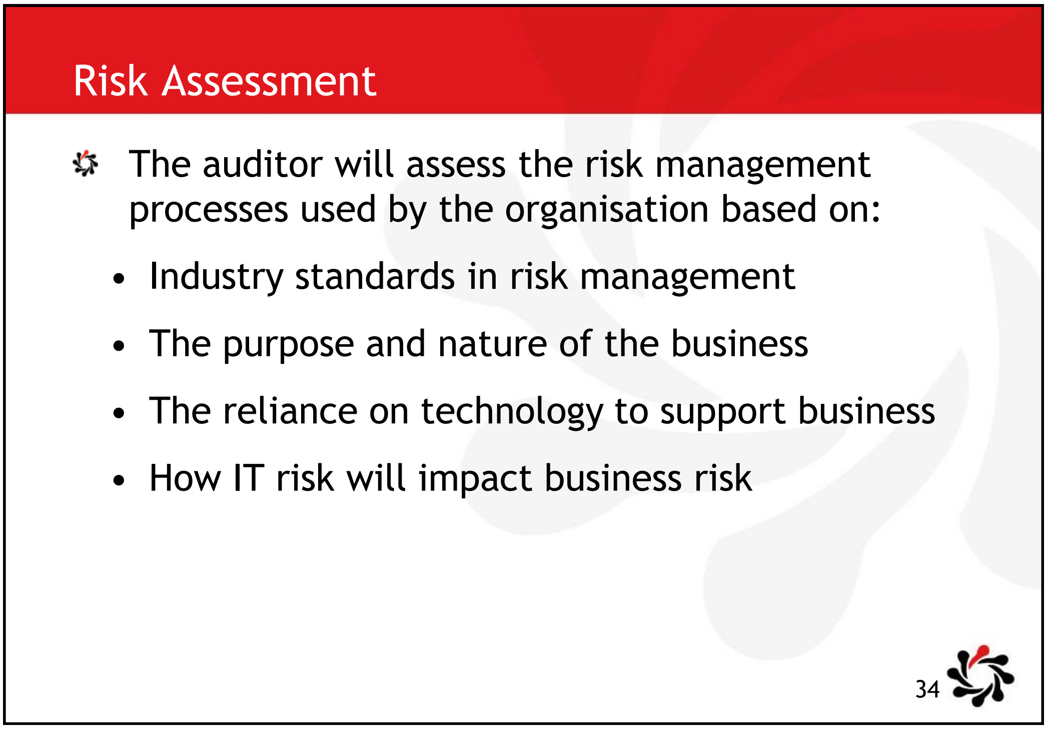
Risk Analysis

- Part of audit planning
  - Identify risk and vulnerabilities
  - Ensures controls in place to mitigate risk
- Auditors must recognise:
  - Business risk
  - Technical risk
  - Relevant controls



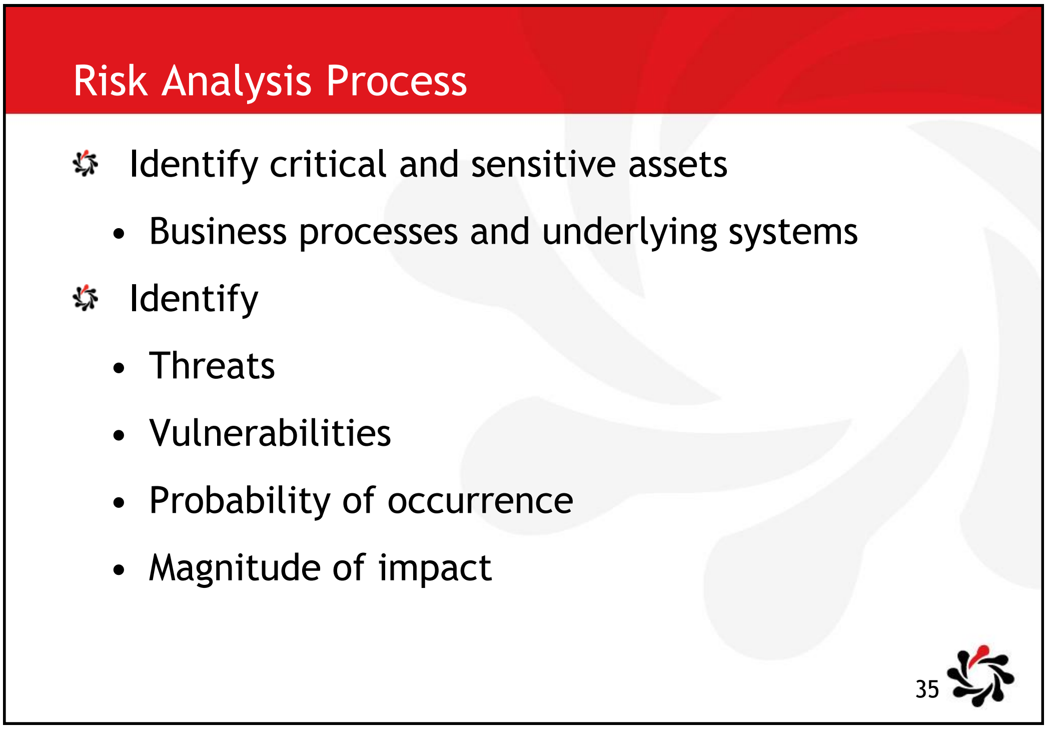
Risk Definition

- Risk is the combination of the probability of an event and its consequence (ISO3100)
- Risk to IT focuses on risk to information and information systems, and processes:
  - Confidentiality
  - Integrity
  - Availability



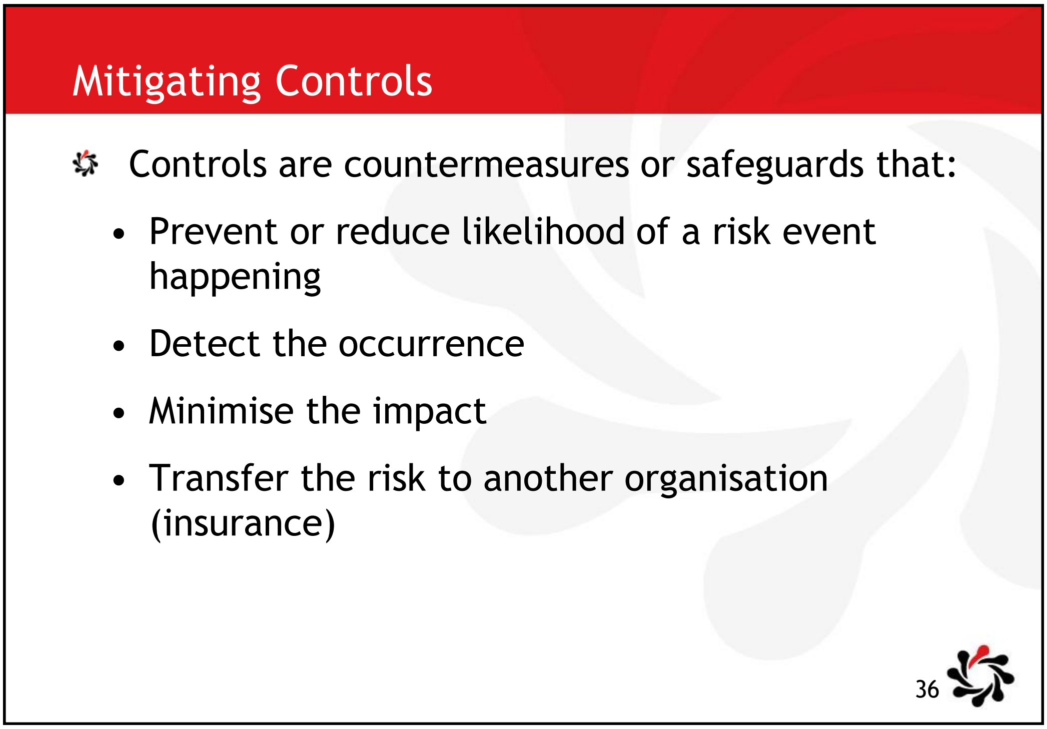
Risk Assessment

- The auditor will assess the risk management processes used by the organisation based on:
  - Industry standards in risk management
  - The purpose and nature of the business
  - The reliance on technology to support business
  - How IT risk will impact business risk



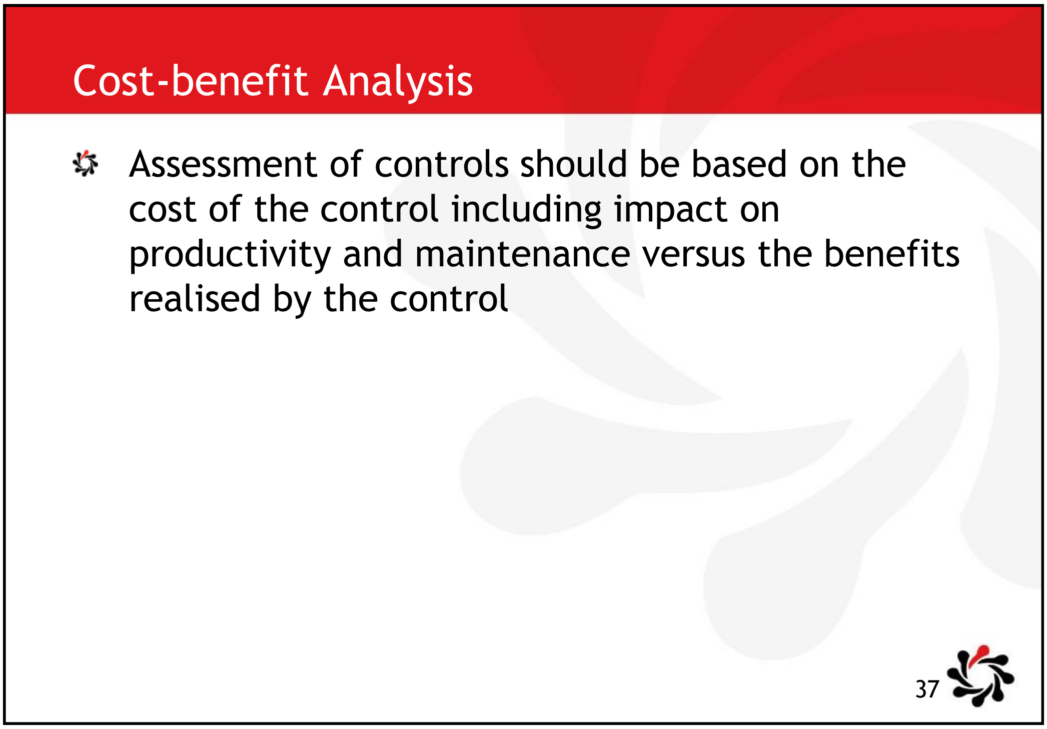
Risk Analysis Process

- Identify critical and sensitive assets
  - Business processes and underlying systems
- Identify
  - Threats
  - Vulnerabilities
  - Probability of occurrence
  - Magnitude of impact



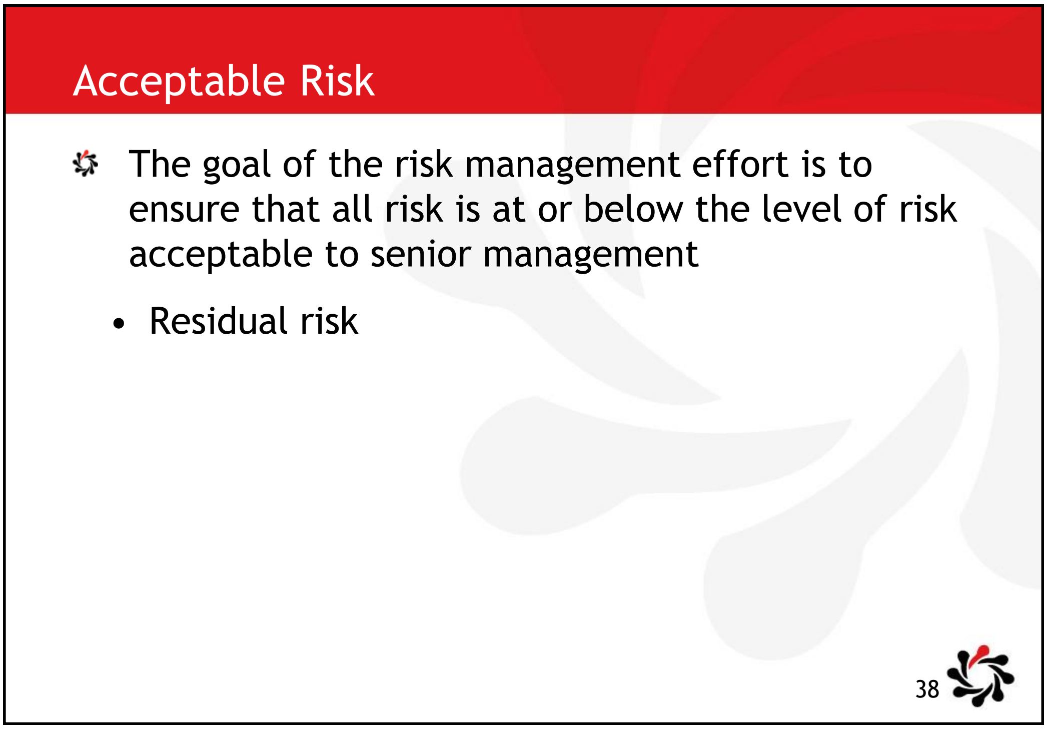
Mitigating Controls

- Controls are countermeasures or safeguards that:
  - Prevent or reduce likelihood of a risk event happening
  - Detect the occurrence
  - Minimise the impact
  - Transfer the risk to another organisation (insurance)



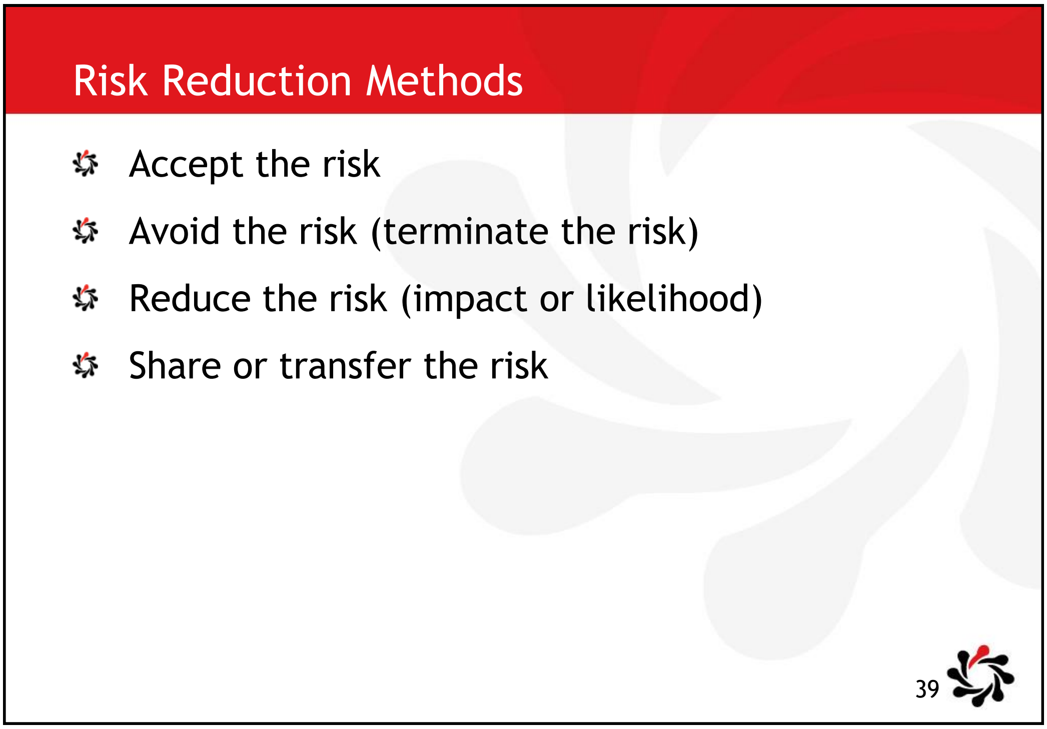
Cost-benefit Analysis

- Assessment of controls should be based on the cost of the control including impact on productivity and maintenance versus the benefits realised by the control



Acceptable Risk

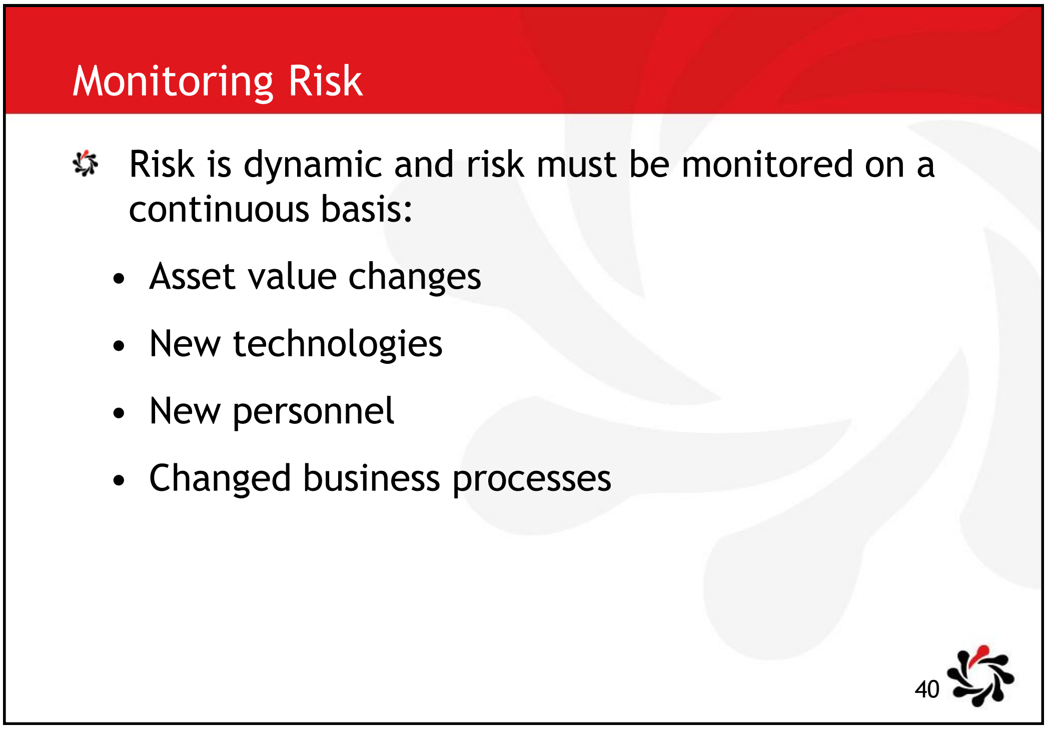
- The goal of the risk management effort is to ensure that all risk is at or below the level of risk acceptable to senior management
  - Residual risk



Risk Reduction Methods

- Accept the risk
- Avoid the risk (terminate the risk)
- Reduce the risk (impact or likelihood)
- Share or transfer the risk

39

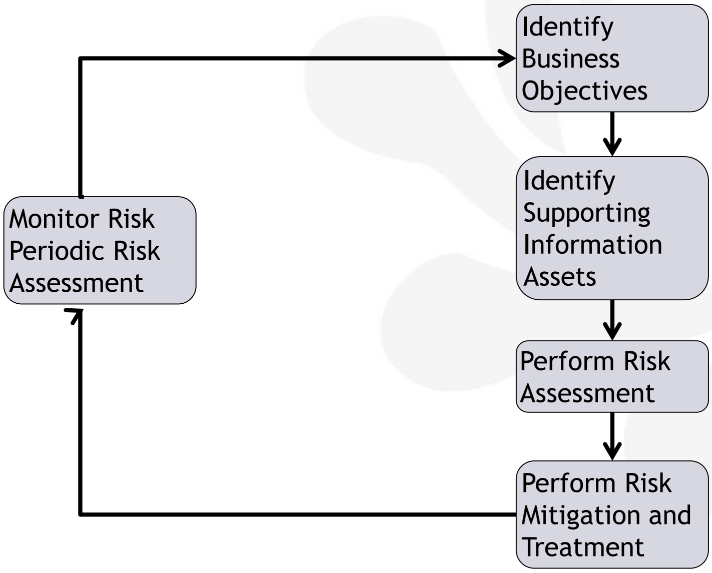


Monitoring Risk

- Risk is dynamic and risk must be monitored on a continuous basis:
  - Asset value changes
  - New technologies
  - New personnel
  - Changed business processes

40

Overview of Risk Management



Identify Business Objectives

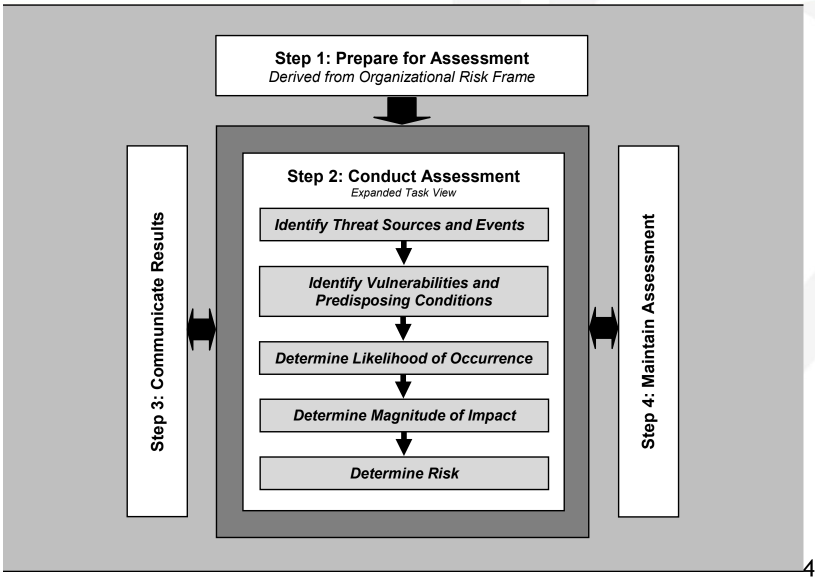
Identify Supporting Information Assets

Perform Risk Assessment

Perform Risk Mitigation and Treatment

Monitor Risk Periodic Risk Assessment

NIST SP800-30 Risk Assessment Process



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

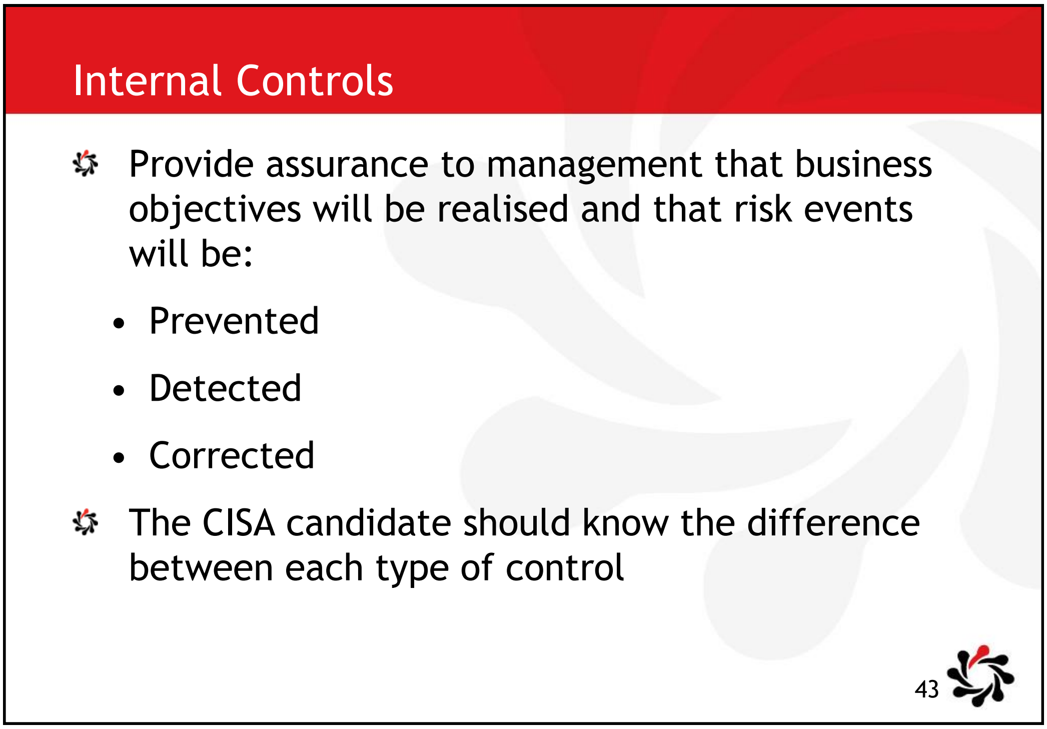
Determine Likelihood of Occurrence

Determine Magnitude of Impact

Determine Risk

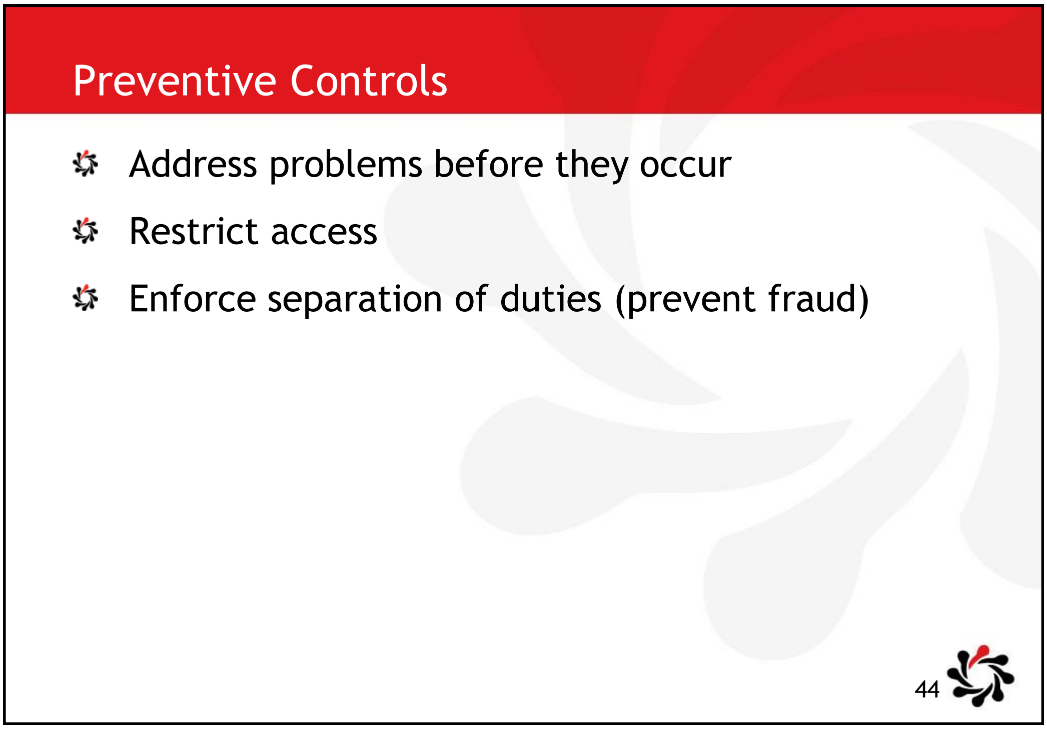
Step 3: Communicate Results

Step 4: Maintain Assessment



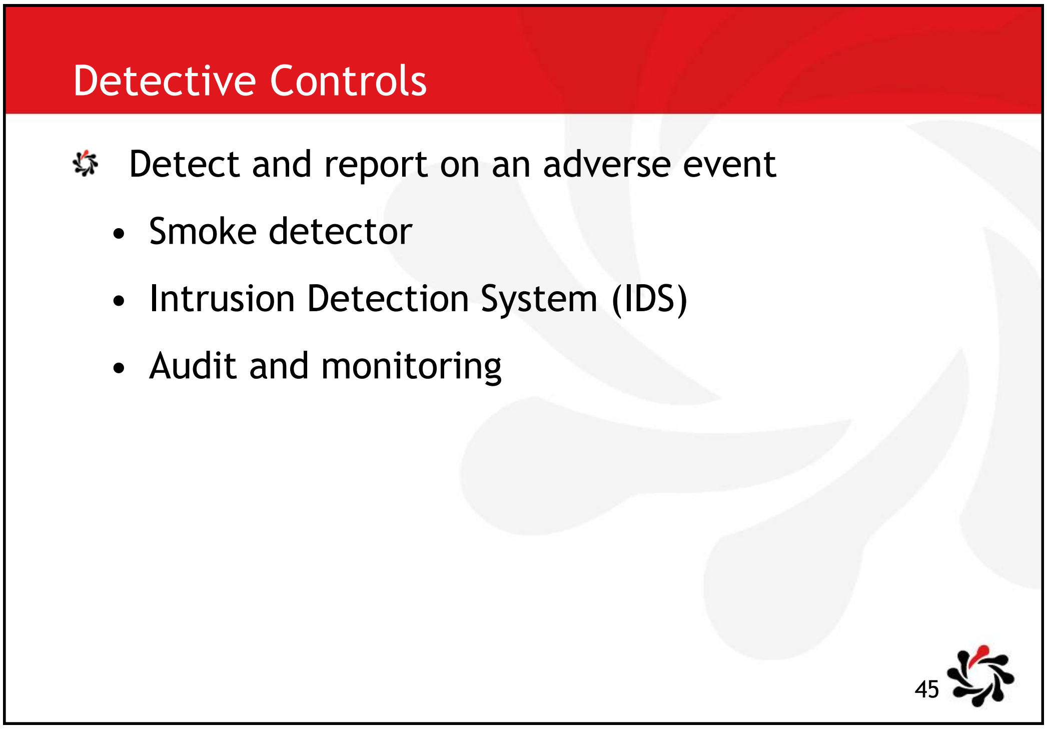
Internal Controls

- Provide assurance to management that business objectives will be realised and that risk events will be:
  - Prevented
  - Detected
  - Corrected
- The CISA candidate should know the difference between each type of control



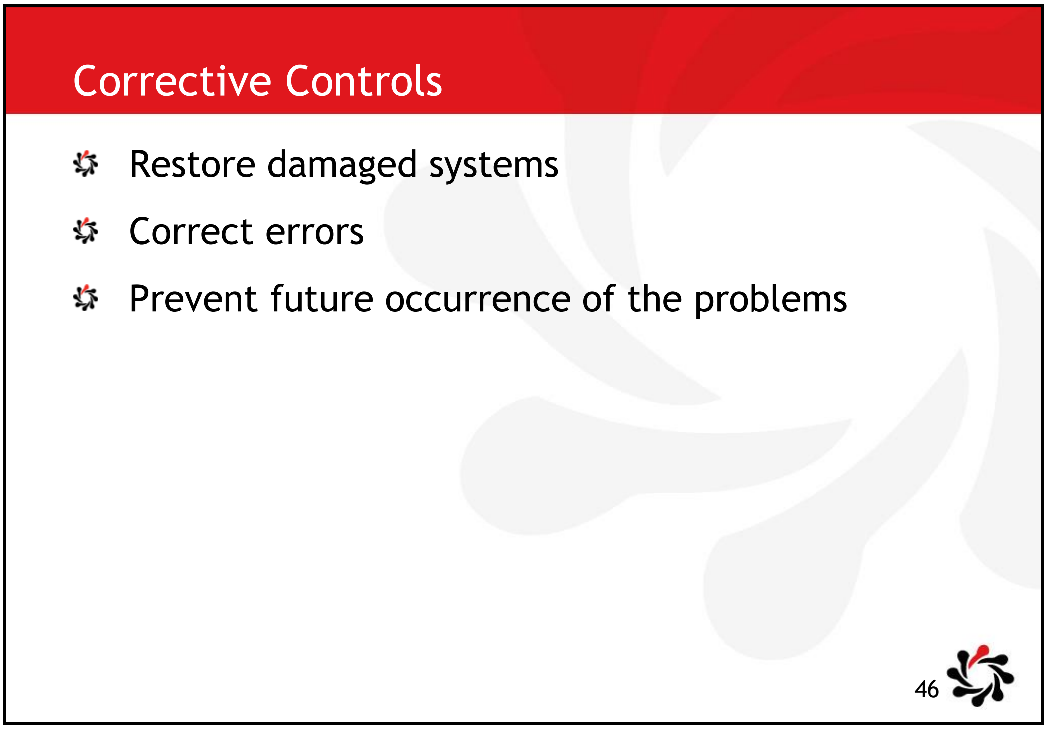
Preventive Controls

- Address problems before they occur
- Restrict access
- Enforce separation of duties (prevent fraud)



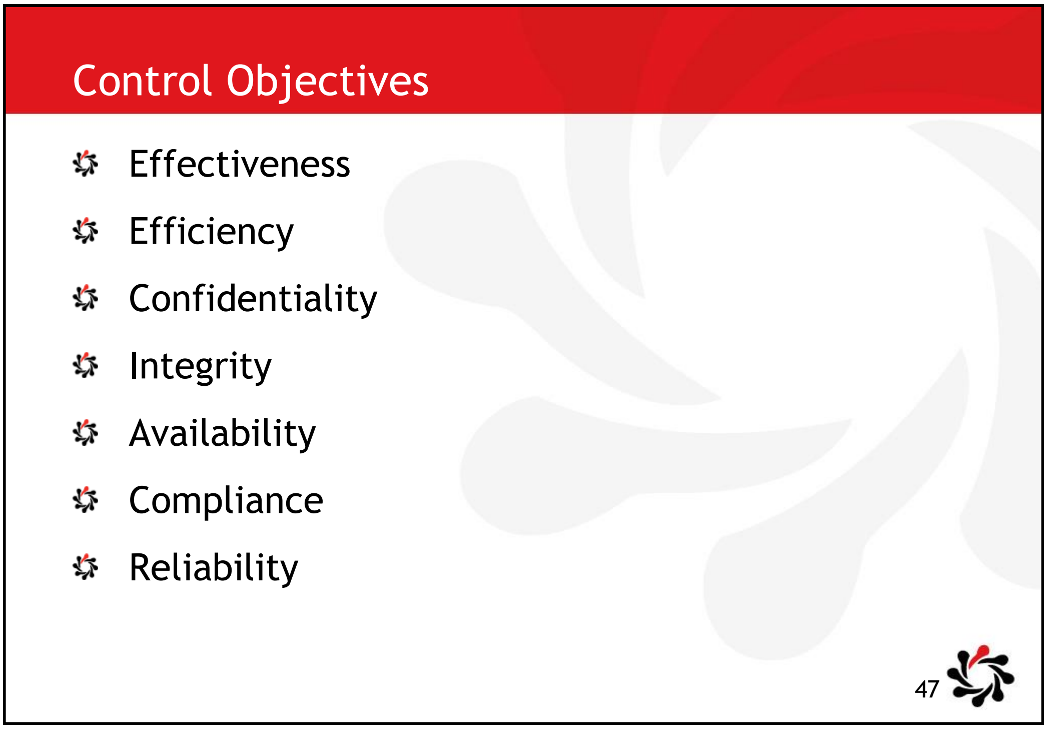
Detective Controls

- Detect and report on an adverse event
  - Smoke detector
  - Intrusion Detection System (IDS)
  - Audit and monitoring



Corrective Controls

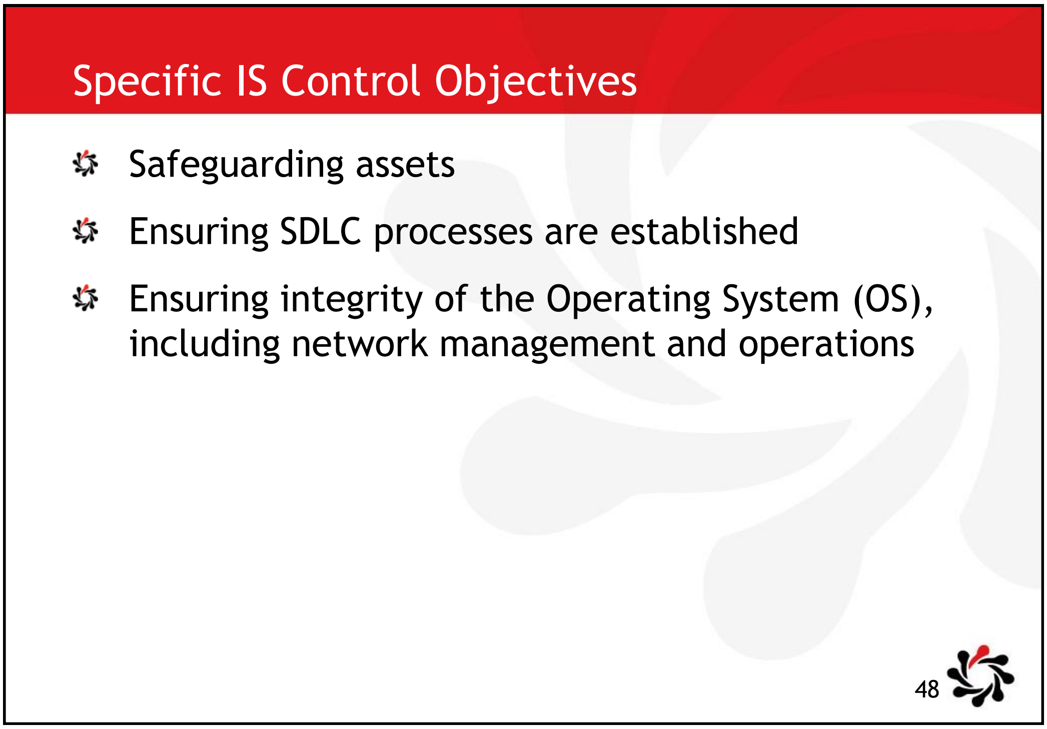
- Restore damaged systems
- Correct errors
- Prevent future occurrence of the problems



Control Objectives

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

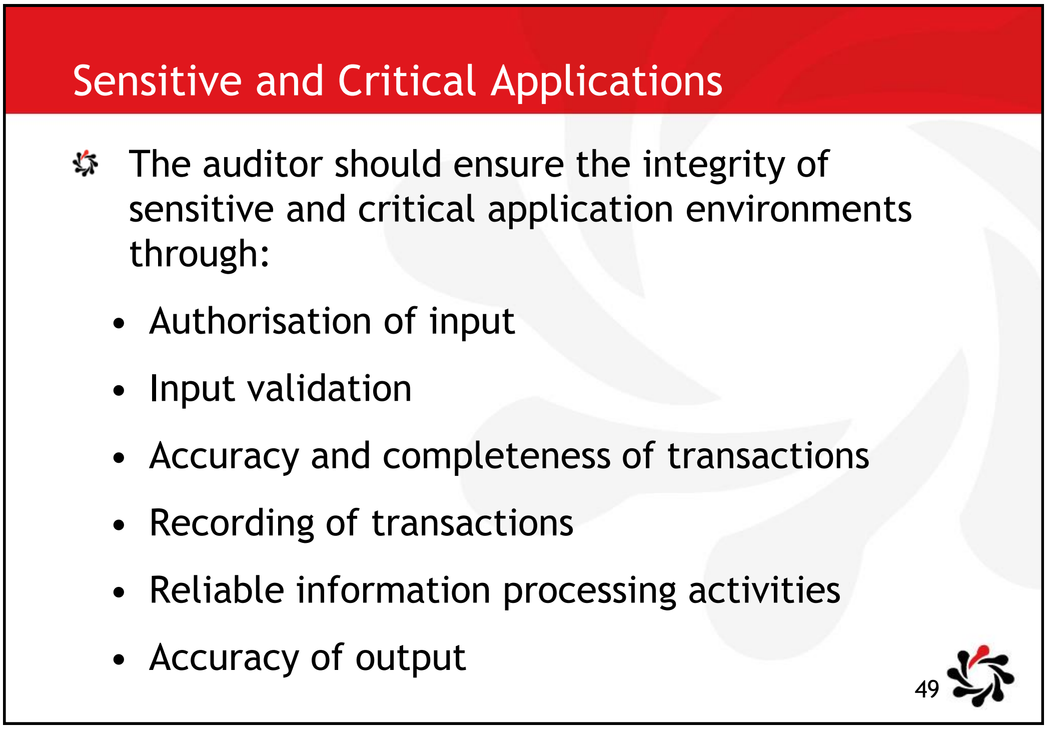
47



Specific IS Control Objectives

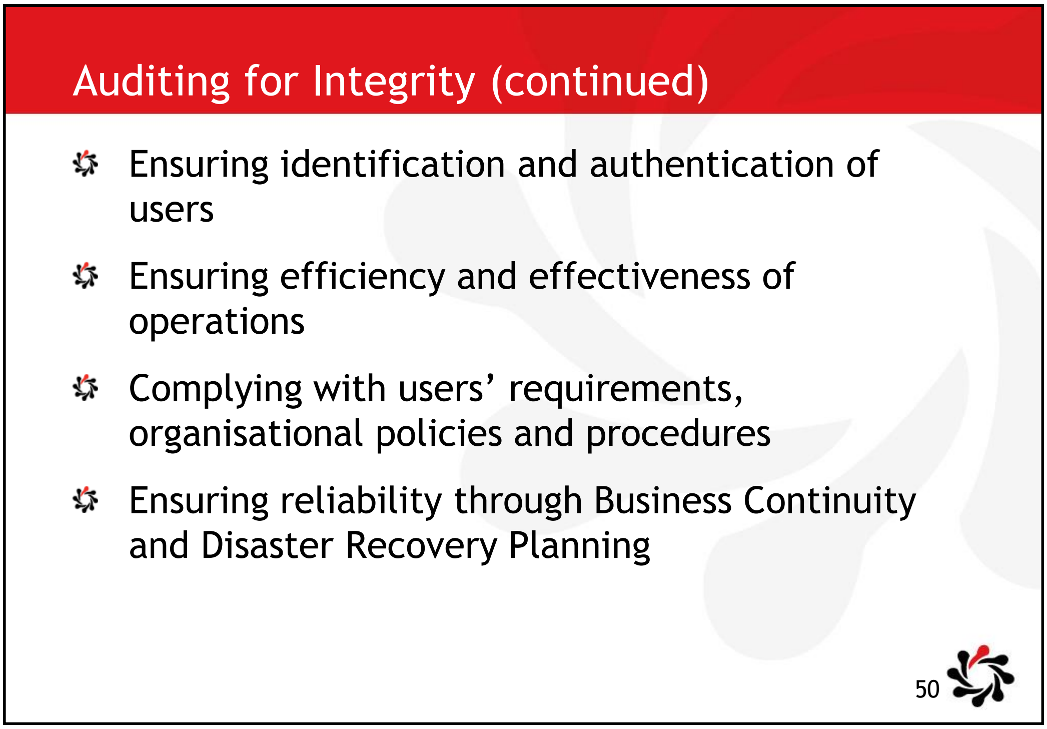
- Safeguarding assets
- Ensuring SDLC processes are established
- Ensuring integrity of the Operating System (OS), including network management and operations

48



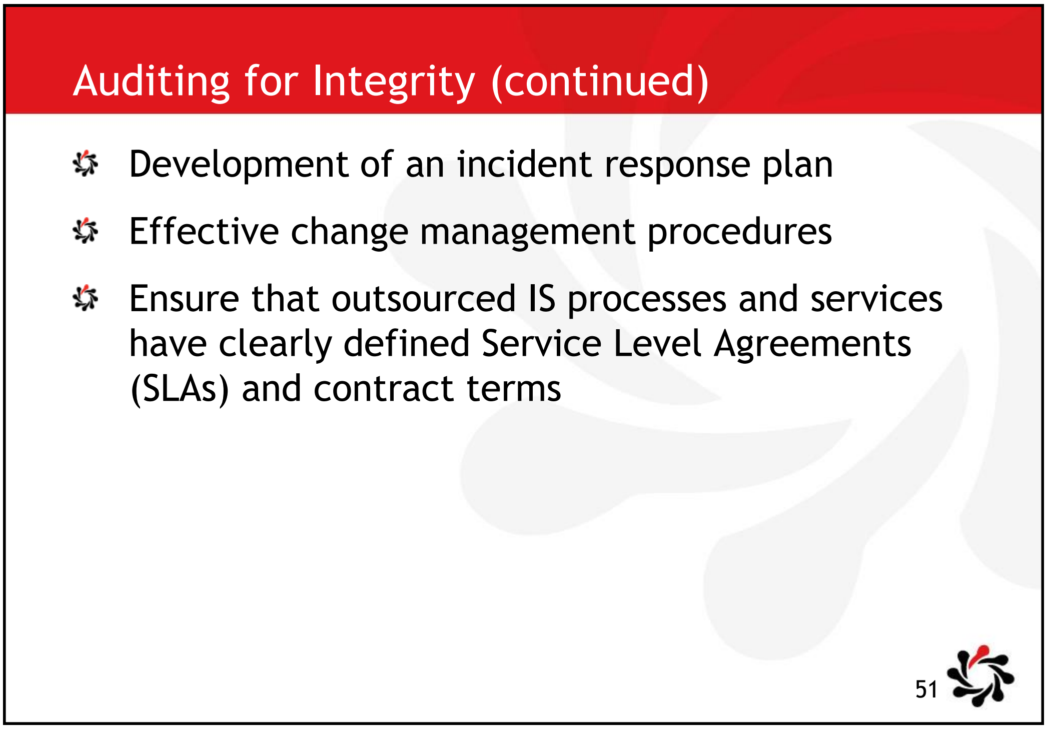
Sensitive and Critical Applications

- The auditor should ensure the integrity of sensitive and critical application environments through:
  - Authorisation of input
  - Input validation
  - Accuracy and completeness of transactions
  - Recording of transactions
  - Reliable information processing activities
  - Accuracy of output



Auditing for Integrity (continued)

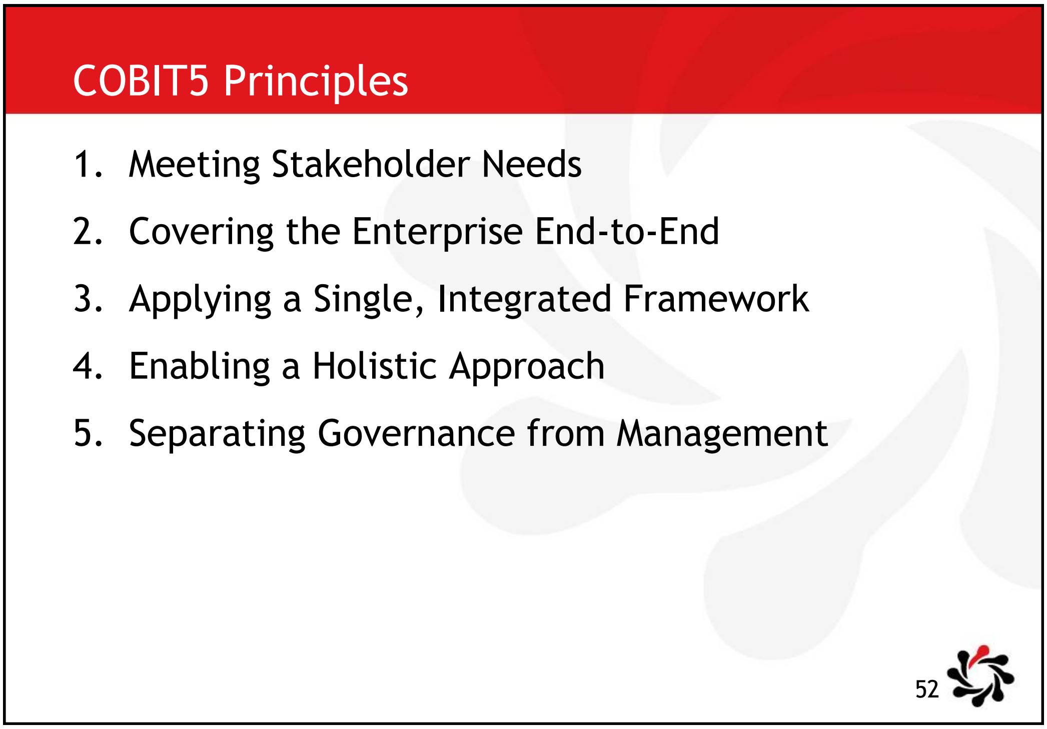
- Ensuring identification and authentication of users
- Ensuring efficiency and effectiveness of operations
- Complying with users’ requirements, organisational policies and procedures
- Ensuring reliability through Business Continuity and Disaster Recovery Planning



Auditing for Integrity (continued)

- Development of an incident response plan
- Effective change management procedures
- Ensure that outsourced IS processes and services have clearly defined Service Level Agreements (SLAs) and contract terms

51



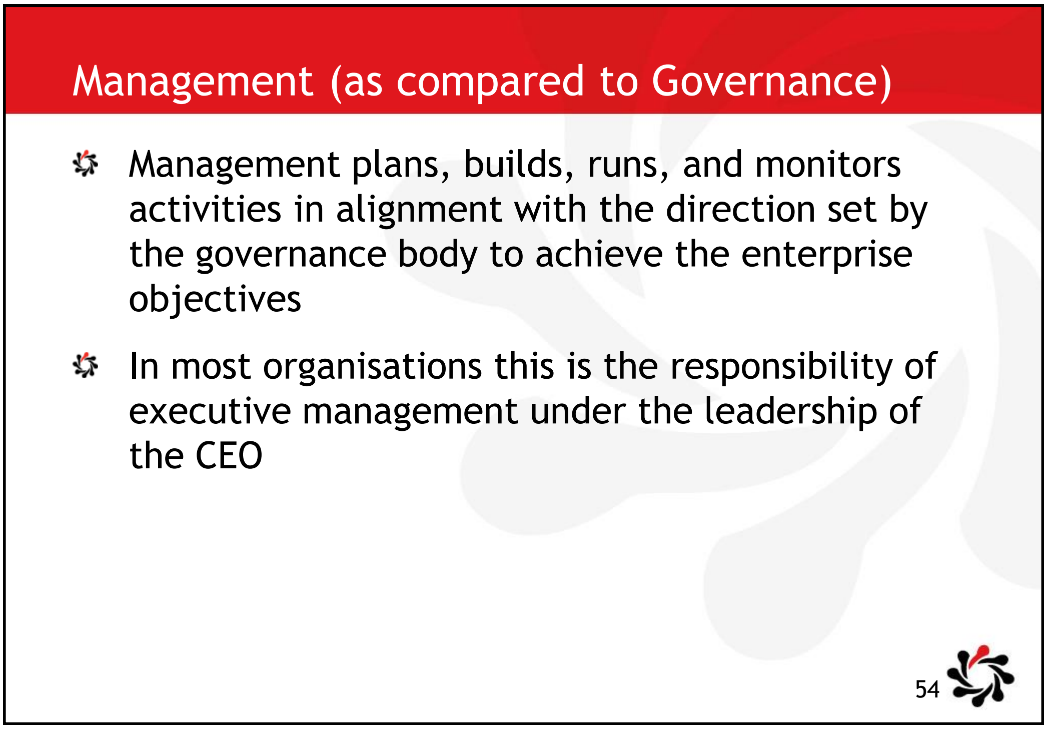
COBIT5 Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-End
3. Applying a Single, Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance from Management

52

Governance

- Ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives
- Responsibility of the Board of Directors



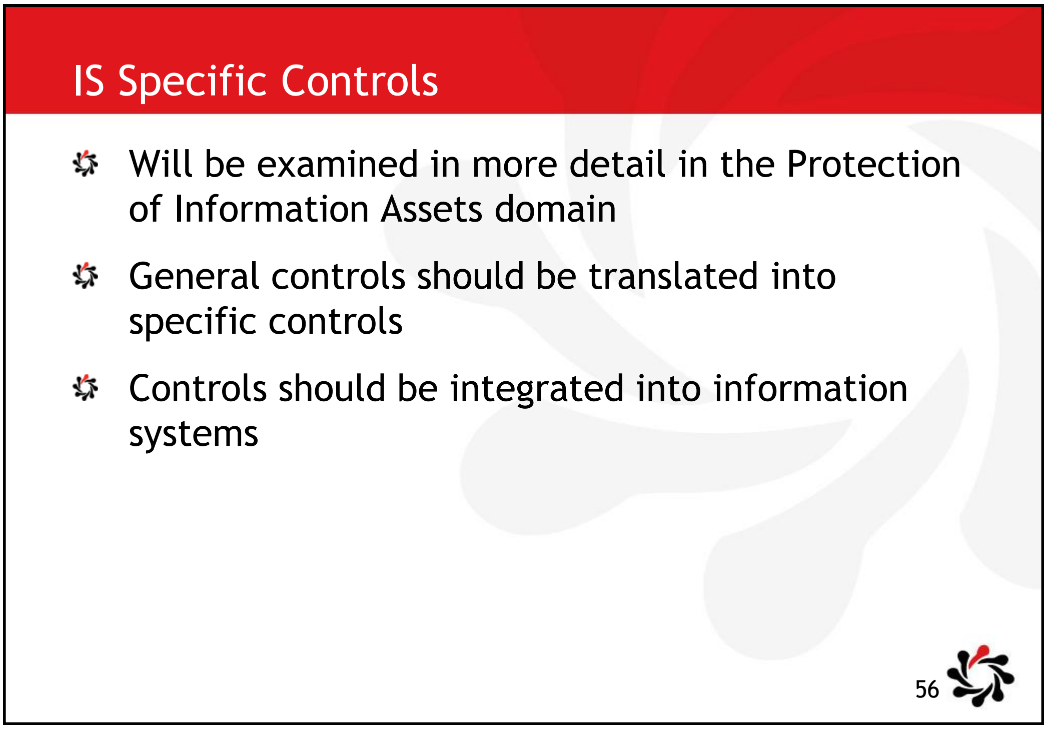
Management (as compared to Governance)

- Management plans, builds, runs, and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
- In most organisations this is the responsibility of executive management under the leadership of the CEO

General Controls

- General controls include:
  - Internal accounting controls
  - Operational controls
  - Administrative controls
  - Organisational security policies and procedures
  - Audit trail and recording of transactions
  - Controls over access to the facility
  - Physical and logical security policies

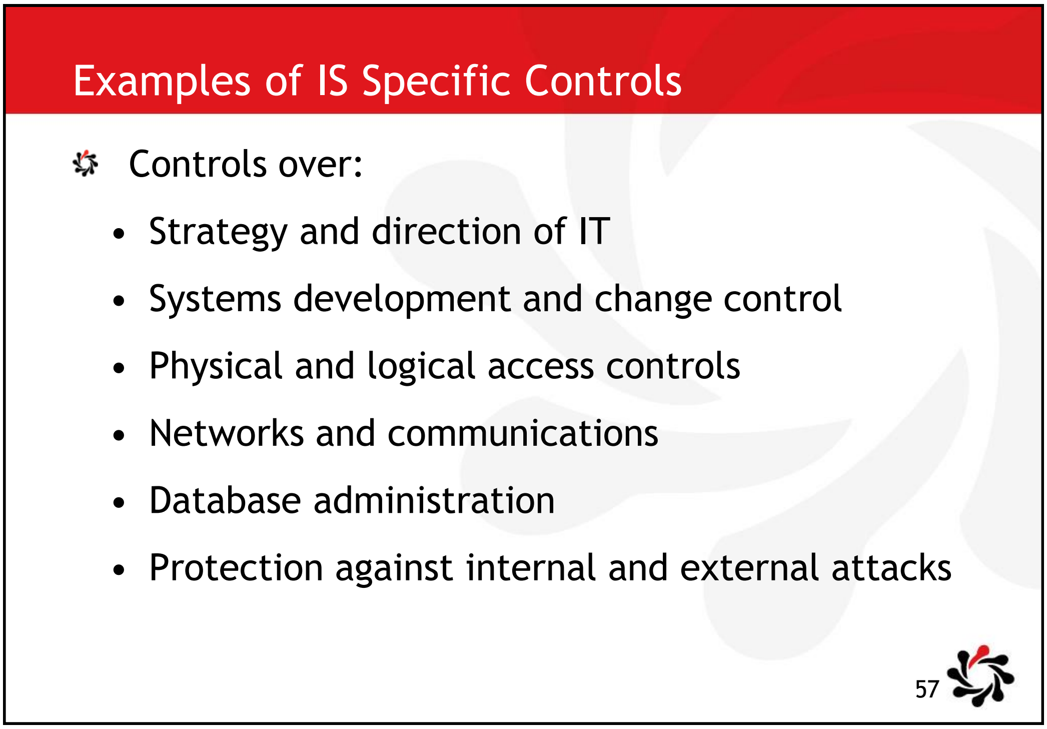
55



IS Specific Controls

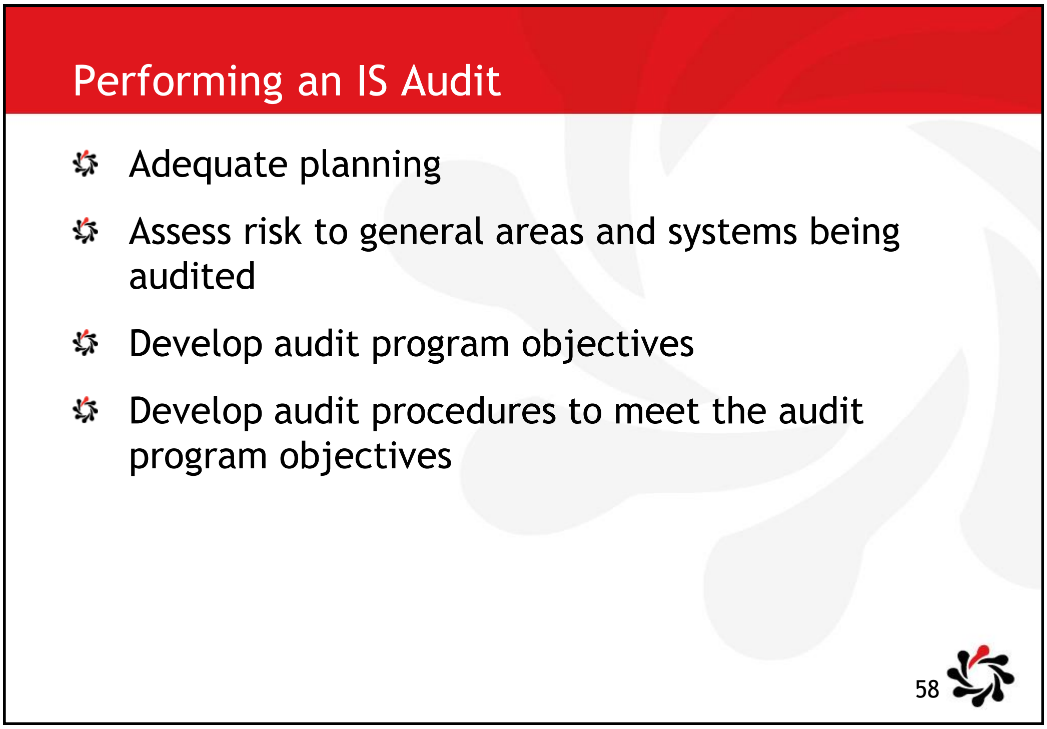
- Will be examined in more detail in the Protection of Information Assets domain
- General controls should be translated into specific controls
- Controls should be integrated into information systems

56



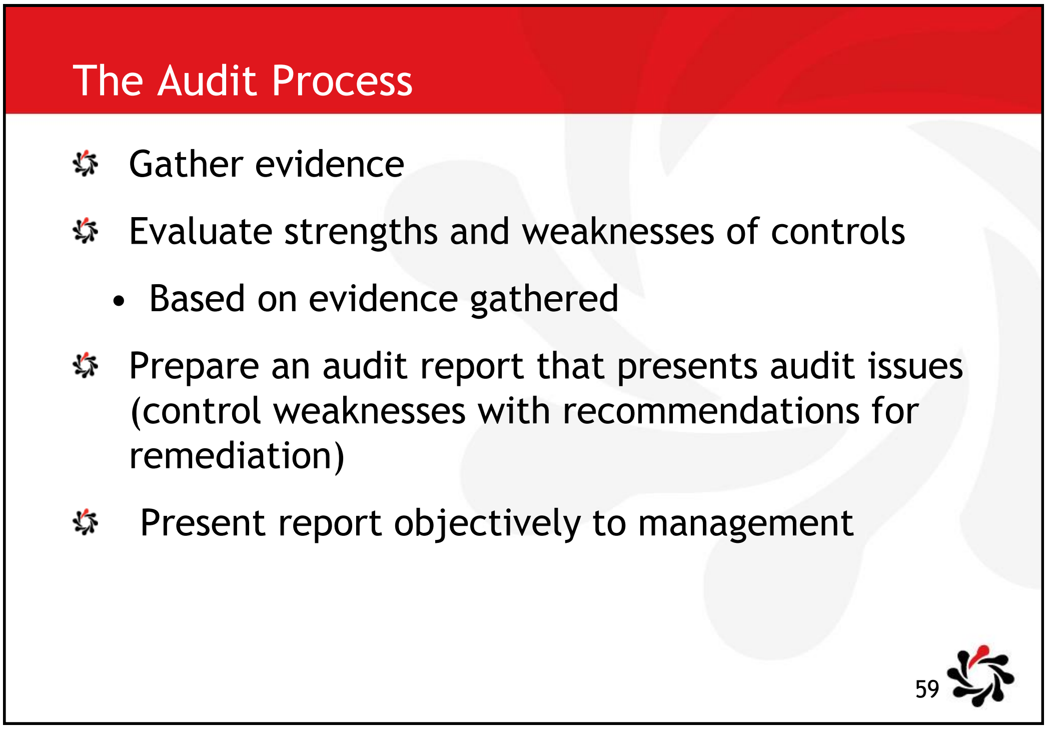
Examples of IS Specific Controls

- Controls over:
  - Strategy and direction of IT
  - Systems development and change control
  - Physical and logical access controls
  - Networks and communications
  - Database administration
  - Protection against internal and external attacks



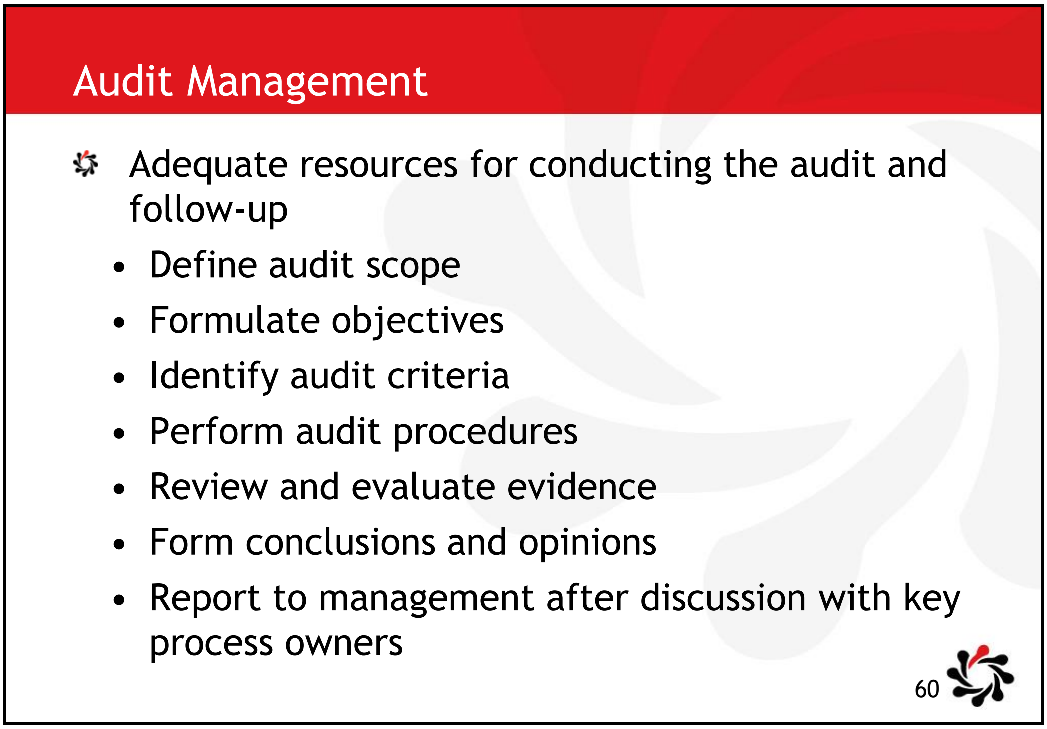
Performing an IS Audit

- Adequate planning
- Assess risk to general areas and systems being audited
- Develop audit program objectives
- Develop audit procedures to meet the audit program objectives



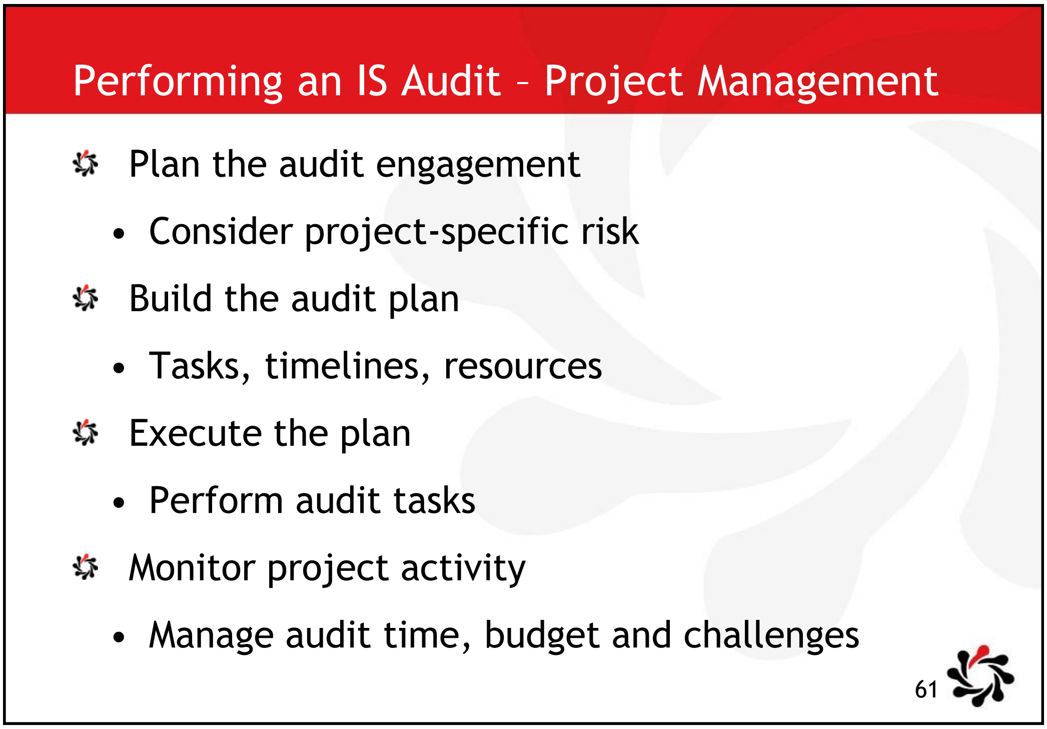
The Audit Process

- Gather evidence
- Evaluate strengths and weaknesses of controls
  - Based on evidence gathered
- Prepare an audit report that presents audit issues (control weaknesses with recommendations for remediation)
- Present report objectively to management



Audit Management

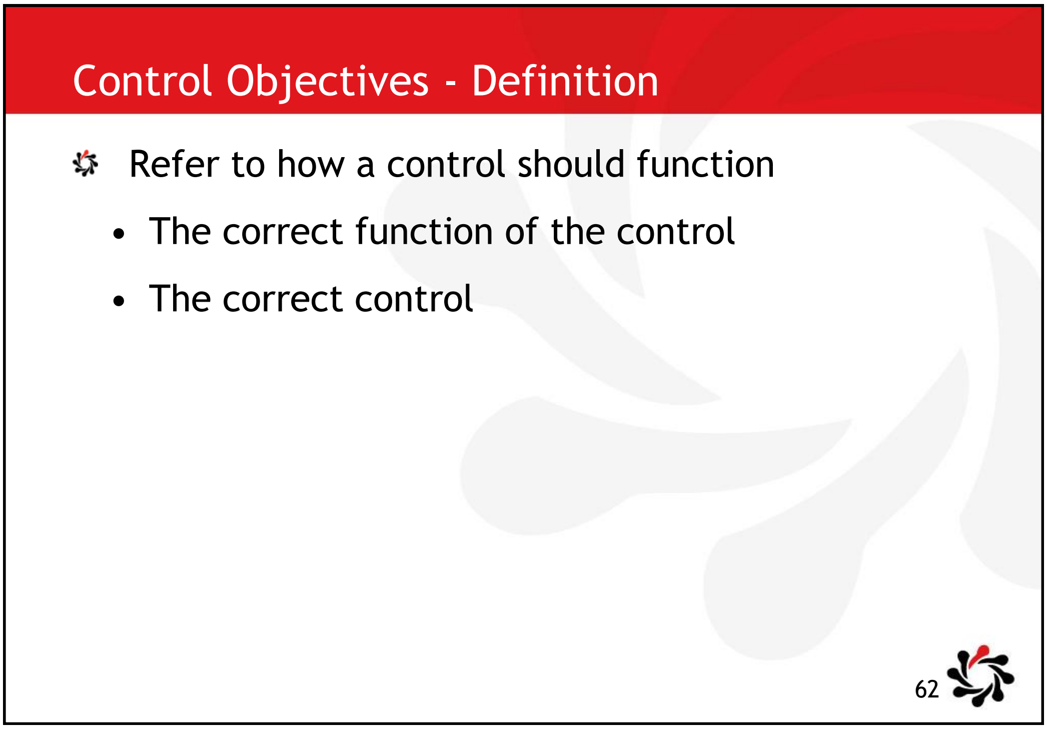
- Adequate resources for conducting the audit and follow-up
  - Define audit scope
  - Formulate objectives
  - Identify audit criteria
  - Perform audit procedures
  - Review and evaluate evidence
  - Form conclusions and opinions
  - Report to management after discussion with key process owners



Performing an IS Audit – Project Management

- Plan the audit engagement
  - Consider project-specific risk
- Build the audit plan
  - Tasks, timelines, resources
- Execute the plan
  - Perform audit tasks
- Monitor project activity
  - Manage audit time, budget and challenges

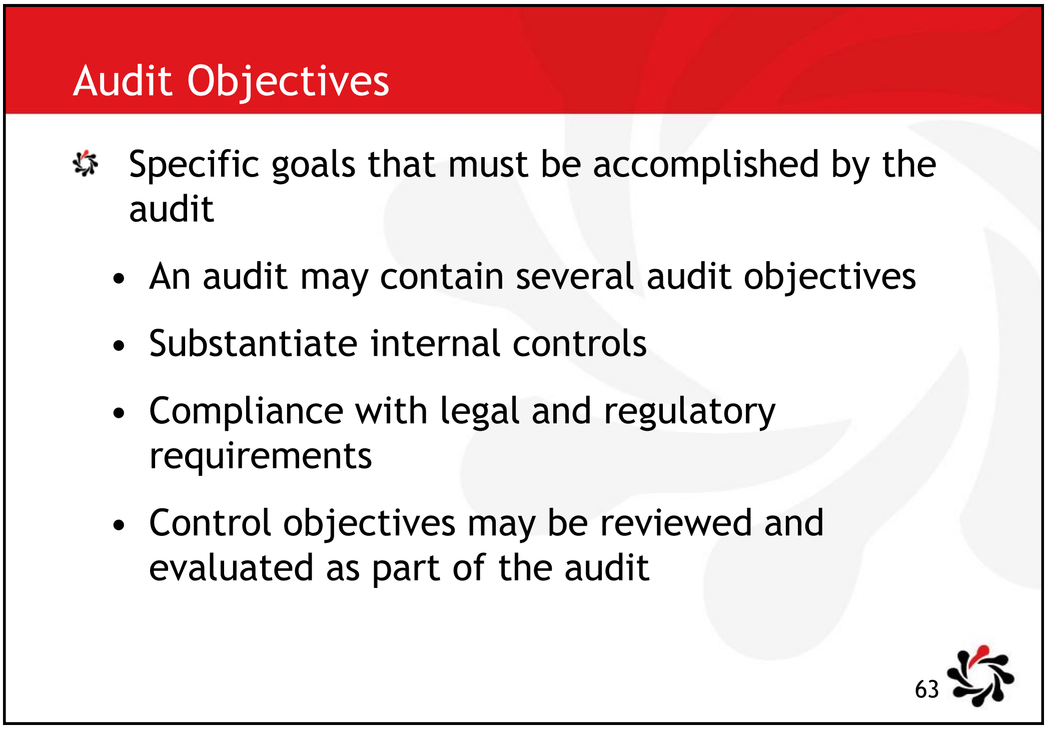
61



Control Objectives - Definition

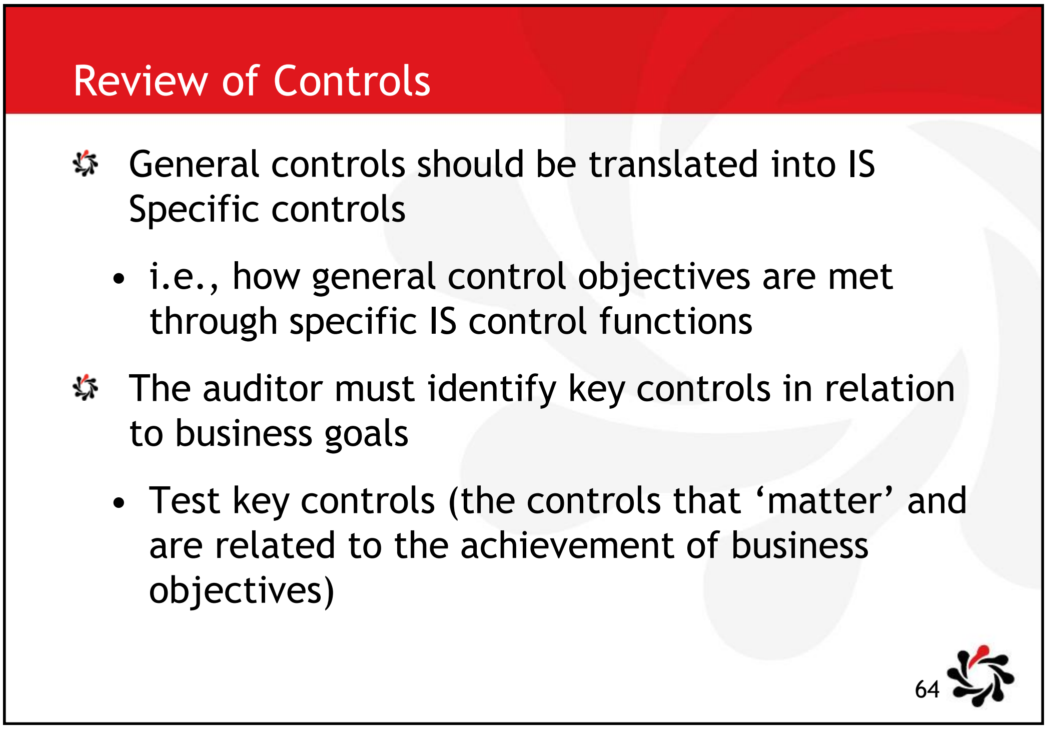
- Refer to how a control should function
  - The correct function of the control
  - The correct control

62



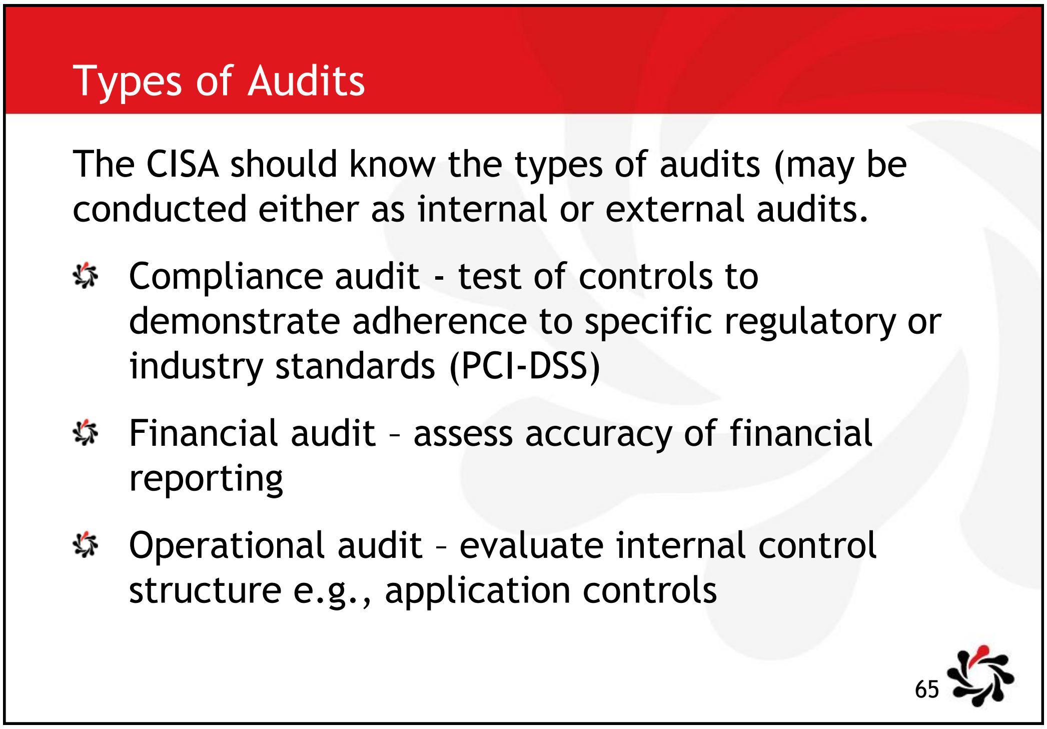
Audit Objectives

- Specific goals that must be accomplished by the audit
  - An audit may contain several audit objectives
  - Substantiate internal controls
  - Compliance with legal and regulatory requirements
  - Control objectives may be reviewed and evaluated as part of the audit



Review of Controls

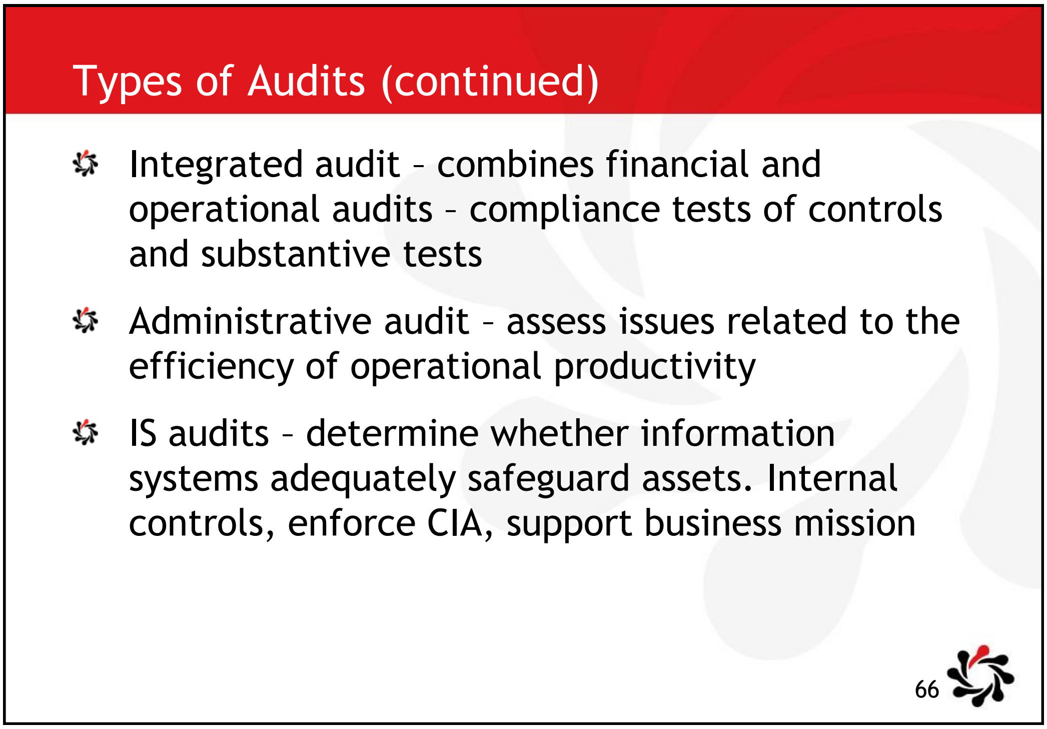
- General controls should be translated into IS Specific controls
  - i.e., how general control objectives are met through specific IS control functions
- The auditor must identify key controls in relation to business goals
  - Test key controls (the controls that ‘matter’ and are related to the achievement of business objectives)



Types of Audits

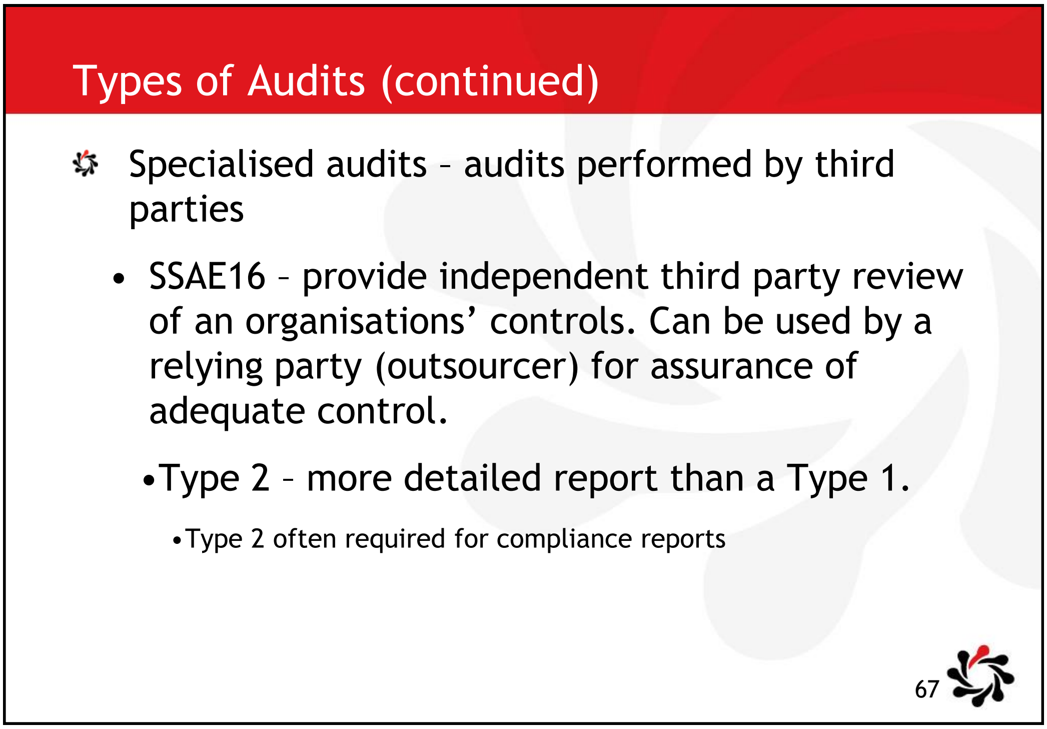
The CISA should know the types of audits (may be conducted either as internal or external audits.

- Compliance audit - test of controls to demonstrate adherence to specific regulatory or industry standards (PCI-DSS)
- Financial audit – assess accuracy of financial reporting
- Operational audit – evaluate internal control structure e.g., application controls



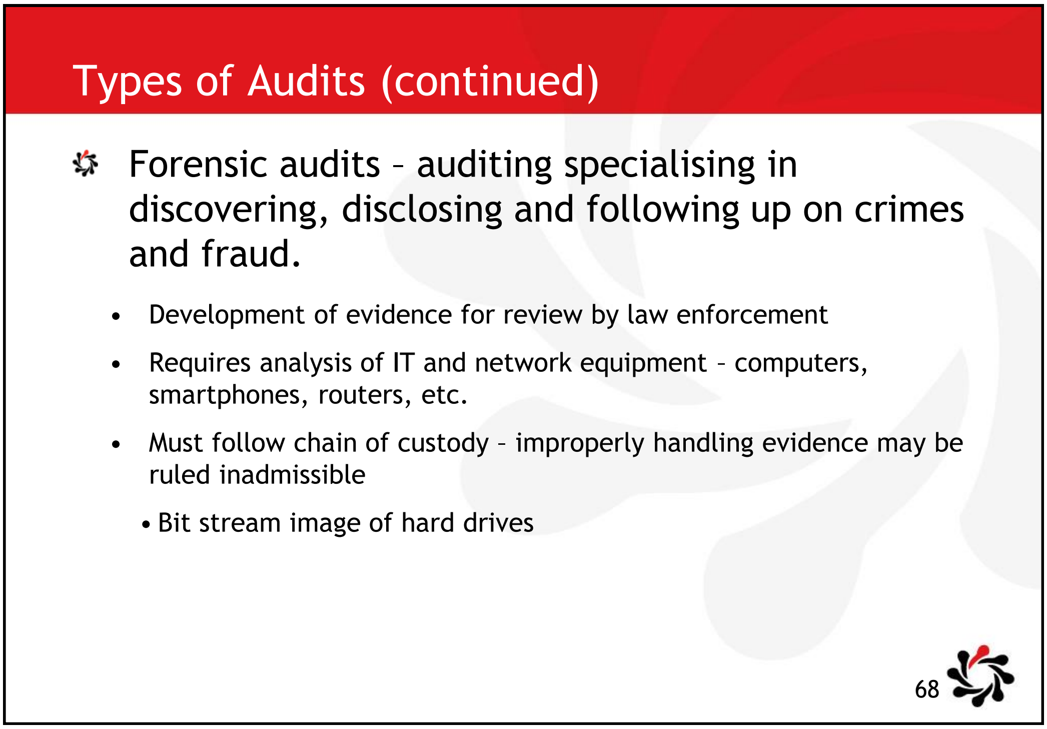
Types of Audits (continued)

- Integrated audit – combines financial and operational audits – compliance tests of controls and substantive tests
- Administrative audit – assess issues related to the efficiency of operational productivity
- IS audits – determine whether information systems adequately safeguard assets. Internal controls, enforce CIA, support business mission



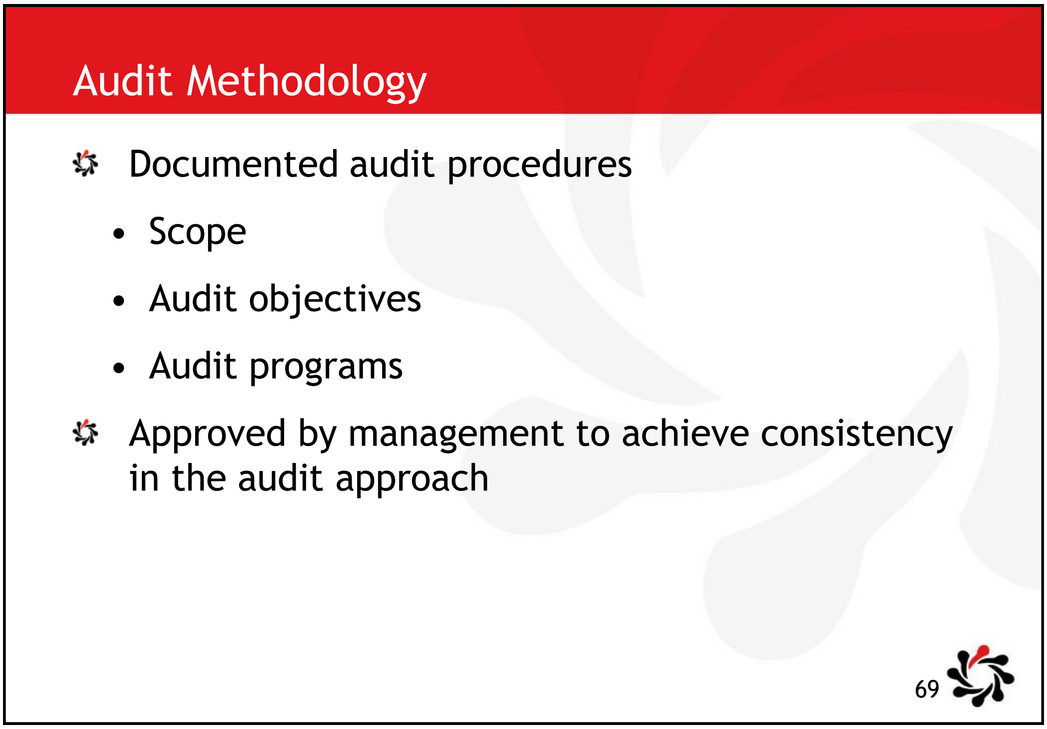
Types of Audits (continued)

- Specialised audits – audits performed by third parties
  - SSAE16 – provide independent third party review of an organisations' controls. Can be used by a relying party (outsourcer) for assurance of adequate control.
    - Type 2 – more detailed report than a Type 1.
      - Type 2 often required for compliance reports



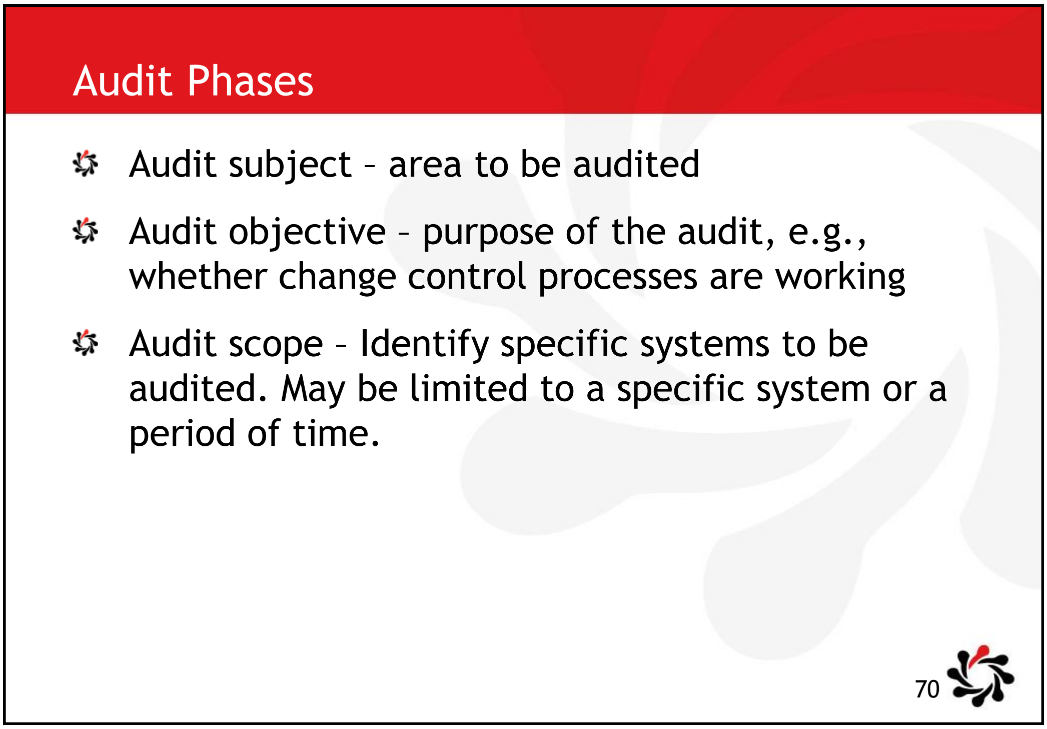
Types of Audits (continued)

- Forensic audits – auditing specialising in discovering, disclosing and following up on crimes and fraud.
  - Development of evidence for review by law enforcement
  - Requires analysis of IT and network equipment – computers, smartphones, routers, etc.
  - Must follow chain of custody – improperly handling evidence may be ruled inadmissible
    - Bit stream image of hard drives



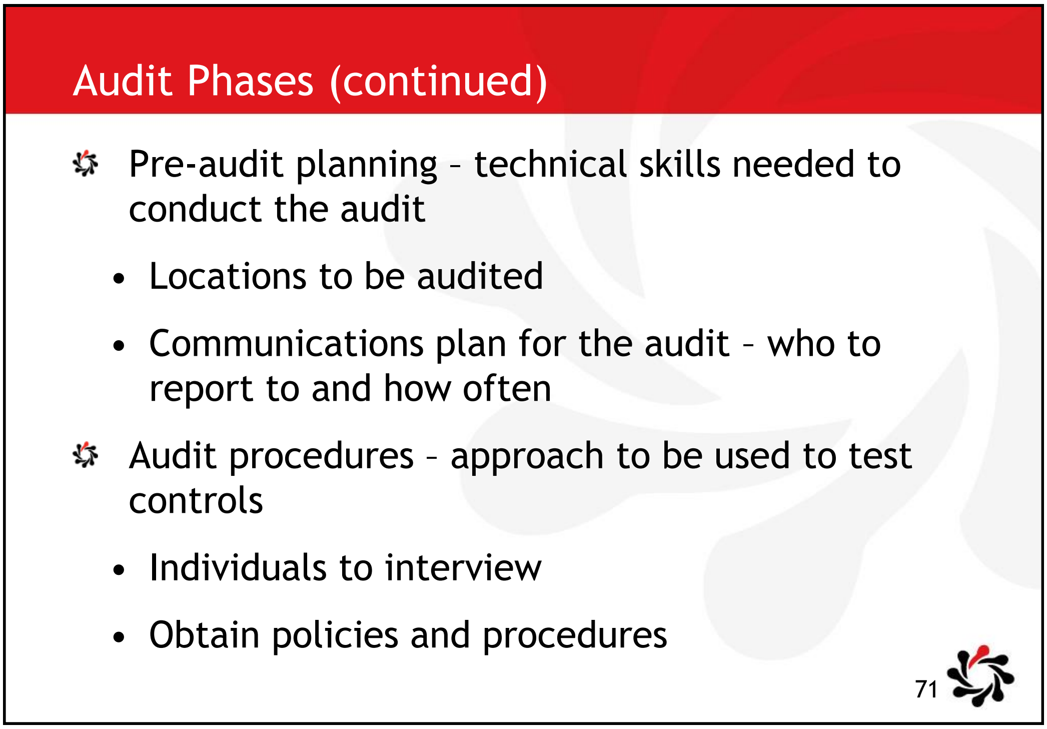
Audit Methodology

- Documented audit procedures
  - Scope
  - Audit objectives
  - Audit programs
- Approved by management to achieve consistency in the audit approach



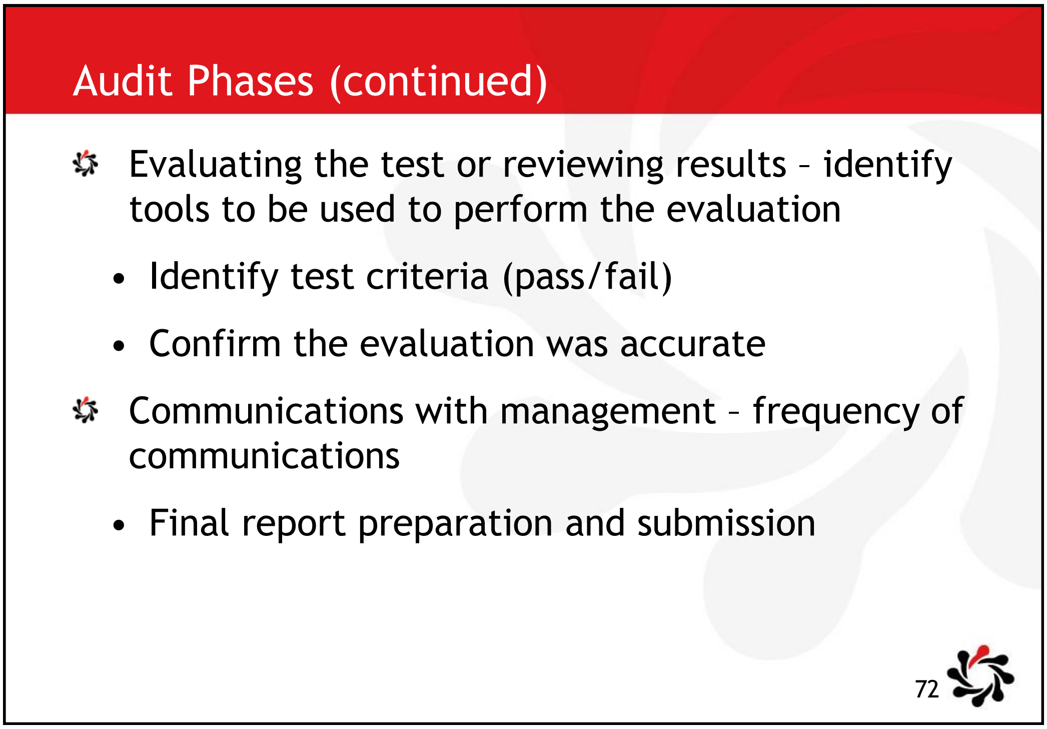
Audit Phases

- Audit subject – area to be audited
- Audit objective – purpose of the audit, e.g., whether change control processes are working
- Audit scope – Identify specific systems to be audited. May be limited to a specific system or a period of time.



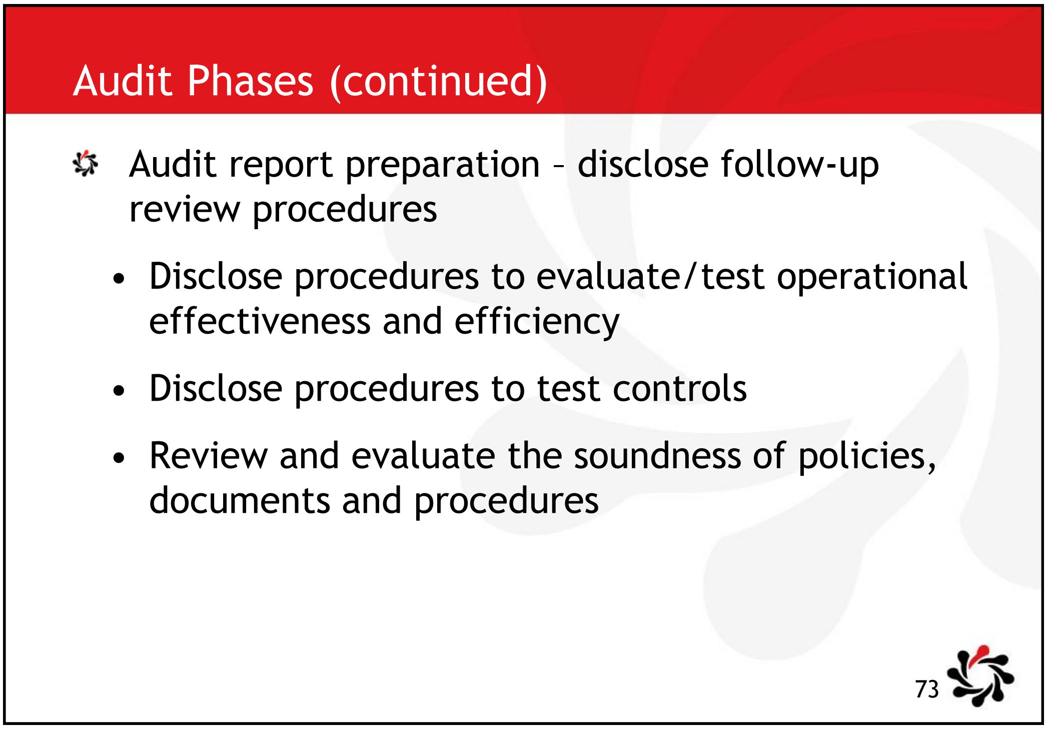
Audit Phases (continued)

- Pre-audit planning – technical skills needed to conduct the audit
  - Locations to be audited
  - Communications plan for the audit – who to report to and how often
- Audit procedures – approach to be used to test controls
  - Individuals to interview
  - Obtain policies and procedures



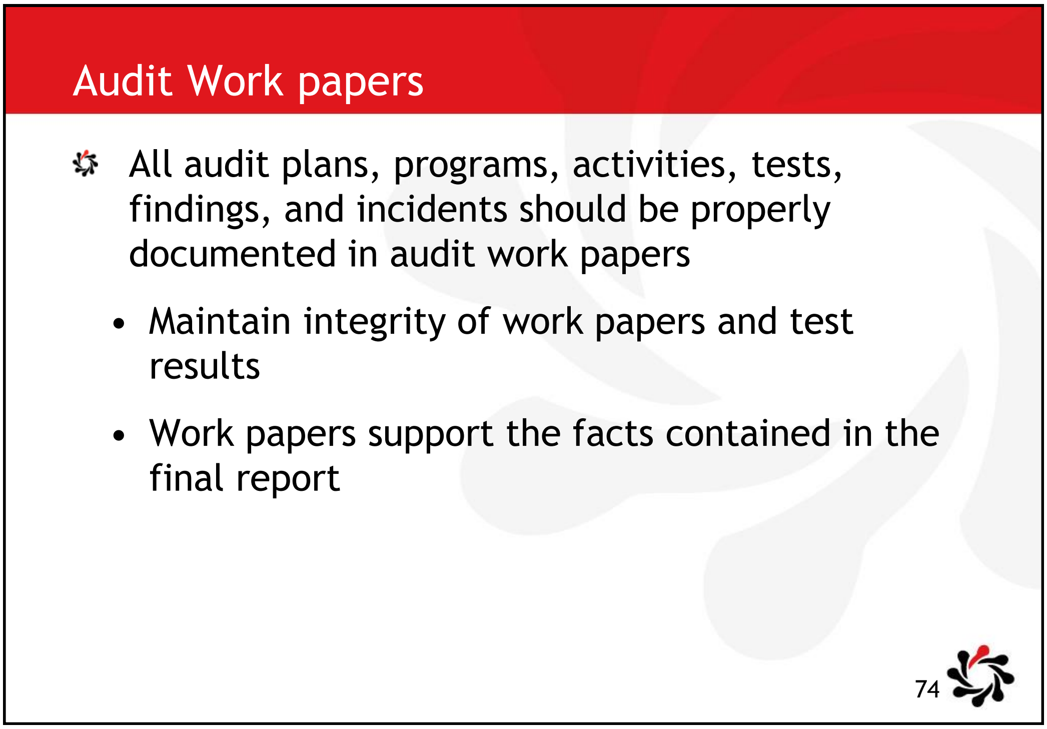
Audit Phases (continued)

- Evaluating the test or reviewing results – identify tools to be used to perform the evaluation
  - Identify test criteria (pass/fail)
  - Confirm the evaluation was accurate
- Communications with management – frequency of communications
  - Final report preparation and submission



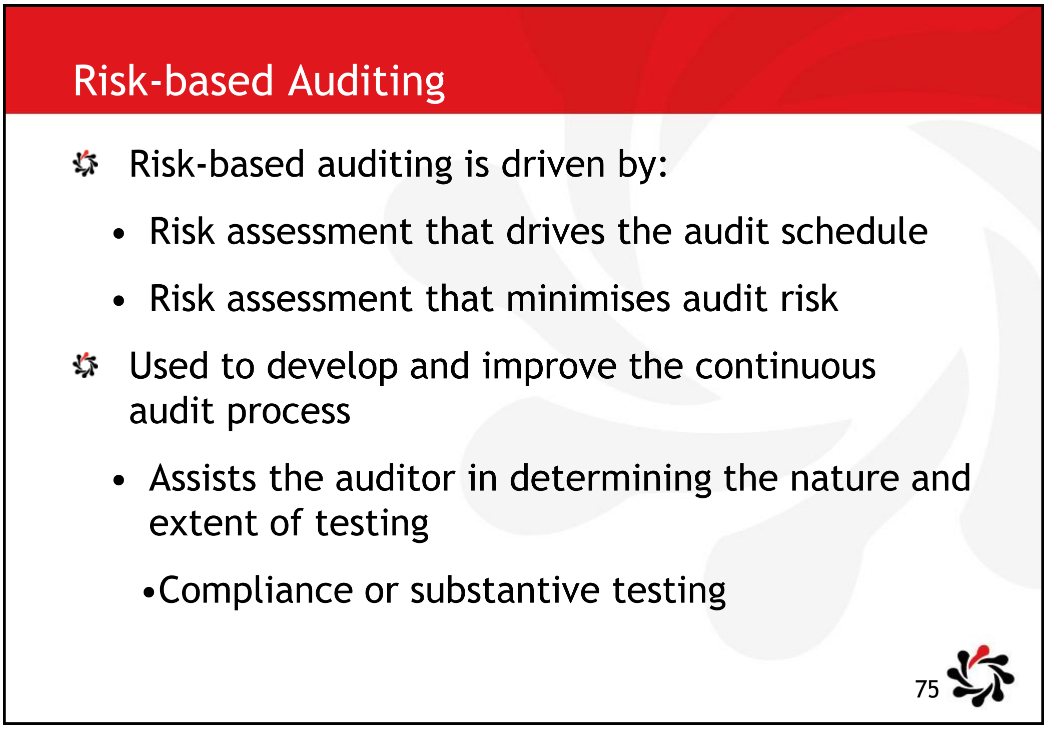
Audit Phases (continued)

- Audit report preparation – disclose follow-up review procedures
  - Disclose procedures to evaluate/test operational effectiveness and efficiency
  - Disclose procedures to test controls
  - Review and evaluate the soundness of policies, documents and procedures



Audit Work papers

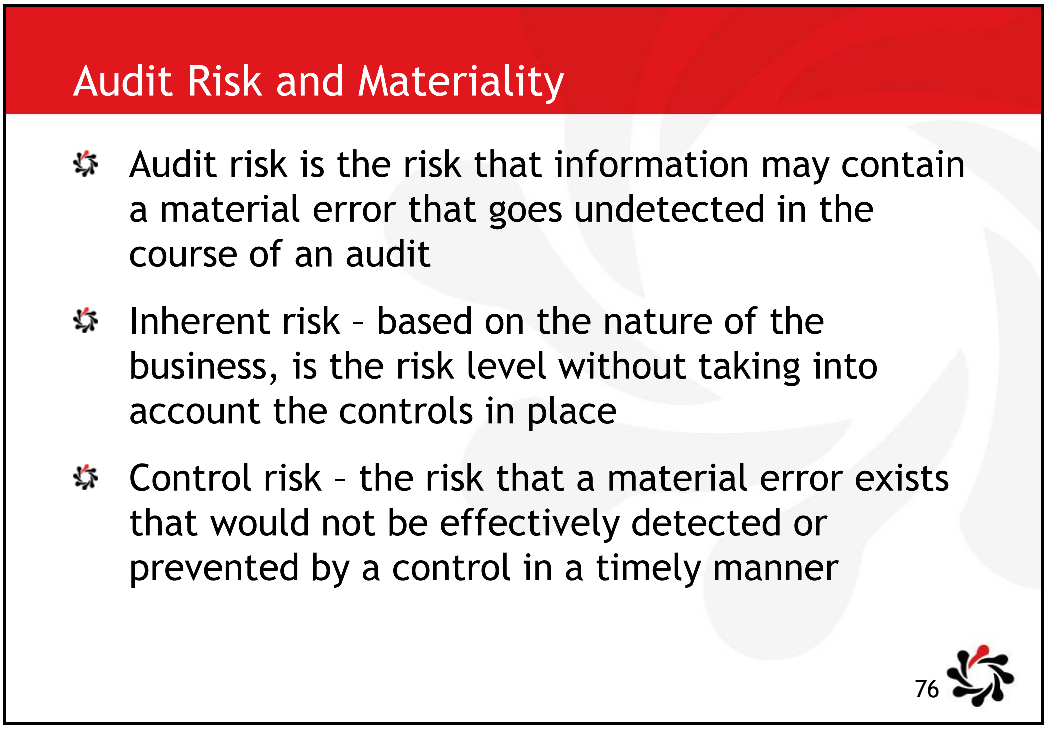
- All audit plans, programs, activities, tests, findings, and incidents should be properly documented in audit work papers
  - Maintain integrity of work papers and test results
  - Work papers support the facts contained in the final report



Risk-based Auditing

- Risk-based auditing is driven by:
  - Risk assessment that drives the audit schedule
  - Risk assessment that minimises audit risk
- Used to develop and improve the continuous audit process
  - Assists the auditor in determining the nature and extent of testing
    - Compliance or substantive testing

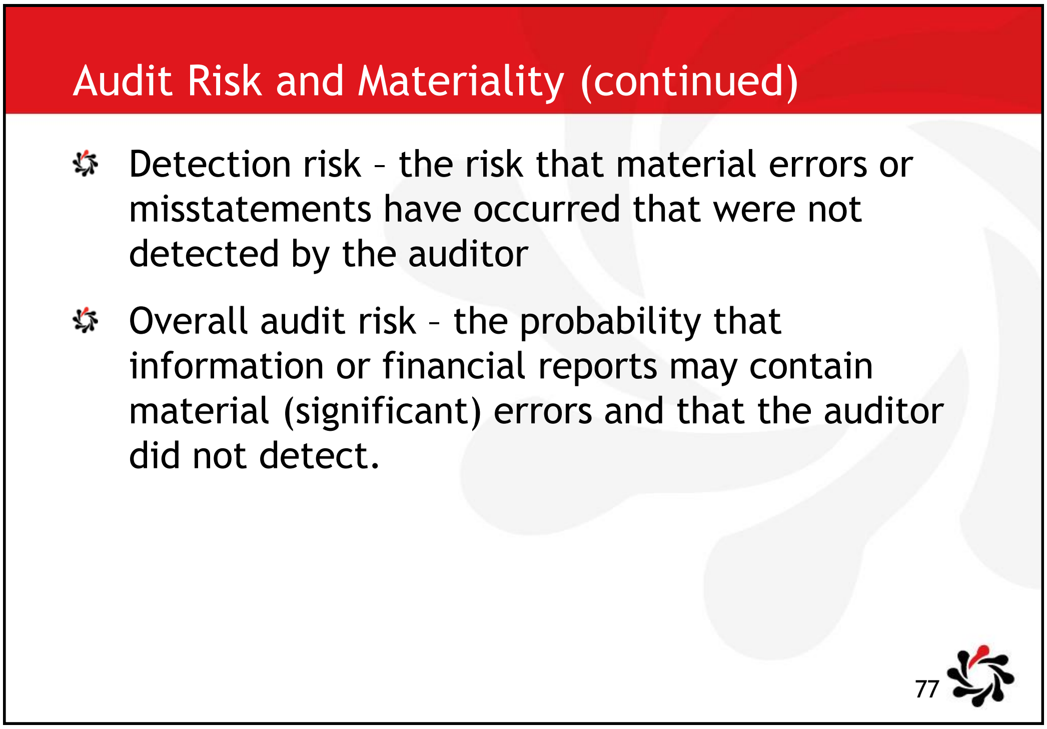
75



Audit Risk and Materiality

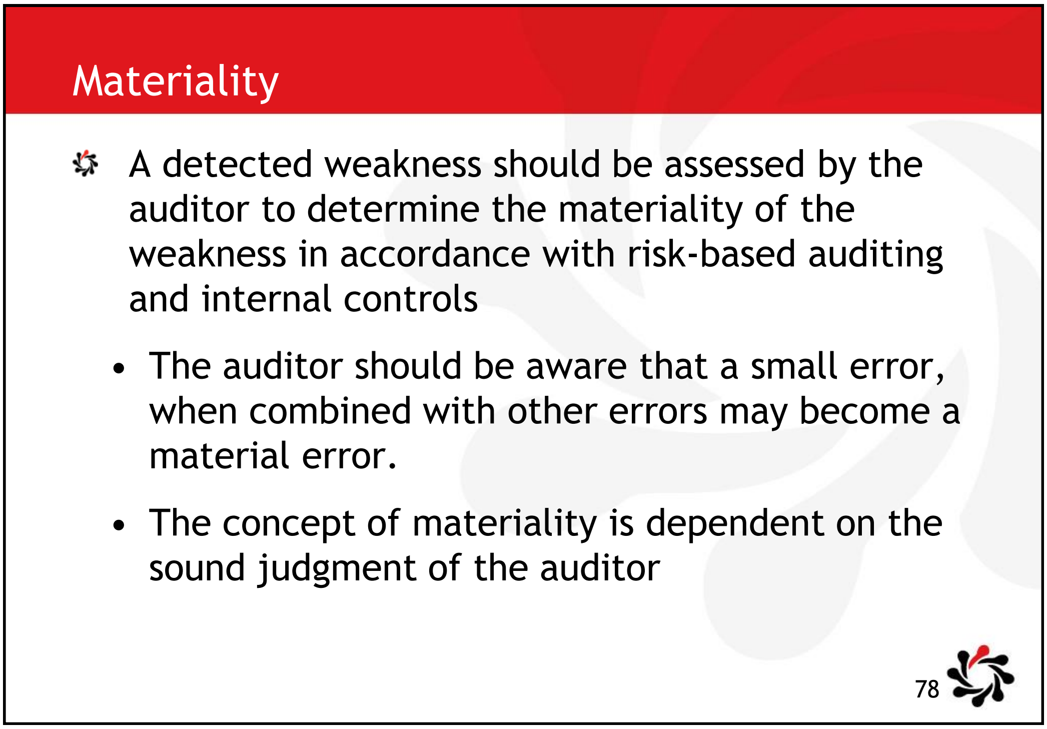
- Audit risk is the risk that information may contain a material error that goes undetected in the course of an audit
- Inherent risk – based on the nature of the business, is the risk level without taking into account the controls in place
- Control risk – the risk that a material error exists that would not be effectively detected or prevented by a control in a timely manner

76



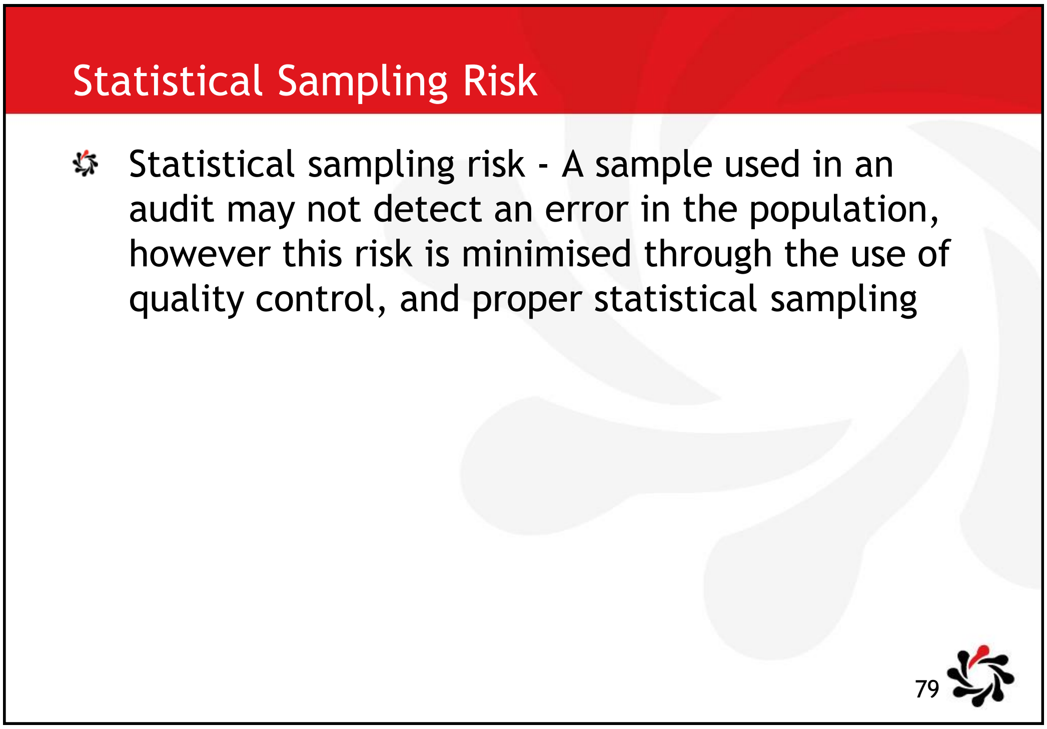
Audit Risk and Materiality (continued)

- Detection risk – the risk that material errors or misstatements have occurred that were not detected by the auditor
- Overall audit risk – the probability that information or financial reports may contain material (significant) errors and that the auditor did not detect.



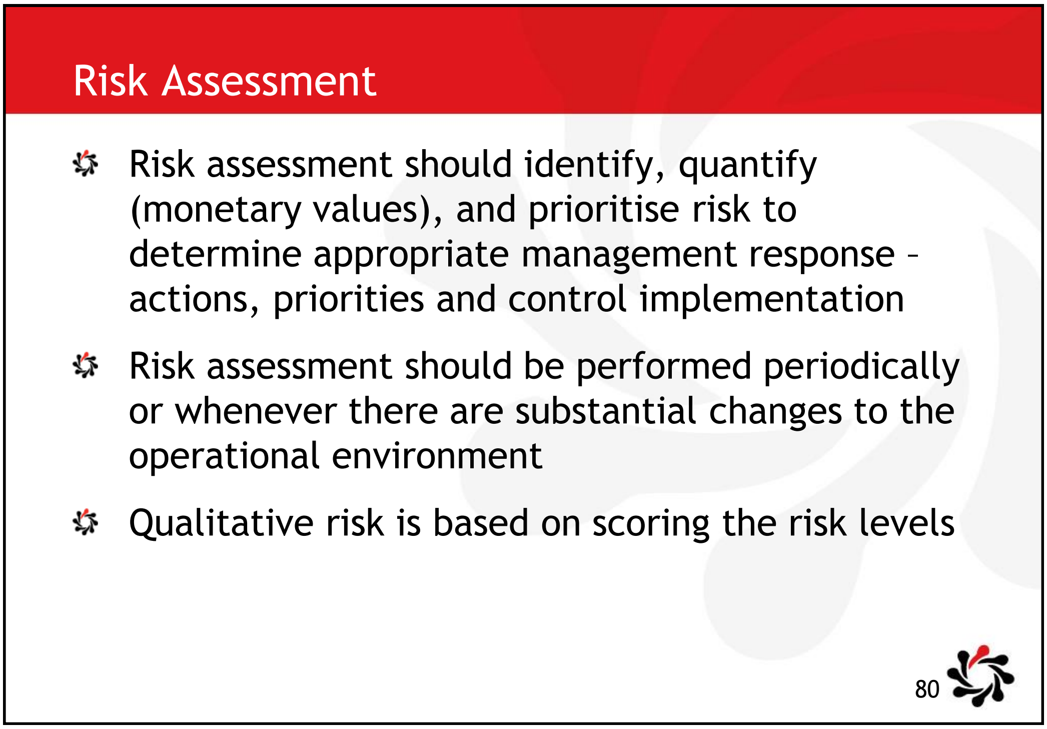
Materiality

- A detected weakness should be assessed by the auditor to determine the materiality of the weakness in accordance with risk-based auditing and internal controls
  - The auditor should be aware that a small error, when combined with other errors may become a material error.
  - The concept of materiality is dependent on the sound judgment of the auditor



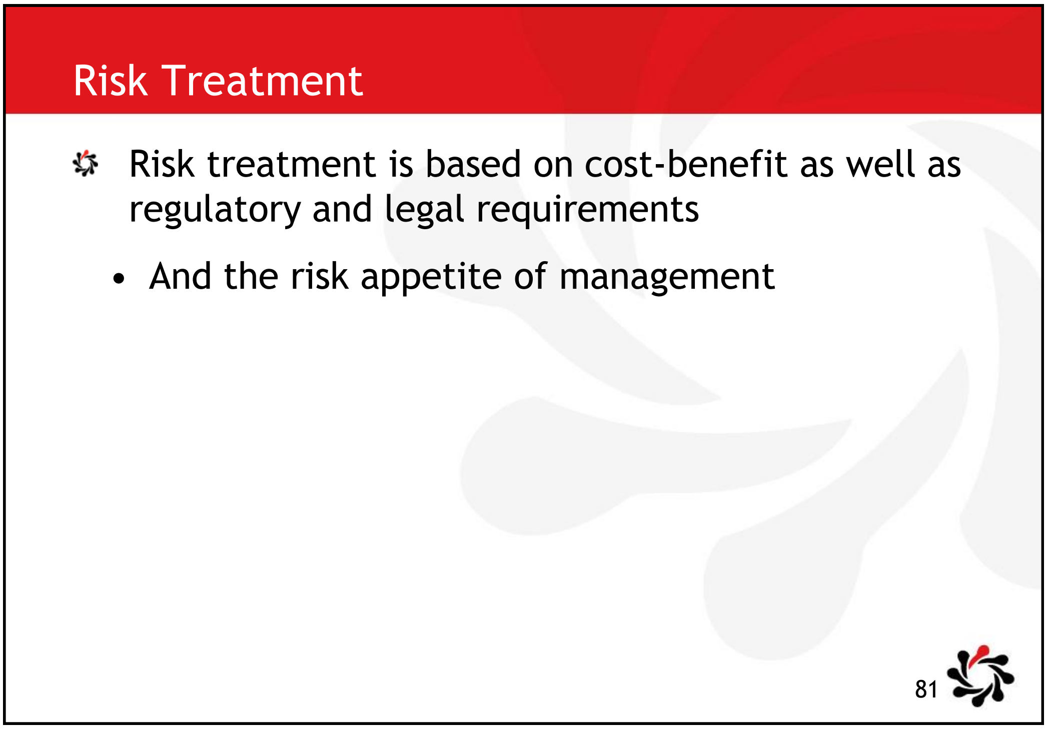
Statistical Sampling Risk

- Statistical sampling risk - A sample used in an audit may not detect an error in the population, however this risk is minimised through the use of quality control, and proper statistical sampling



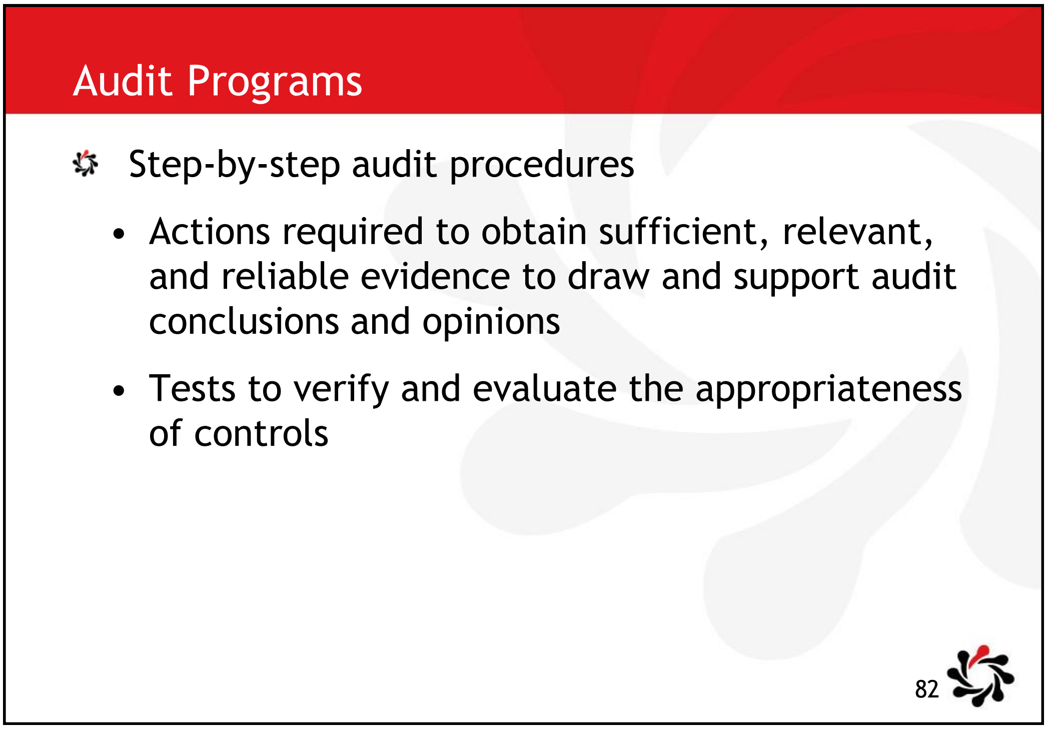
Risk Assessment

- Risk assessment should identify, quantify (monetary values), and prioritise risk to determine appropriate management response – actions, priorities and control implementation
- Risk assessment should be performed periodically or whenever there are substantial changes to the operational environment
- Qualitative risk is based on scoring the risk levels



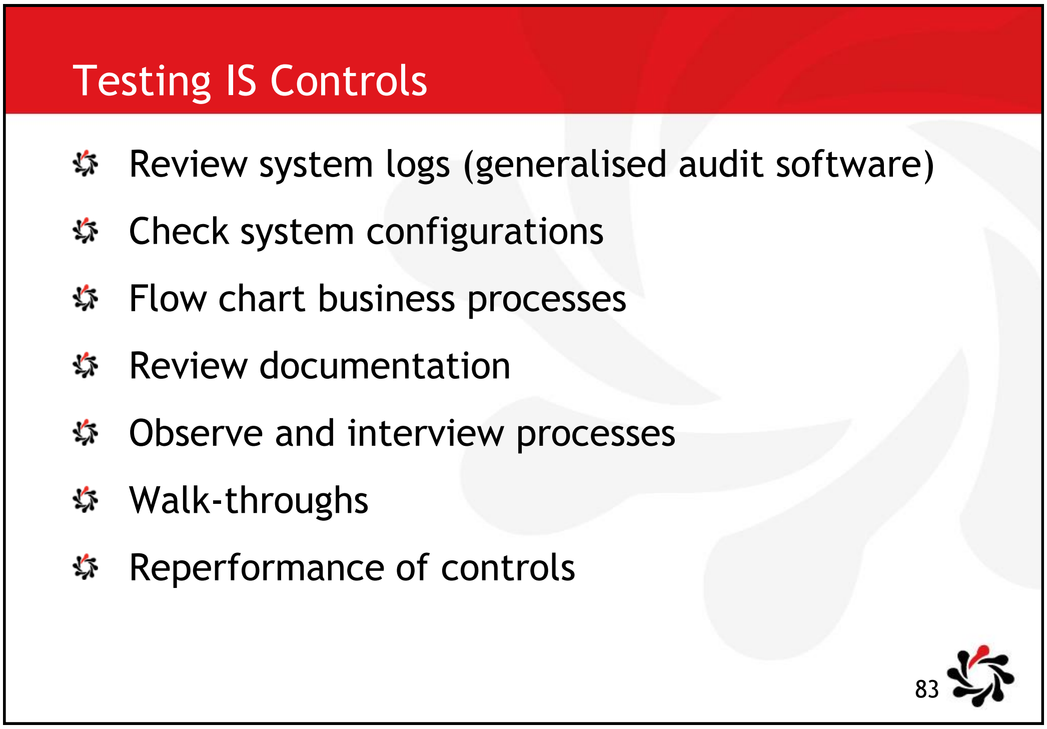
Risk Treatment

- Risk treatment is based on cost-benefit as well as regulatory and legal requirements
  - And the risk appetite of management



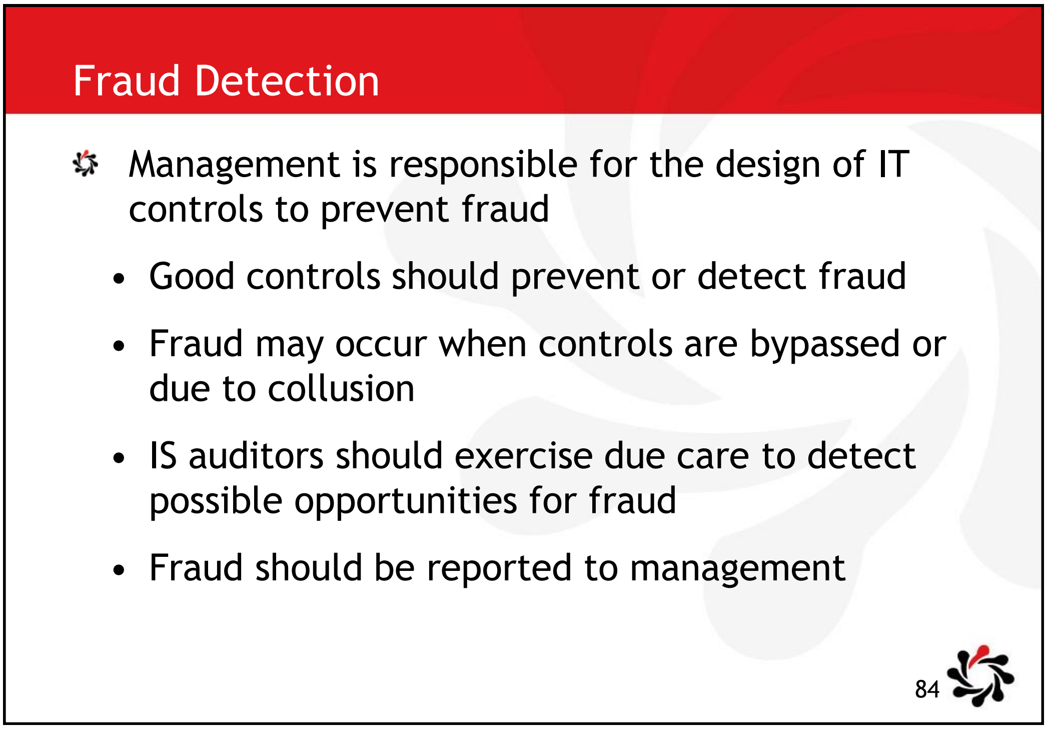
Audit Programs

- Step-by-step audit procedures
  - Actions required to obtain sufficient, relevant, and reliable evidence to draw and support audit conclusions and opinions
  - Tests to verify and evaluate the appropriateness of controls



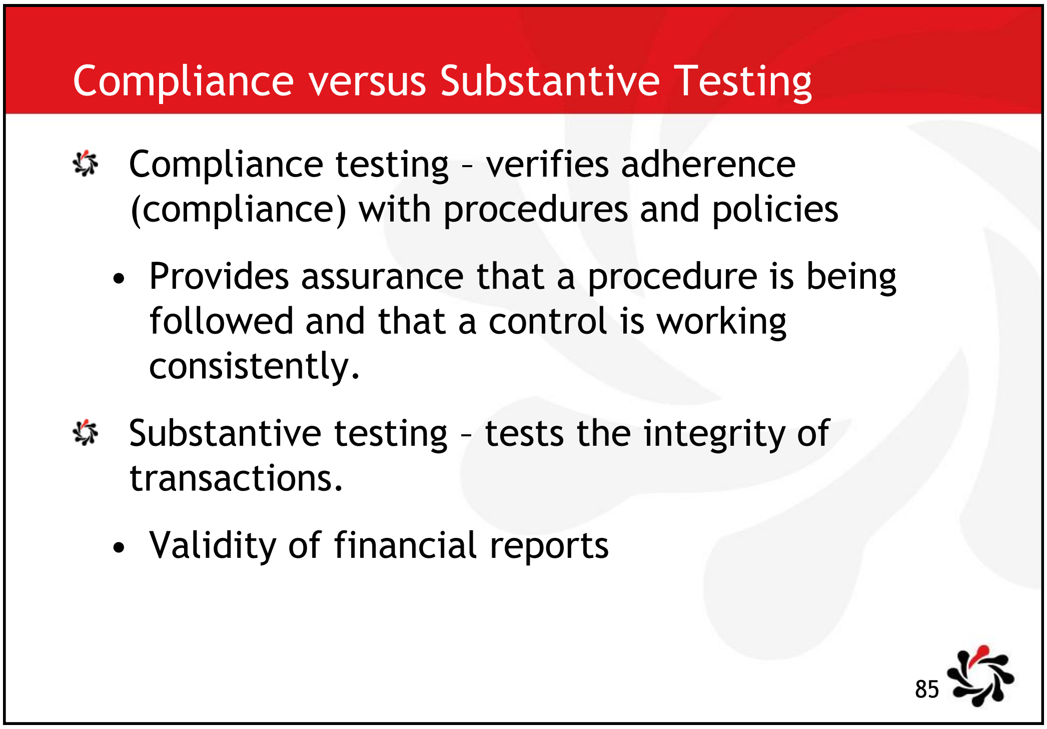
Testing IS Controls

- Review system logs (generalised audit software)
- Check system configurations
- Flow chart business processes
- Review documentation
- Observe and interview processes
- Walk-throughs
- Reperformance of controls



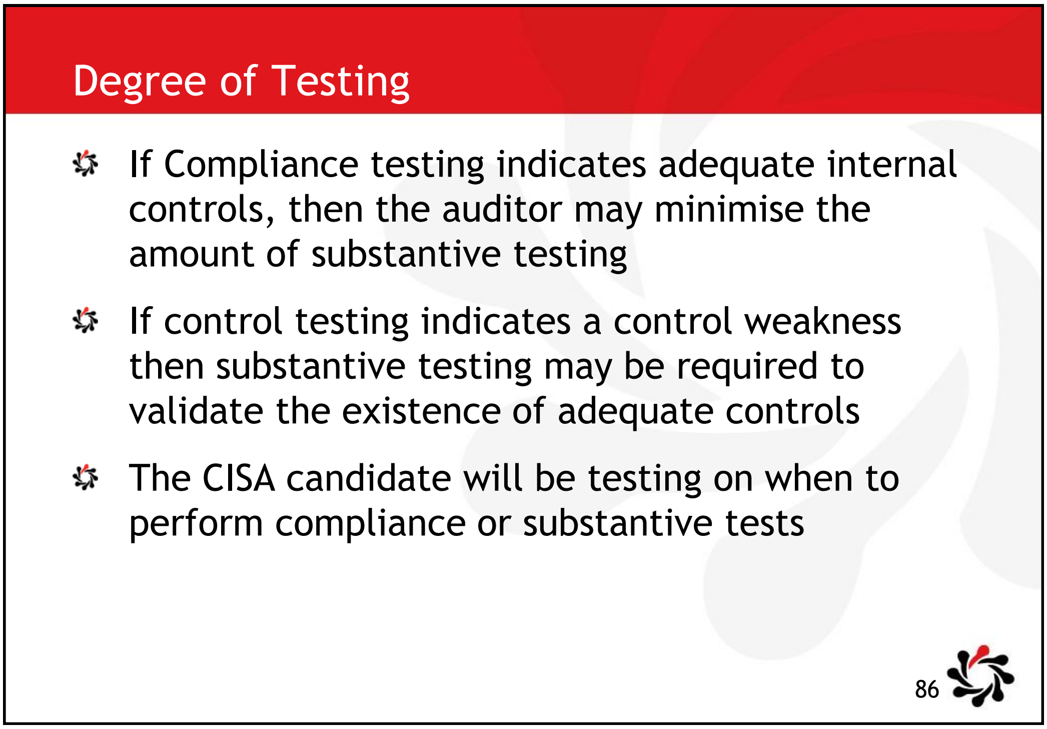
Fraud Detection

- Management is responsible for the design of IT controls to prevent fraud
  - Good controls should prevent or detect fraud
  - Fraud may occur when controls are bypassed or due to collusion
  - IS auditors should exercise due care to detect possible opportunities for fraud
  - Fraud should be reported to management



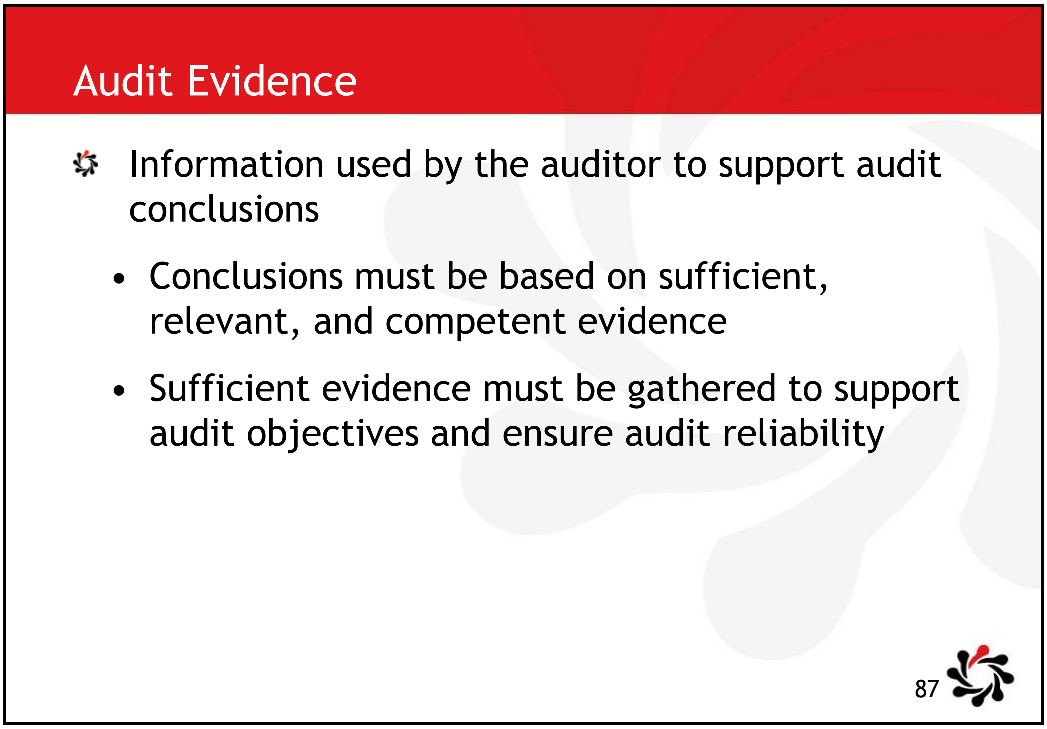
Compliance versus Substantive Testing

- Compliance testing – verifies adherence (compliance) with procedures and policies
  - Provides assurance that a procedure is being followed and that a control is working consistently.
- Substantive testing – tests the integrity of transactions.
  - Validity of financial reports



Degree of Testing

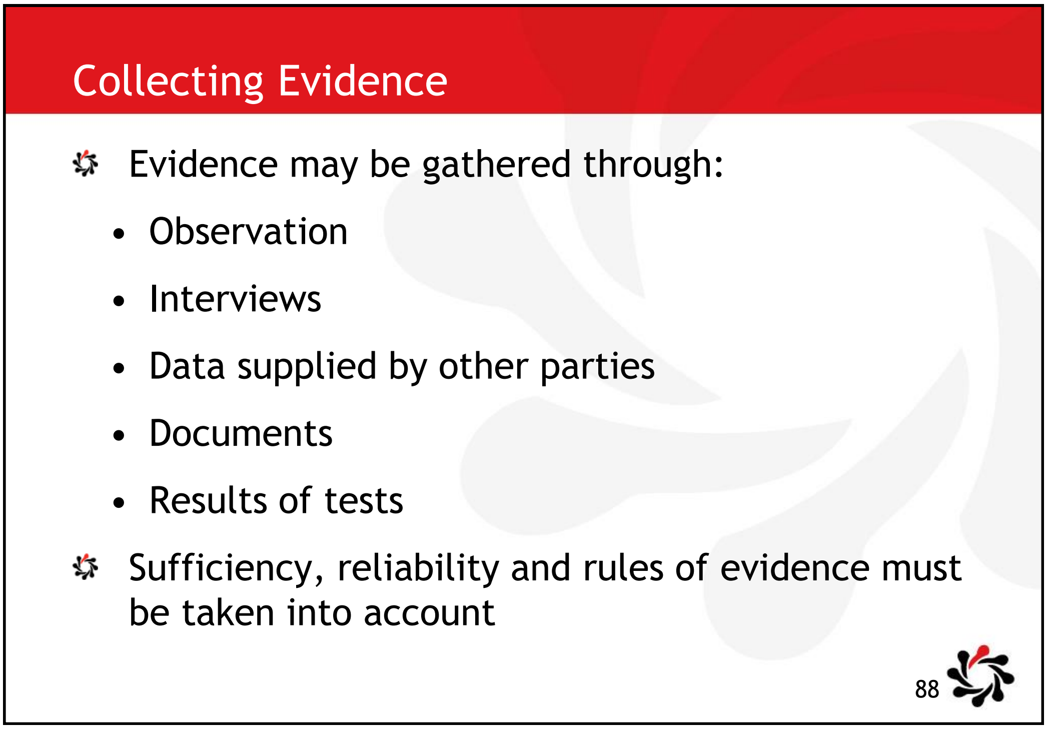
- If Compliance testing indicates adequate internal controls, then the auditor may minimise the amount of substantive testing
- If control testing indicates a control weakness then substantive testing may be required to validate the existence of adequate controls
- The CISA candidate will be testing on when to perform compliance or substantive tests



Audit Evidence

- Information used by the auditor to support audit conclusions
  - Conclusions must be based on sufficient, relevant, and competent evidence
  - Sufficient evidence must be gathered to support audit objectives and ensure audit reliability

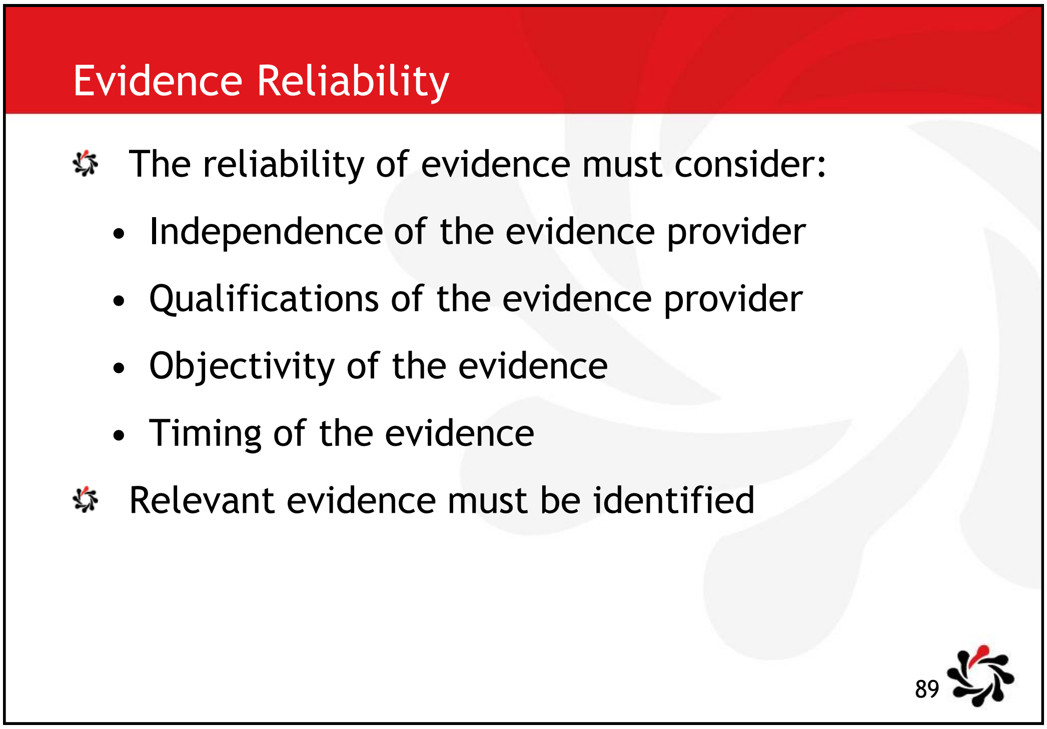
87



Collecting Evidence

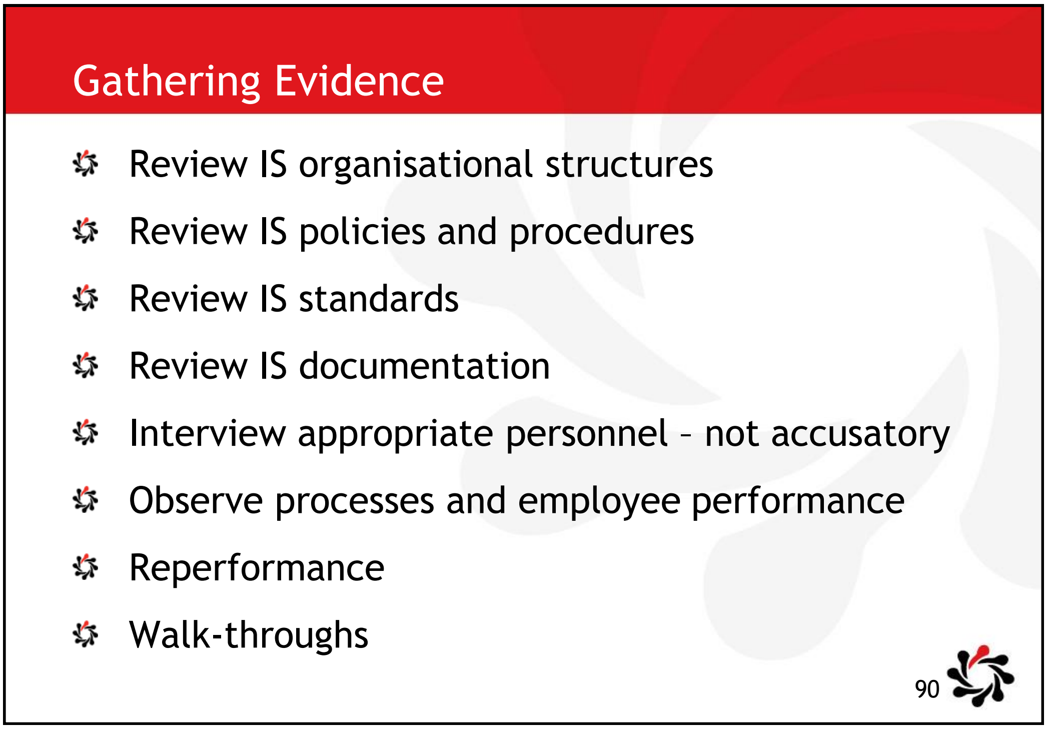
- Evidence may be gathered through:
  - Observation
  - Interviews
  - Data supplied by other parties
  - Documents
  - Results of tests
- Sufficiency, reliability and rules of evidence must be taken into account

88



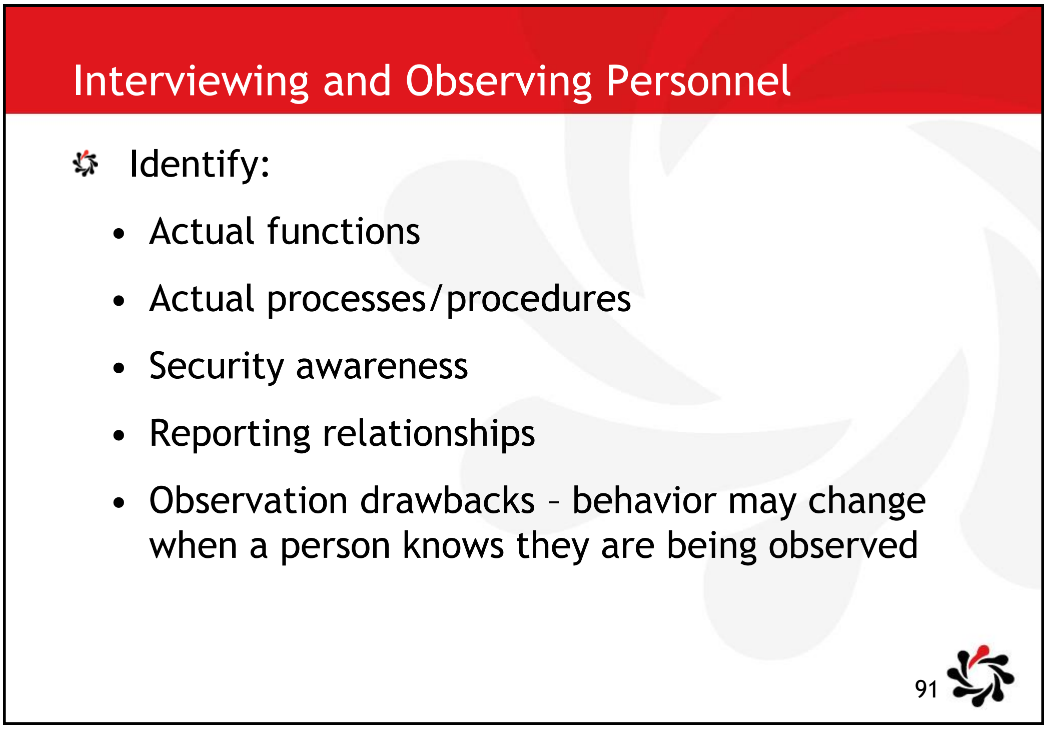
Evidence Reliability

- The reliability of evidence must consider:
  - Independence of the evidence provider
  - Qualifications of the evidence provider
  - Objectivity of the evidence
  - Timing of the evidence
- Relevant evidence must be identified



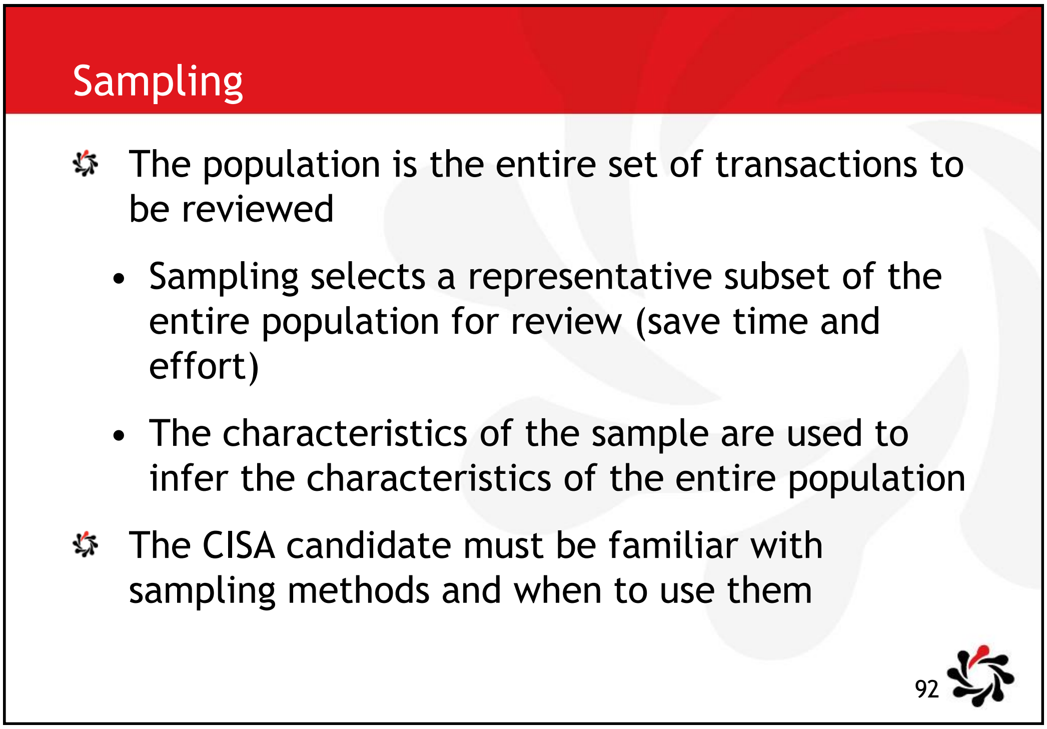
Gathering Evidence

- Review IS organisational structures
- Review IS policies and procedures
- Review IS standards
- Review IS documentation
- Interview appropriate personnel – not accusatory
- Observe processes and employee performance
- Reperformance
- Walk-throughs



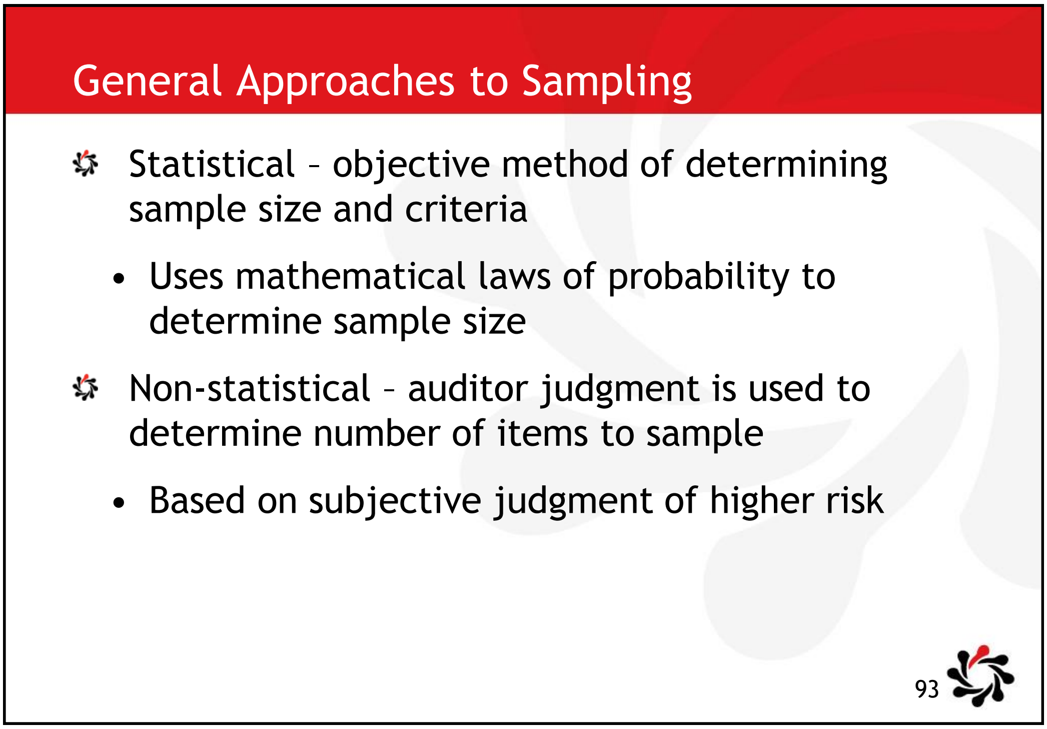
Interviewing and Observing Personnel

- Identify:
  - Actual functions
  - Actual processes/procedures
  - Security awareness
  - Reporting relationships
  - Observation drawbacks – behavior may change when a person knows they are being observed



Sampling

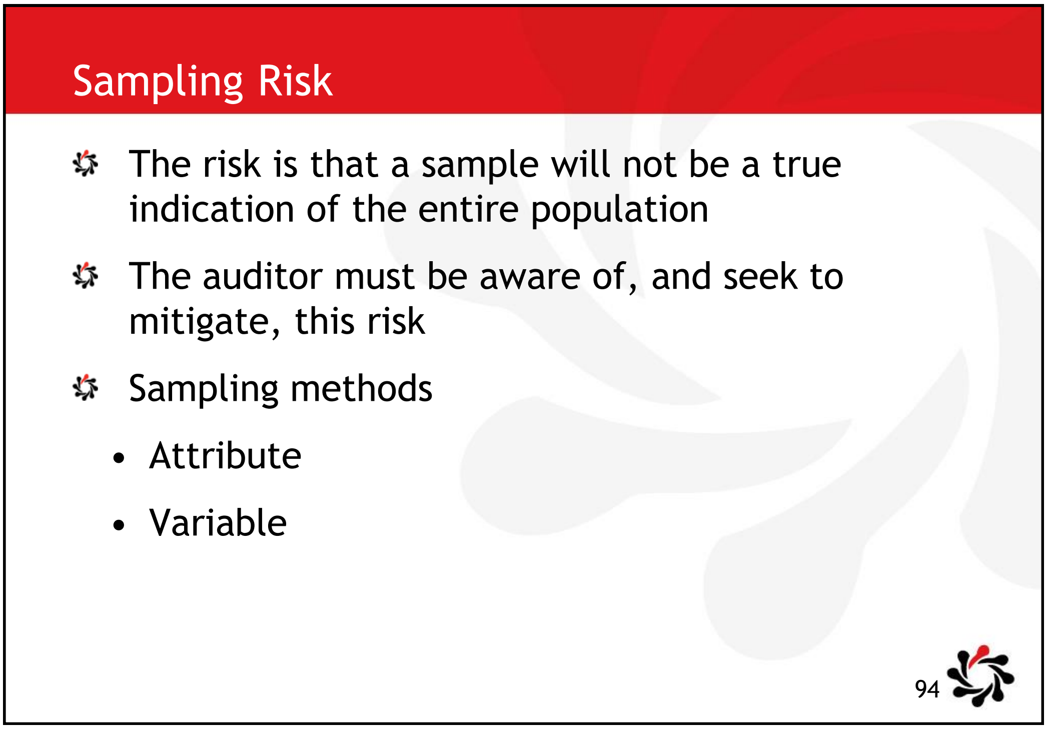
- The population is the entire set of transactions to be reviewed
  - Sampling selects a representative subset of the entire population for review (save time and effort)
  - The characteristics of the sample are used to infer the characteristics of the entire population
- The CISA candidate must be familiar with sampling methods and when to use them



General Approaches to Sampling

- Statistical – objective method of determining sample size and criteria
  - Uses mathematical laws of probability to determine sample size
- Non-statistical – auditor judgment is used to determine number of items to sample
  - Based on subjective judgment of higher risk

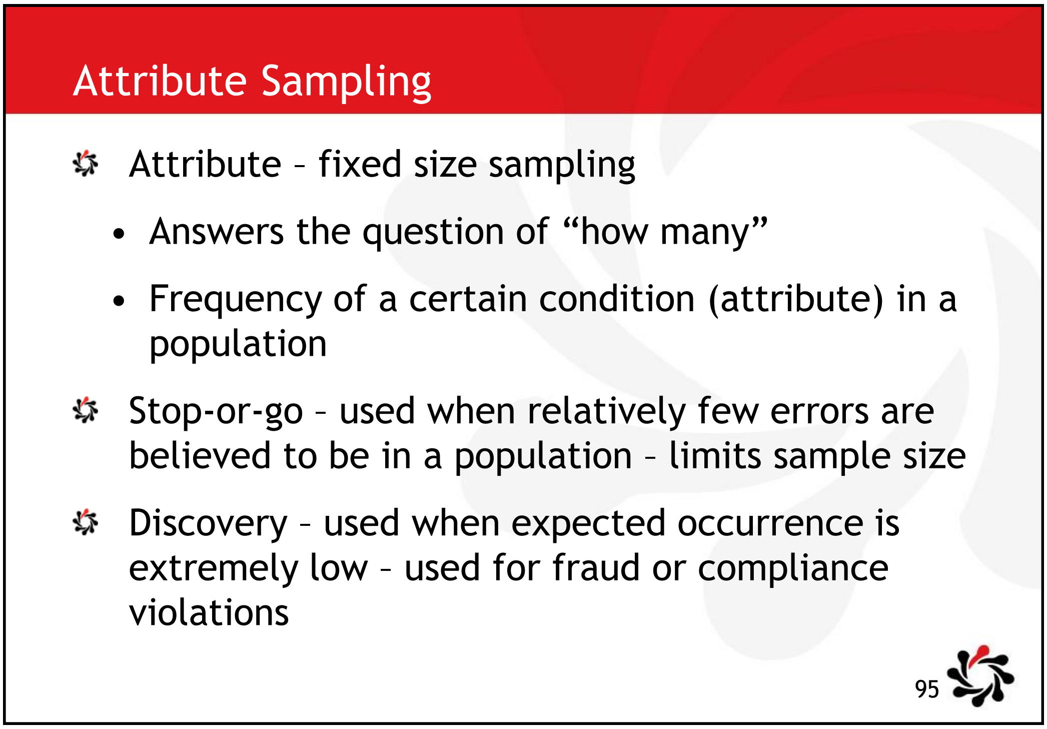
93



Sampling Risk

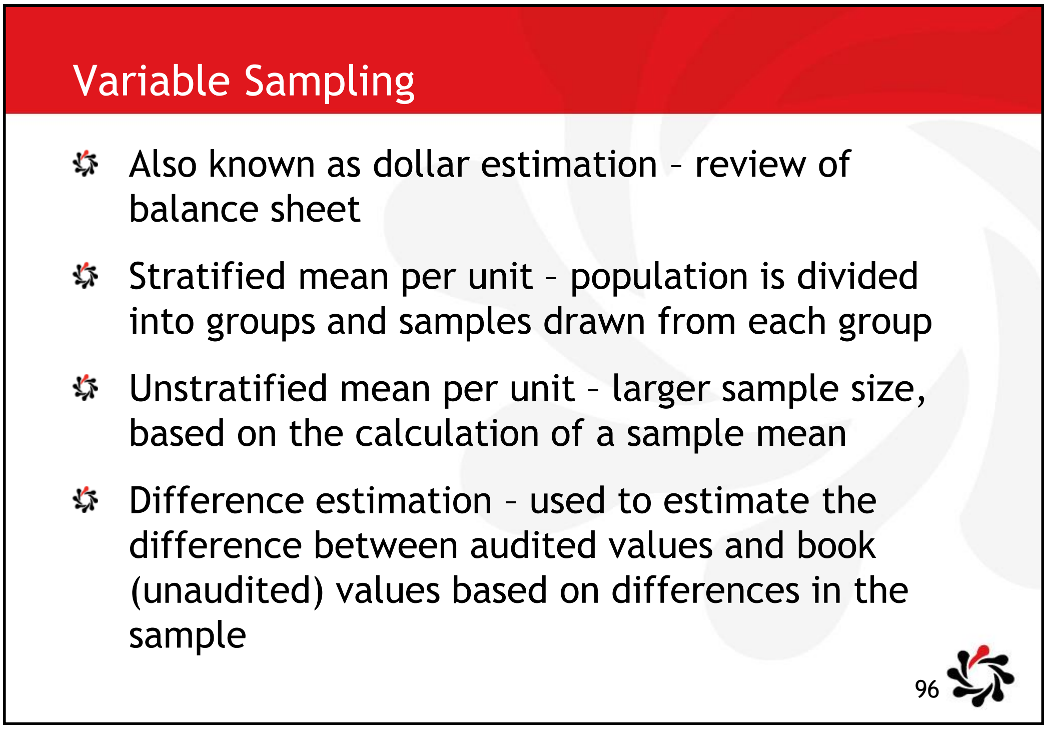
- The risk is that a sample will not be a true indication of the entire population
- The auditor must be aware of, and seek to mitigate, this risk
- Sampling methods
  - Attribute
  - Variable

94



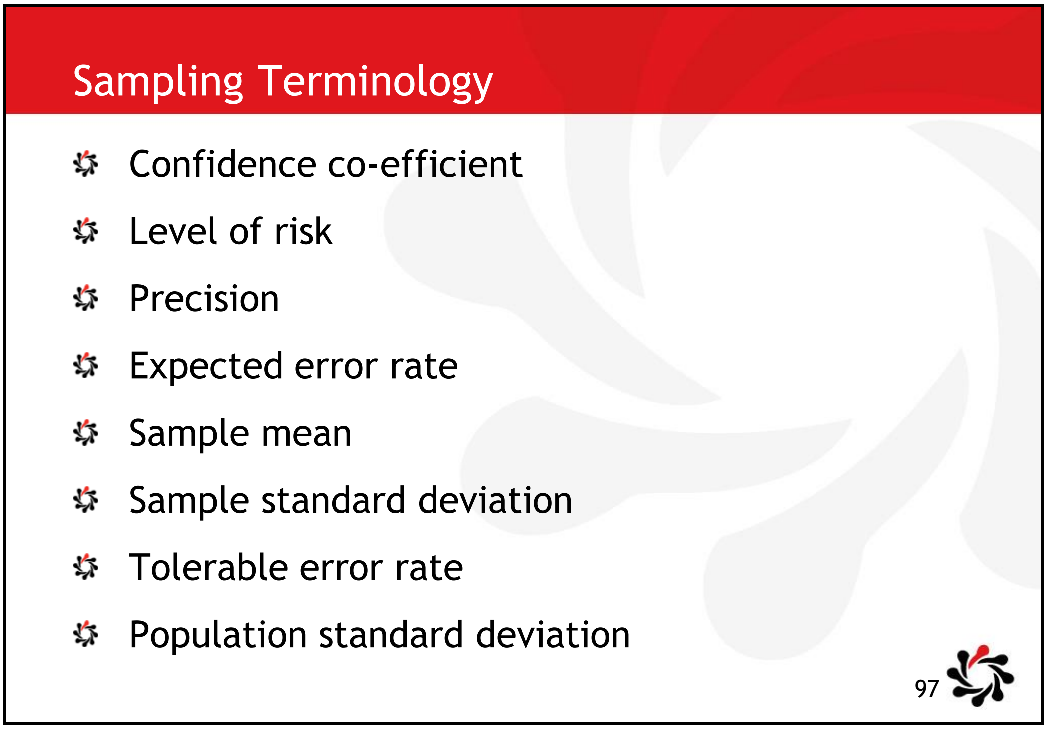
Attribute Sampling

- Attribute – fixed size sampling
  - Answers the question of “how many”
  - Frequency of a certain condition (attribute) in a population
- Stop-or-go – used when relatively few errors are believed to be in a population – limits sample size
- Discovery – used when expected occurrence is extremely low – used for fraud or compliance violations



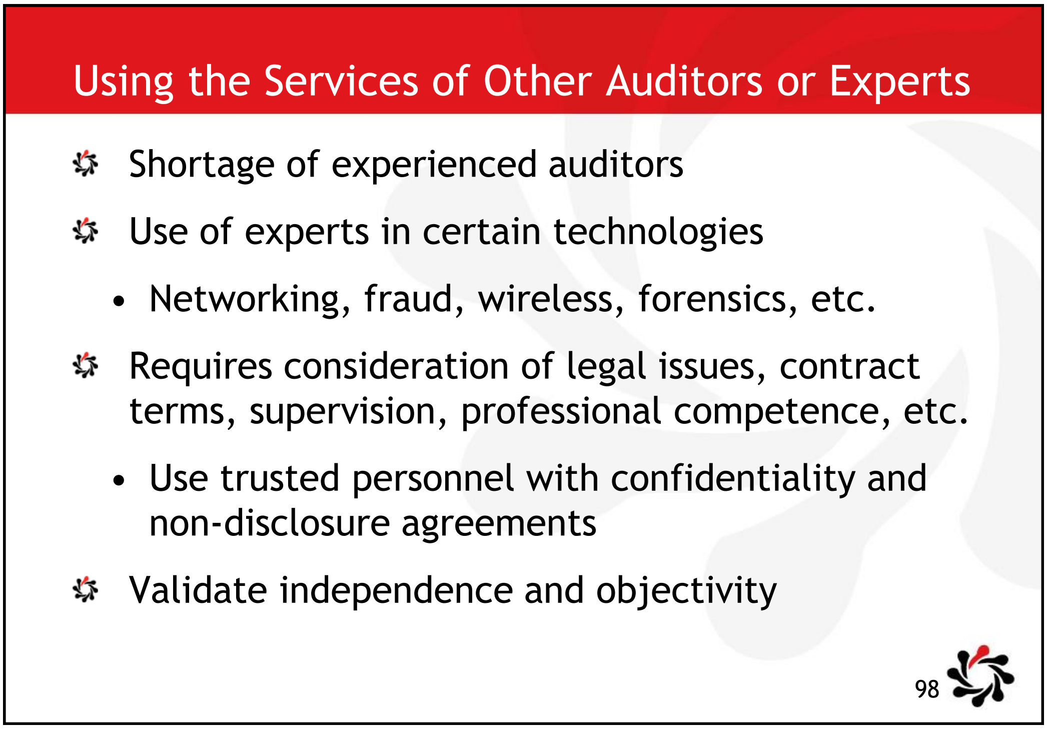
Variable Sampling

- Also known as dollar estimation – review of balance sheet
- Stratified mean per unit – population is divided into groups and samples drawn from each group
- Unstratified mean per unit – larger sample size, based on the calculation of a sample mean
- Difference estimation – used to estimate the difference between audited values and book (unaudited) values based on differences in the sample



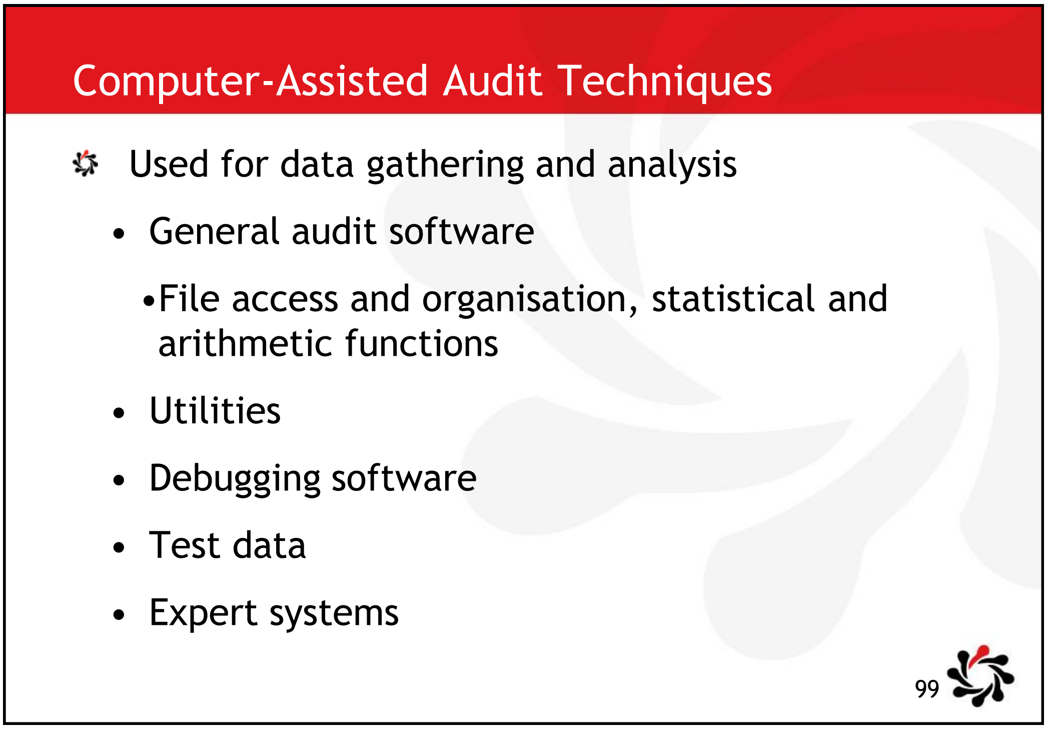
Sampling Terminology

- Confidence co-efficient
- Level of risk
- Precision
- Expected error rate
- Sample mean
- Sample standard deviation
- Tolerable error rate
- Population standard deviation



Using the Services of Other Auditors or Experts

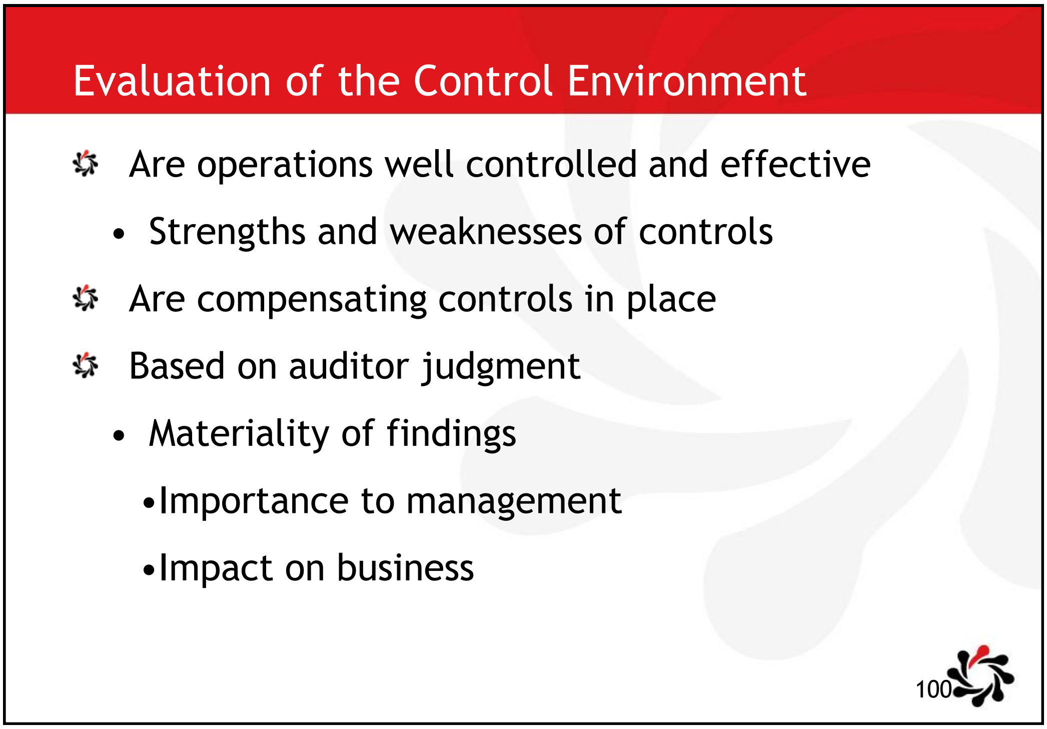
- Shortage of experienced auditors
- Use of experts in certain technologies
  - Networking, fraud, wireless, forensics, etc.
- Requires consideration of legal issues, contract terms, supervision, professional competence, etc.
  - Use trusted personnel with confidentiality and non-disclosure agreements
- Validate independence and objectivity



Computer-Assisted Audit Techniques

- Used for data gathering and analysis
  - General audit software
    - File access and organisation, statistical and arithmetic functions
  - Utilities
  - Debugging software
  - Test data
  - Expert systems

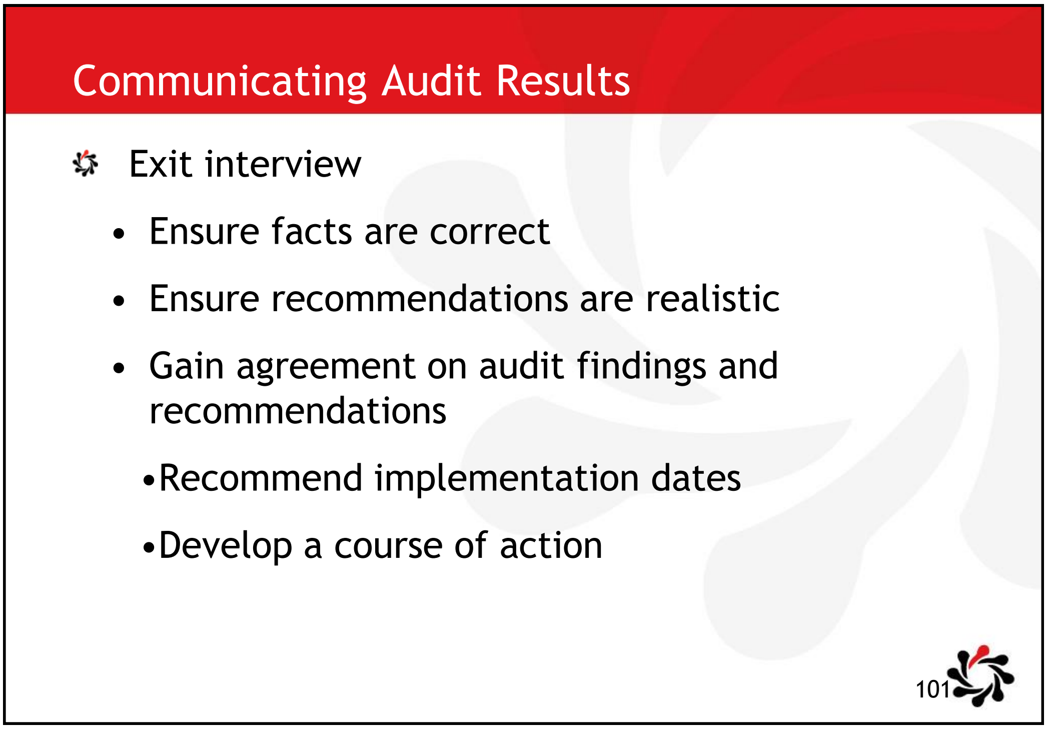
99



Evaluation of the Control Environment

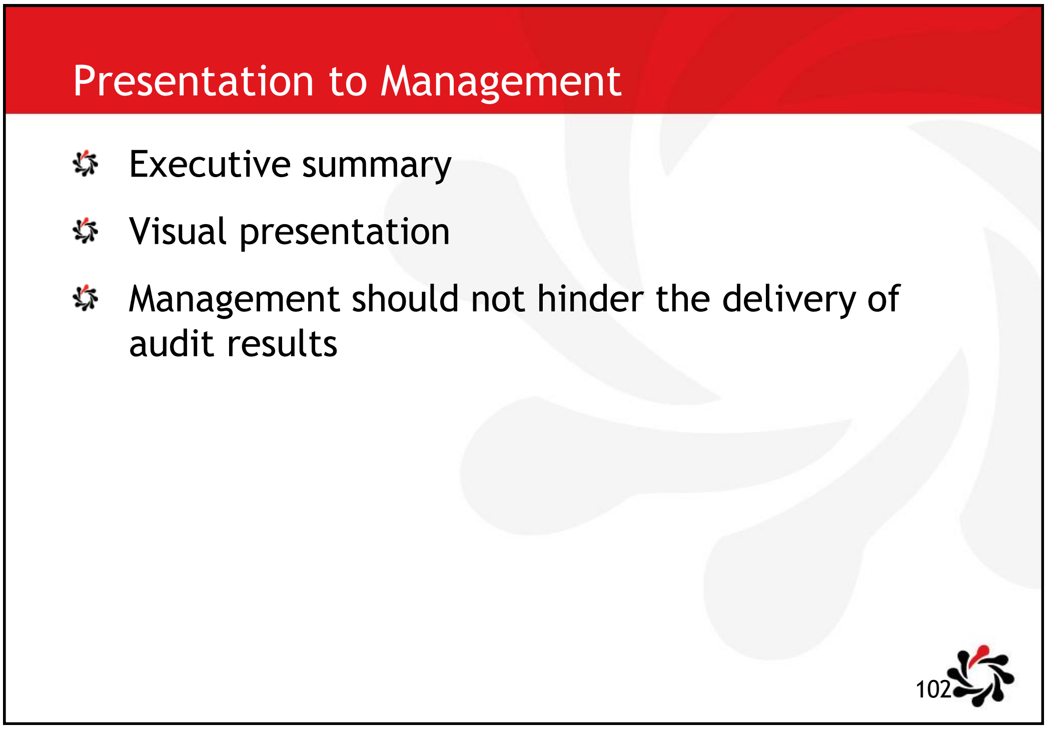
- Are operations well controlled and effective
  - Strengths and weaknesses of controls
- Are compensating controls in place
- Based on auditor judgment
  - Materiality of findings
    - Importance to management
    - Impact on business

100



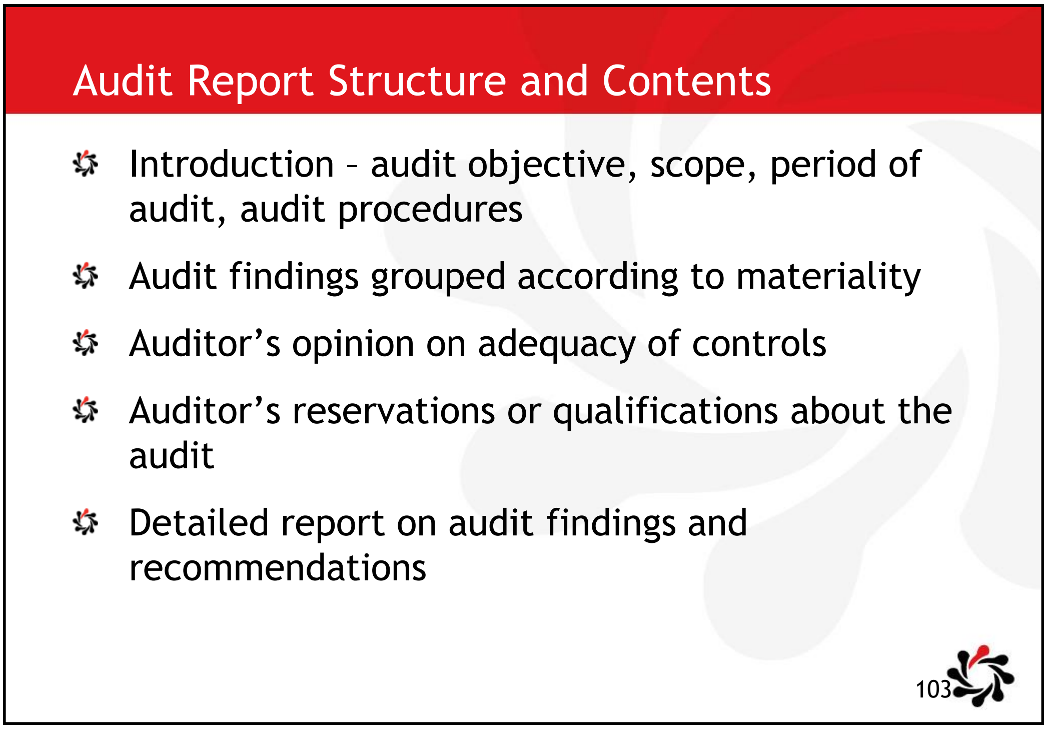
Communicating Audit Results

- Exit interview
  - Ensure facts are correct
  - Ensure recommendations are realistic
  - Gain agreement on audit findings and recommendations
    - Recommend implementation dates
    - Develop a course of action



Presentation to Management

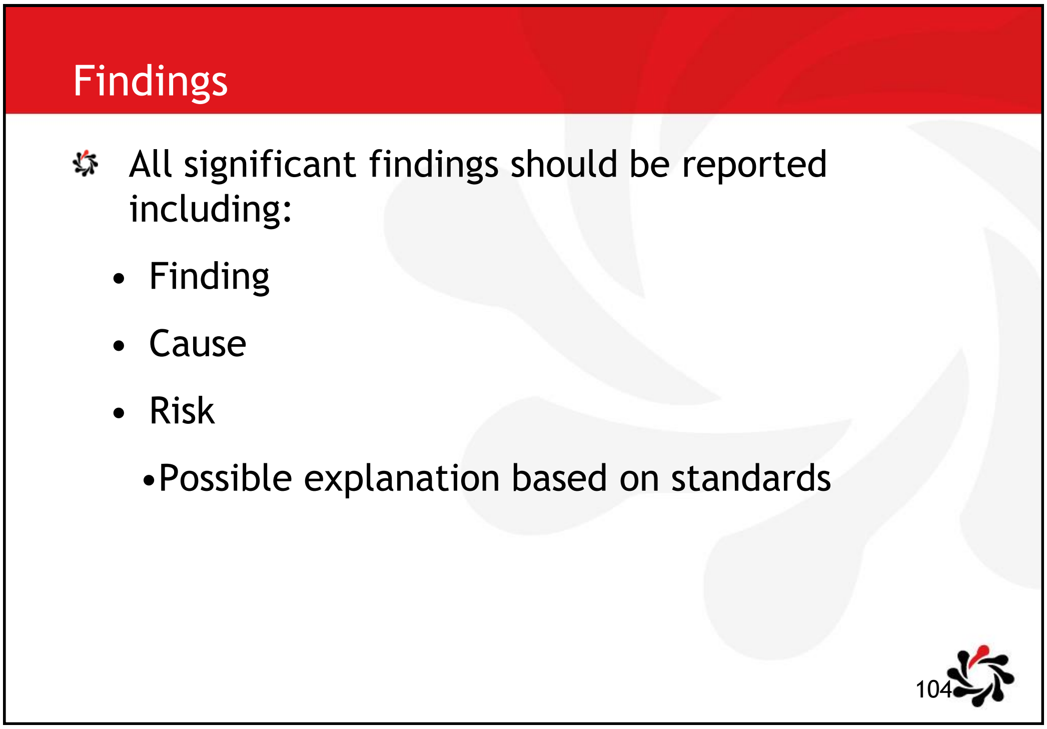
- Executive summary
- Visual presentation
- Management should not hinder the delivery of audit results



Audit Report Structure and Contents

- Introduction – audit objective, scope, period of audit, audit procedures
- Audit findings grouped according to materiality
- Auditor’s opinion on adequacy of controls
- Auditor’s reservations or qualifications about the audit
- Detailed report on audit findings and recommendations

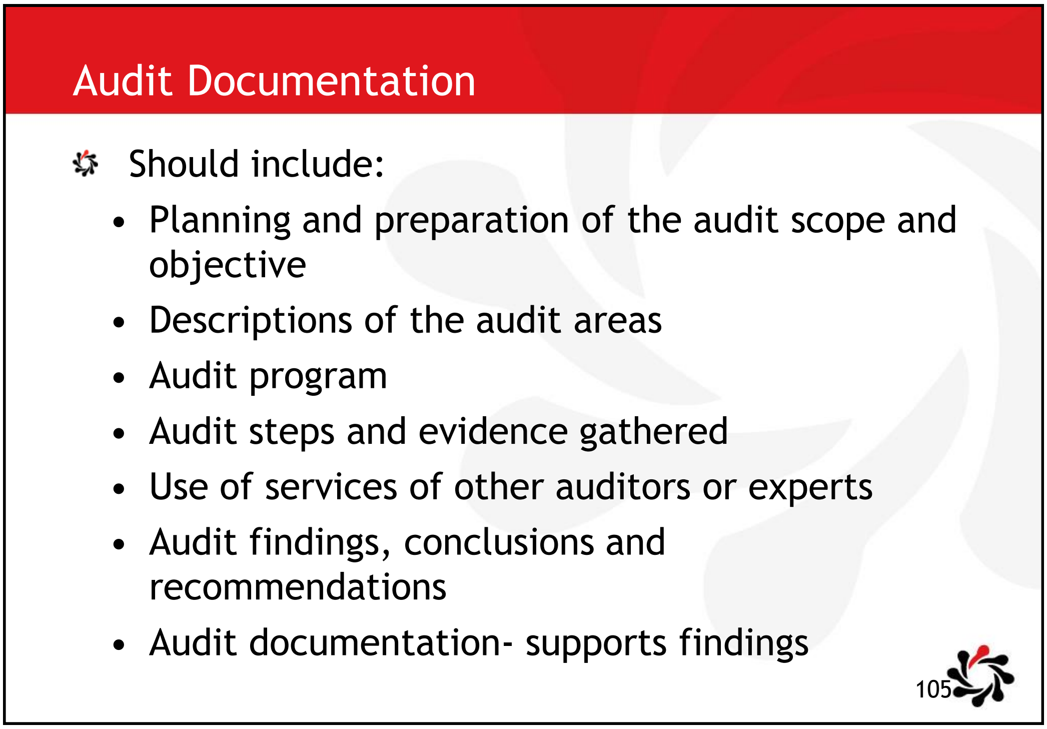
103



Findings

- All significant findings should be reported including:
  - Finding
  - Cause
  - Risk
    - Possible explanation based on standards

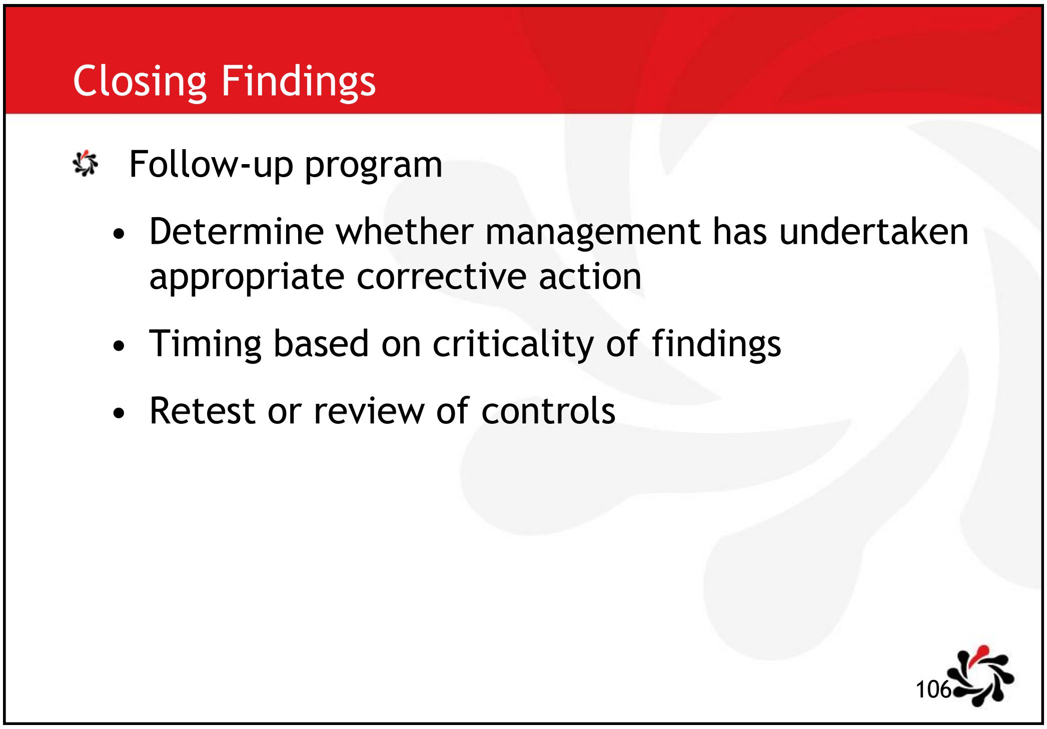
104



Audit Documentation

- Should include:
  - Planning and preparation of the audit scope and objective
  - Descriptions of the audit areas
  - Audit program
  - Audit steps and evidence gathered
  - Use of services of other auditors or experts
  - Audit findings, conclusions and recommendations
  - Audit documentation- supports findings

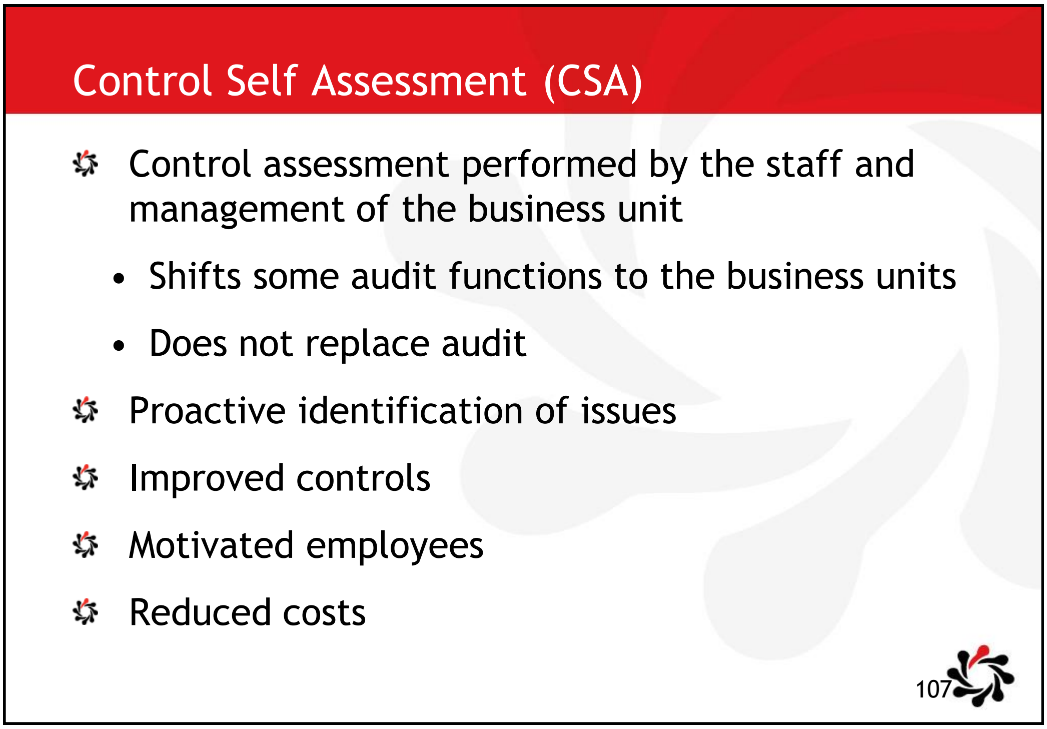
105



Closing Findings

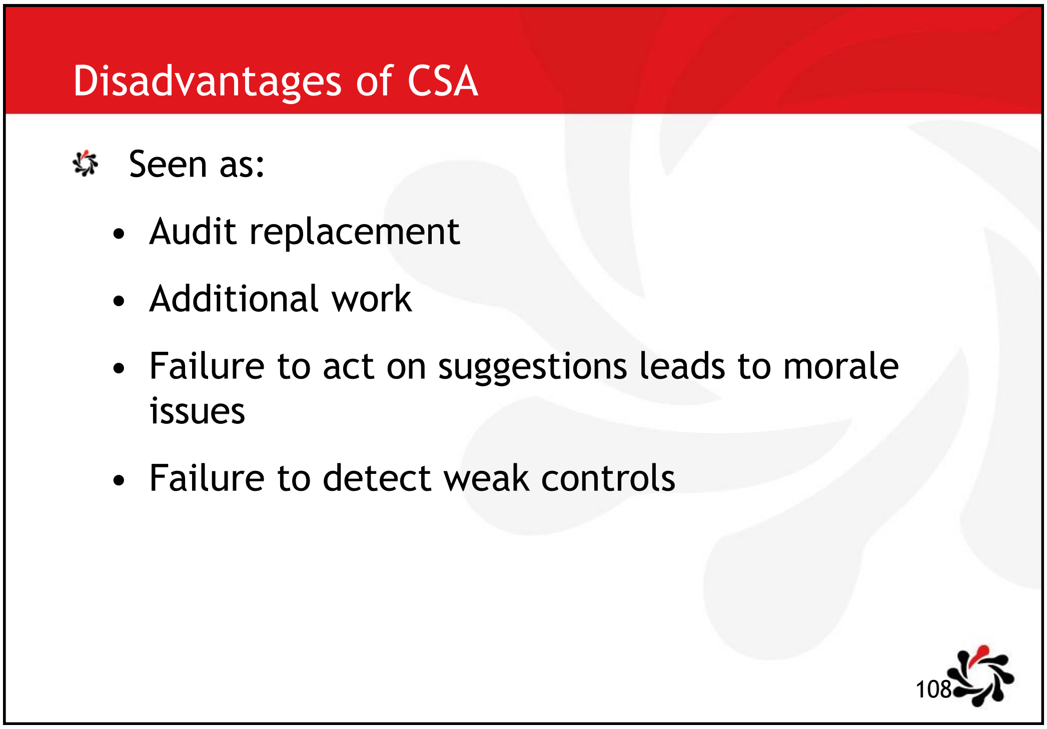
- Follow-up program
  - Determine whether management has undertaken appropriate corrective action
  - Timing based on criticality of findings
  - Retest or review of controls

106



Control Self Assessment (CSA)

- Control assessment performed by the staff and management of the business unit
  - Shifts some audit functions to the business units
  - Does not replace audit
- Proactive identification of issues
- Improved controls
- Motivated employees
- Reduced costs



Disadvantages of CSA

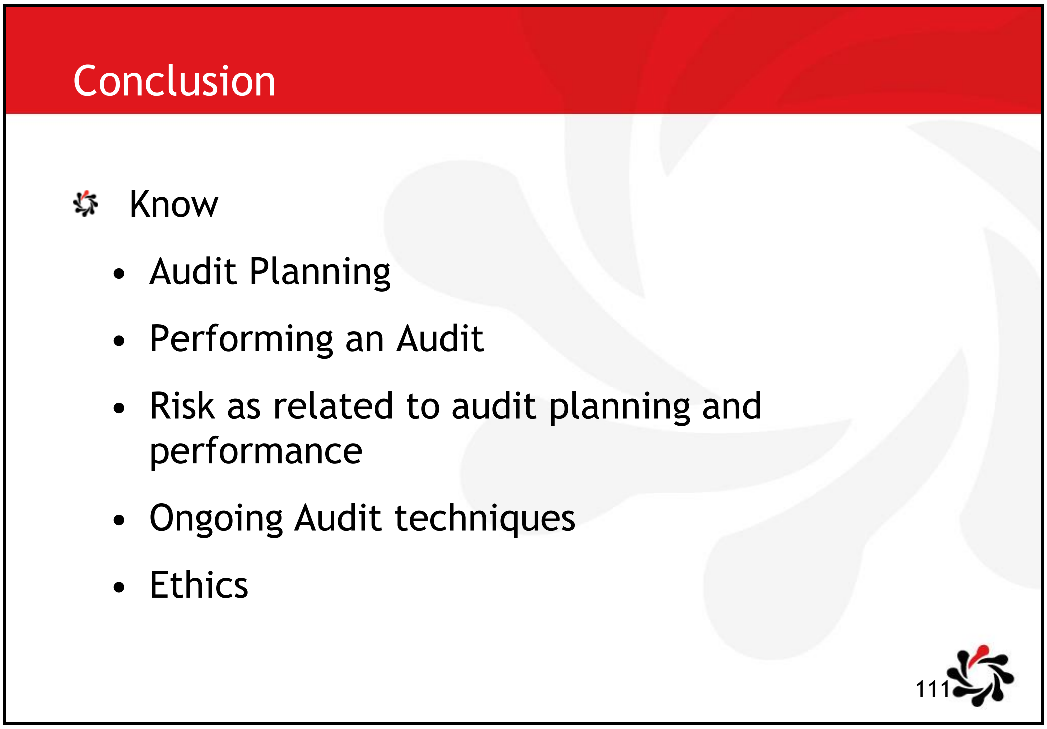
- Seen as:
  - Audit replacement
  - Additional work
  - Failure to act on suggestions leads to morale issues
  - Failure to detect weak controls

Auditor Role in CSA

- Facilitator
- Guide
- Consult management
- Risk analysis

Continuous Monitoring and Auditing

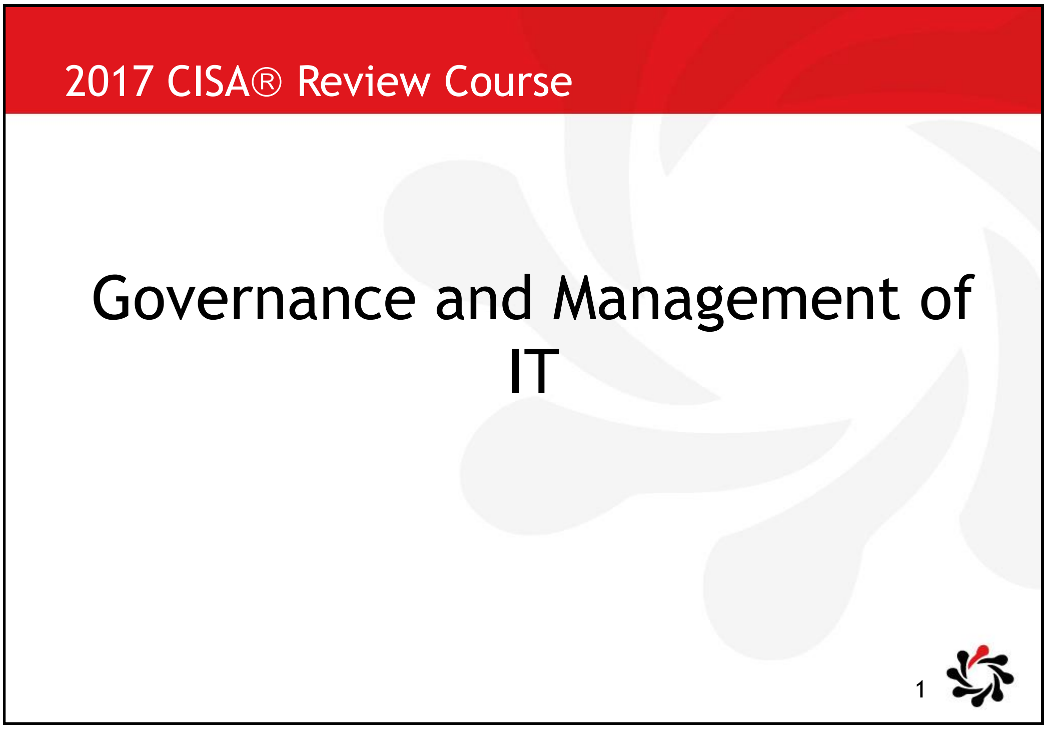
- Continuous Monitoring – provided by IS management tools based on automated procedures i.e., anti-virus
- Continuous Auditing – perform control and risk assessment on a more frequent basis. Uses tools to monitor all transactions.
- Together they provide continuous assurance
  - More secure
  - Less audit work



Conclusion

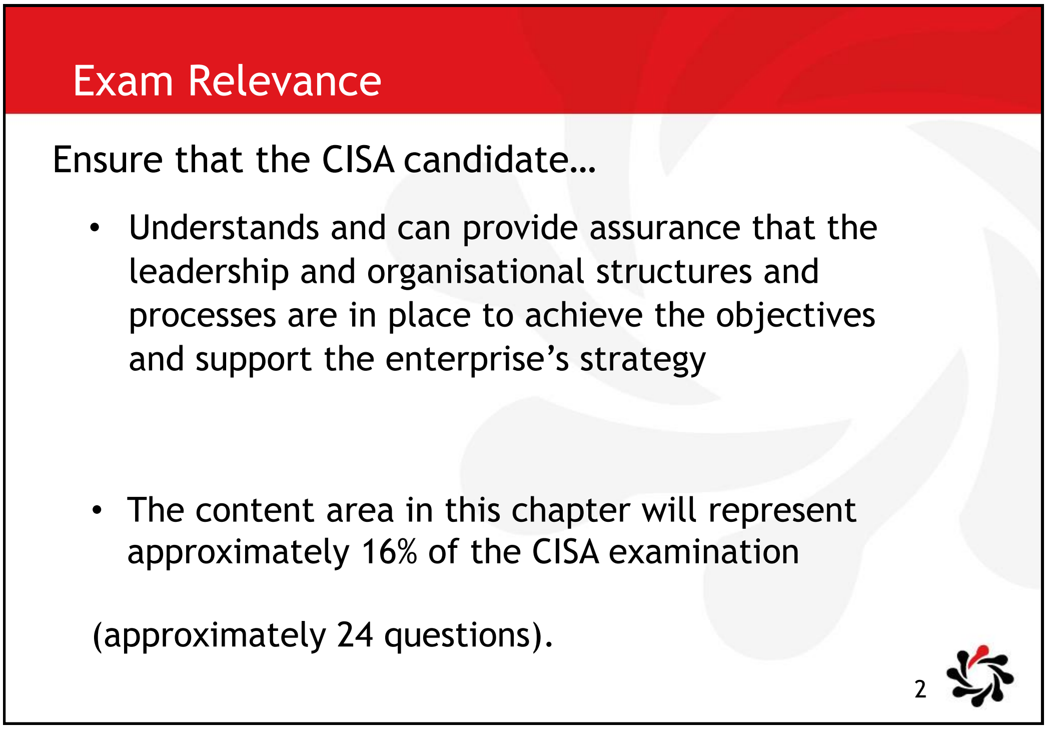
- Know
  - Audit Planning
  - Performing an Audit
  - Risk as related to audit planning and performance
  - Ongoing Audit techniques
  - Ethics

111



2017 CISA® Review Course

Governance and Management of IT



Exam Relevance

Ensure that the CISA candidate…

- Understands and can provide assurance that the leadership and organisational structures and processes are in place to achieve the objectives and support the enterprise's strategy

- The content area in this chapter will represent approximately 16% of the CISA examination

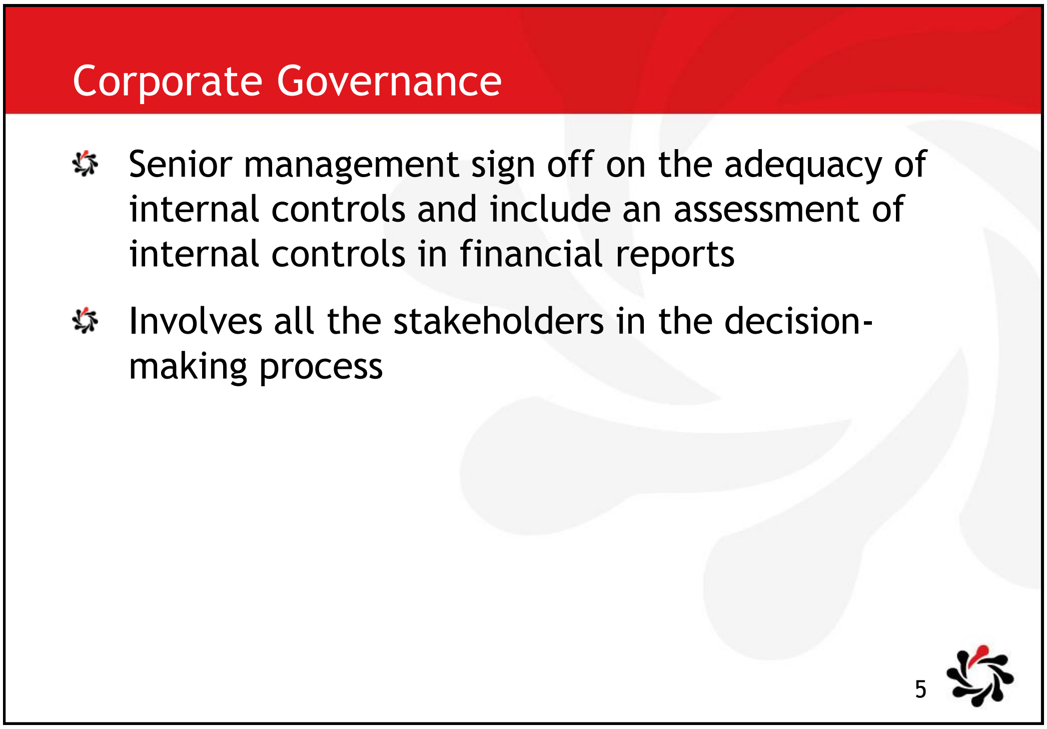
(approximately 24 questions).

Task Statements

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

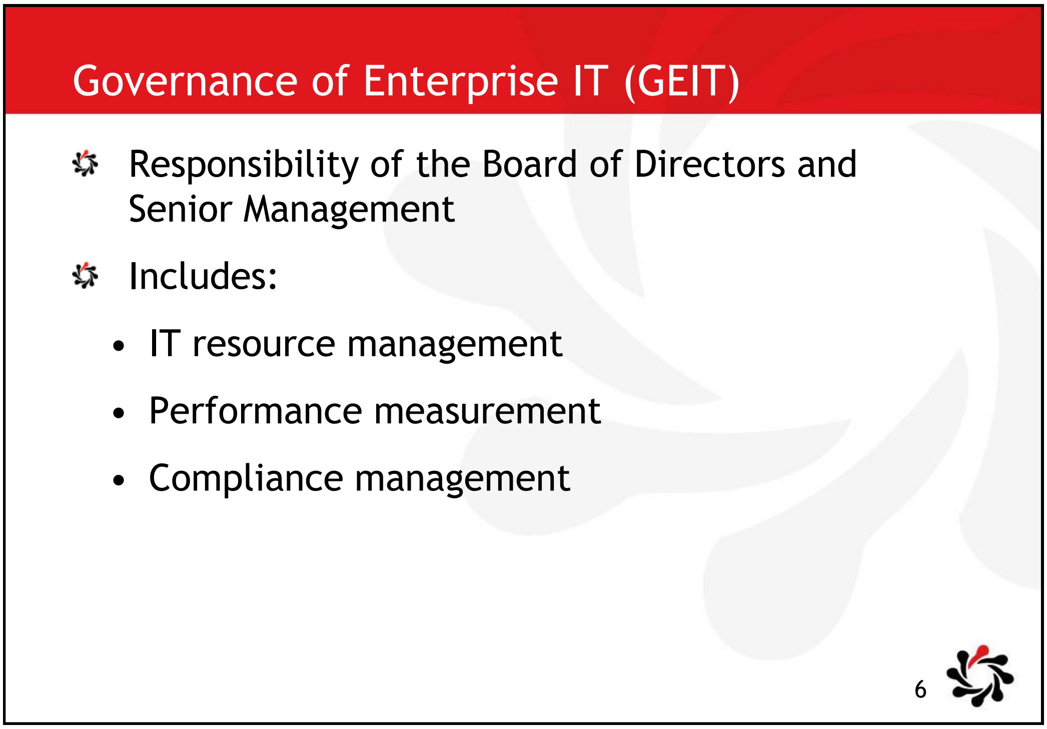
Corporate Governance Defined

- “System by which business corporations are directed and controlled”
- Set of responsibilities and practices used by an organisation’s management to provide strategic direction, thereby ensuring that goals are achievable, risk is properly addressed and organisational resources are properly utilised
  - Structure
  - Reporting relationships



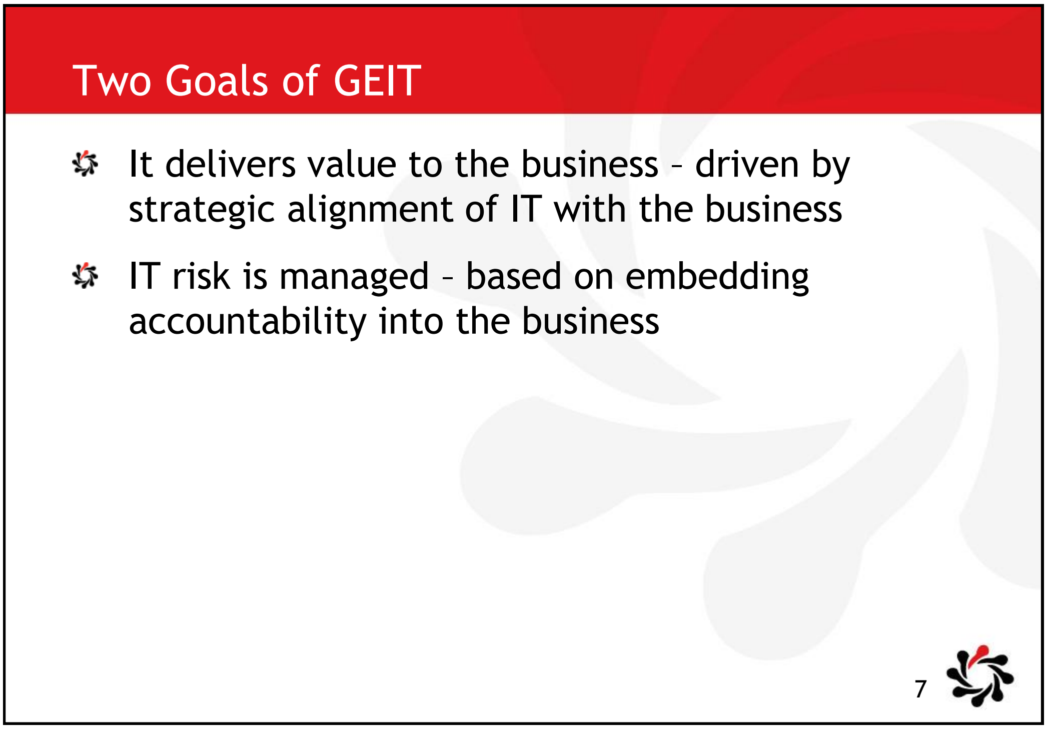
Corporate Governance

- Senior management sign off on the adequacy of internal controls and include an assessment of internal controls in financial reports
- Involves all the stakeholders in the decision-making process



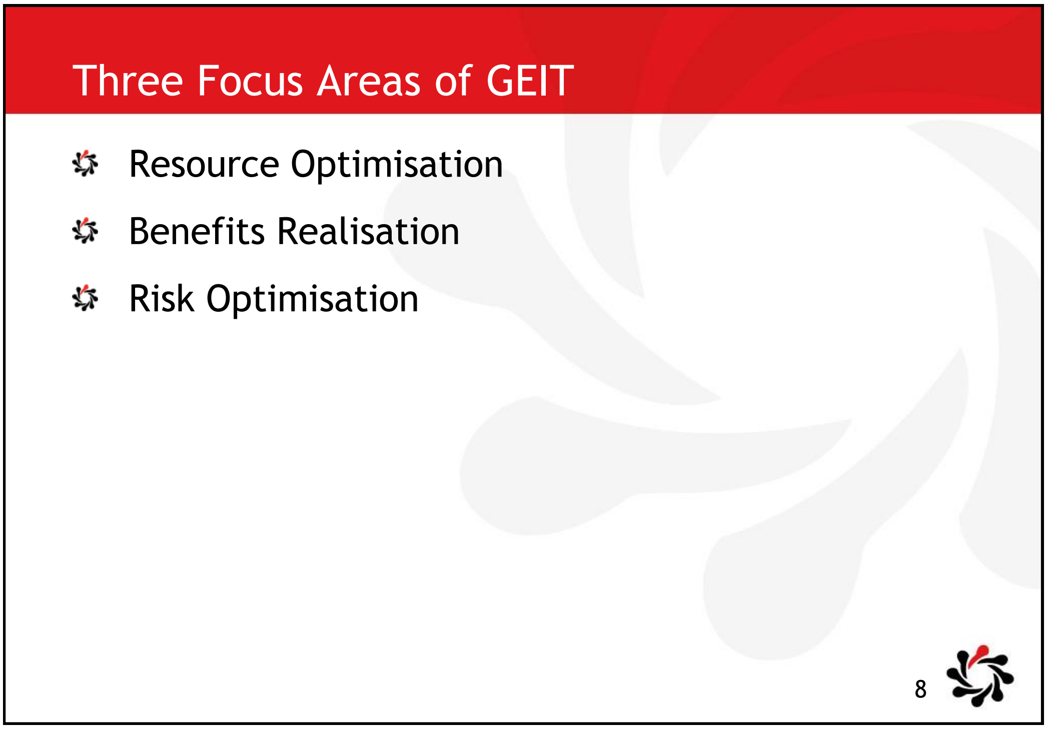
Governance of Enterprise IT (GEIT)

- Responsibility of the Board of Directors and Senior Management
- Includes:
  - IT resource management
  - Performance measurement
  - Compliance management



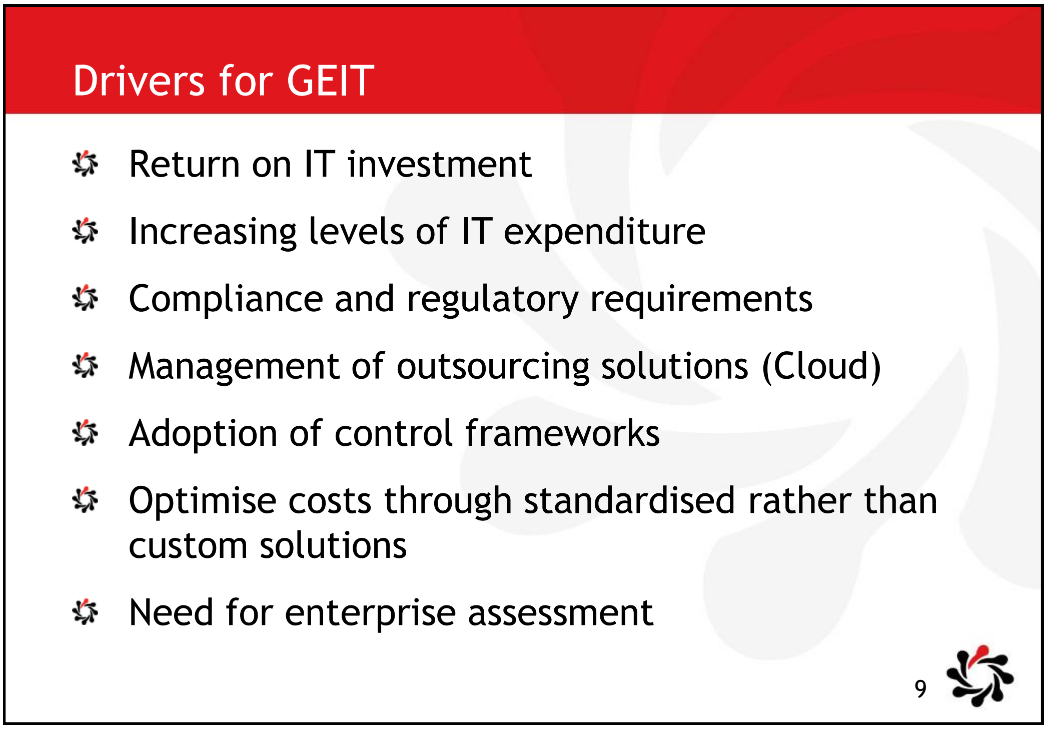
Two Goals of GEIT

- It delivers value to the business – driven by strategic alignment of IT with the business
- IT risk is managed – based on embedding accountability into the business



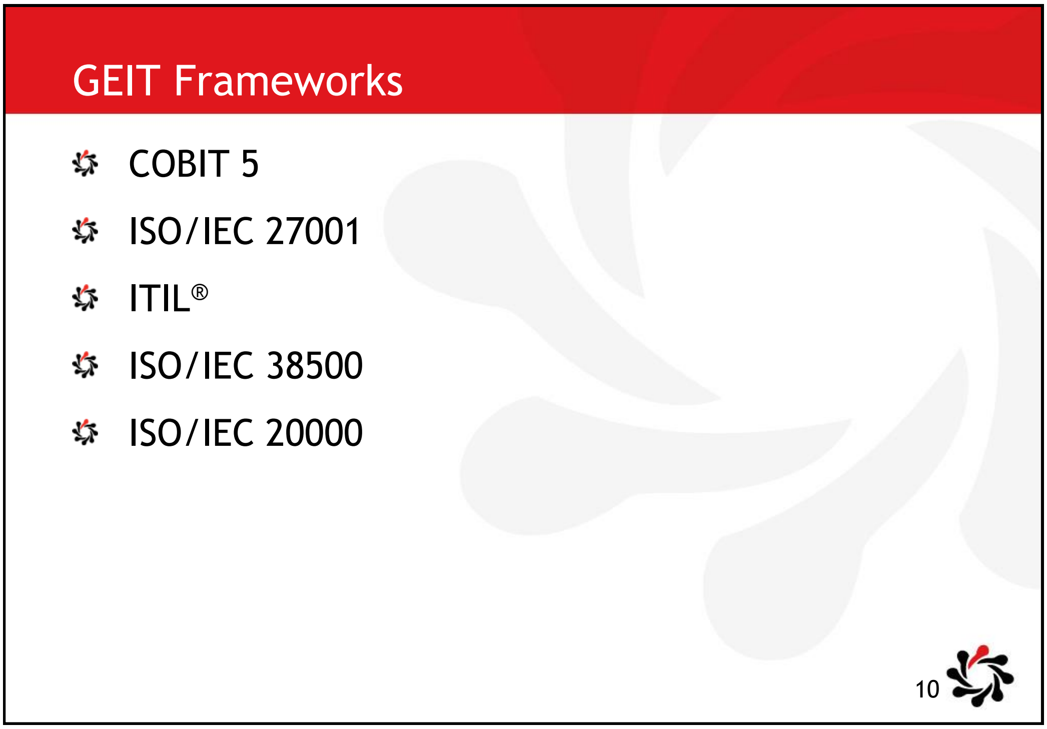
Three Focus Areas of GEIT

- Resource Optimisation
- Benefits Realisation
- Risk Optimisation



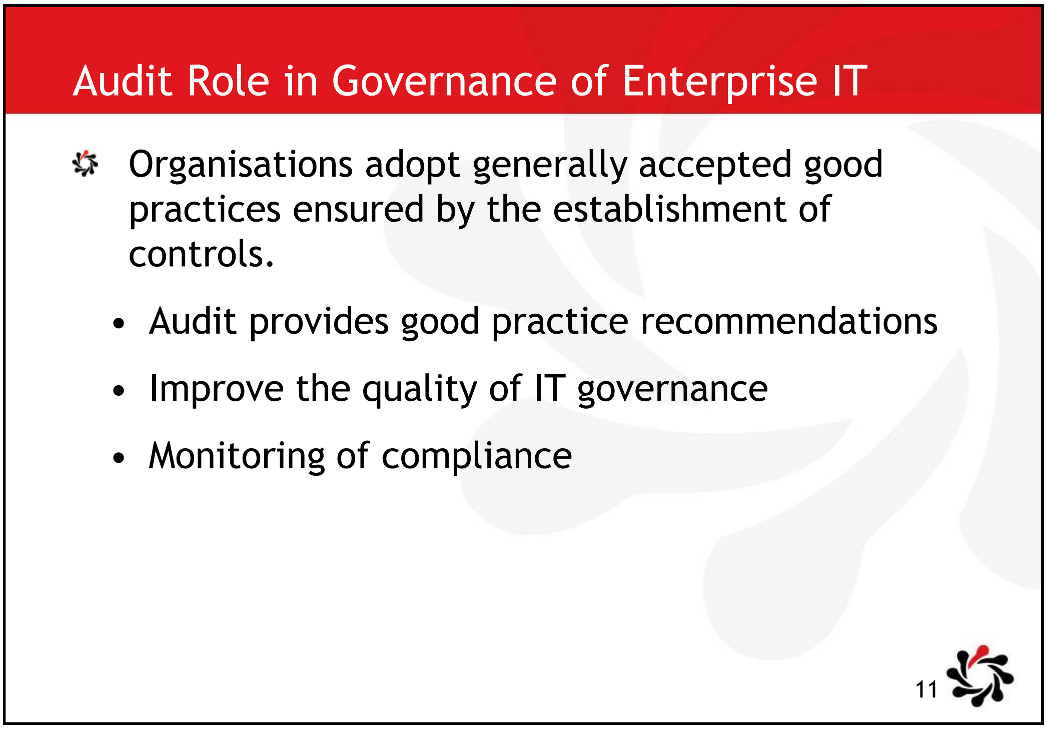
Drivers for GEIT

- Return on IT investment
- Increasing levels of IT expenditure
- Compliance and regulatory requirements
- Management of outsourcing solutions (Cloud)
- Adoption of control frameworks
- Optimise costs through standardised rather than custom solutions
- Need for enterprise assessment



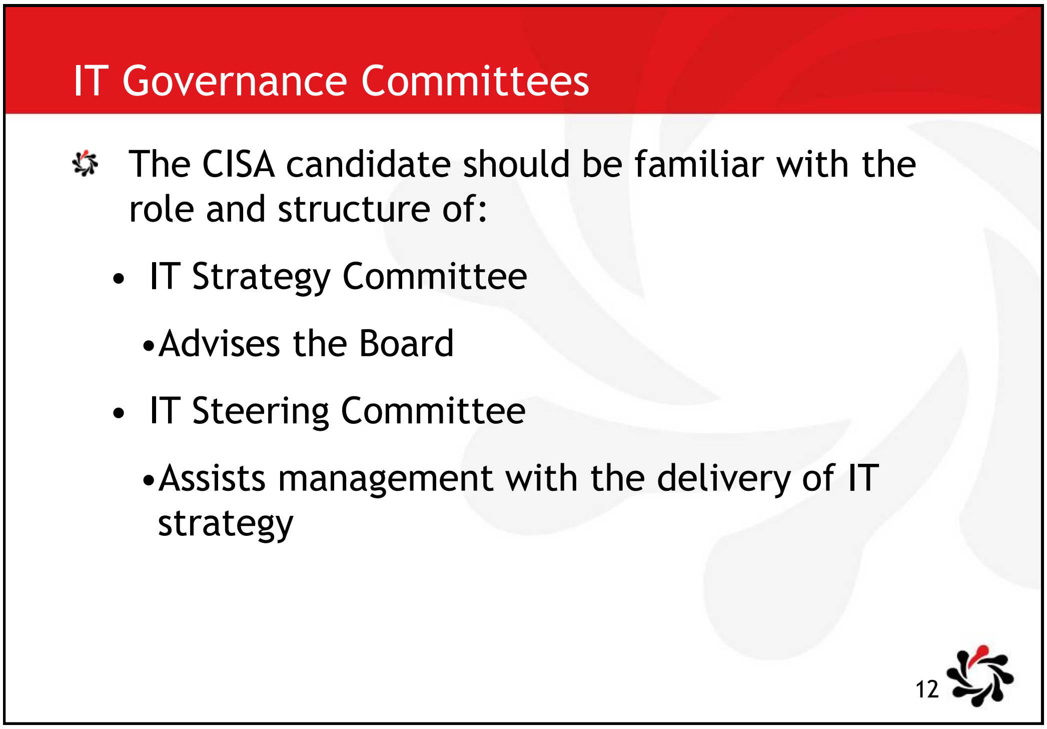
GEIT Frameworks

- COBIT 5
- ISO/IEC 27001
- ITIL®
- ISO/IEC 38500
- ISO/IEC 20000



Audit Role in Governance of Enterprise IT

- Organisations adopt generally accepted good practices ensured by the establishment of controls.
  - Audit provides good practice recommendations
  - Improve the quality of IT governance
  - Monitoring of compliance

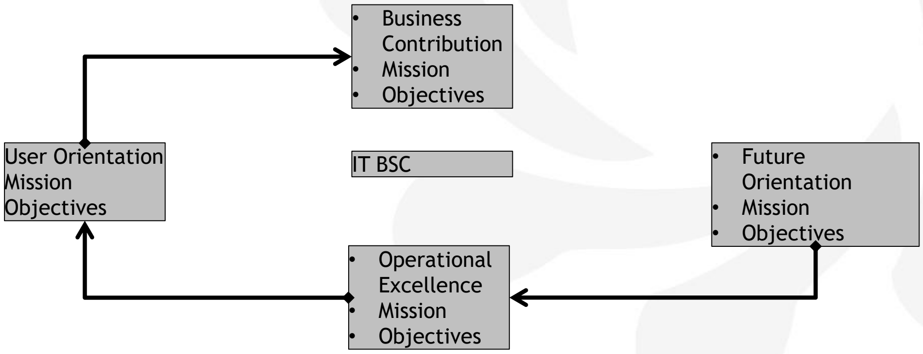


IT Governance Committees

- The CISA candidate should be familiar with the role and structure of:
  - IT Strategy Committee
    - Advises the Board
  - IT Steering Committee
    - Assists management with the delivery of IT strategy

IT Balanced Scorecard

- Process management technique used to assess IT functions and processes



- Business Contribution
- Mission
- Objectives

User Orientation
Mission
Objectives

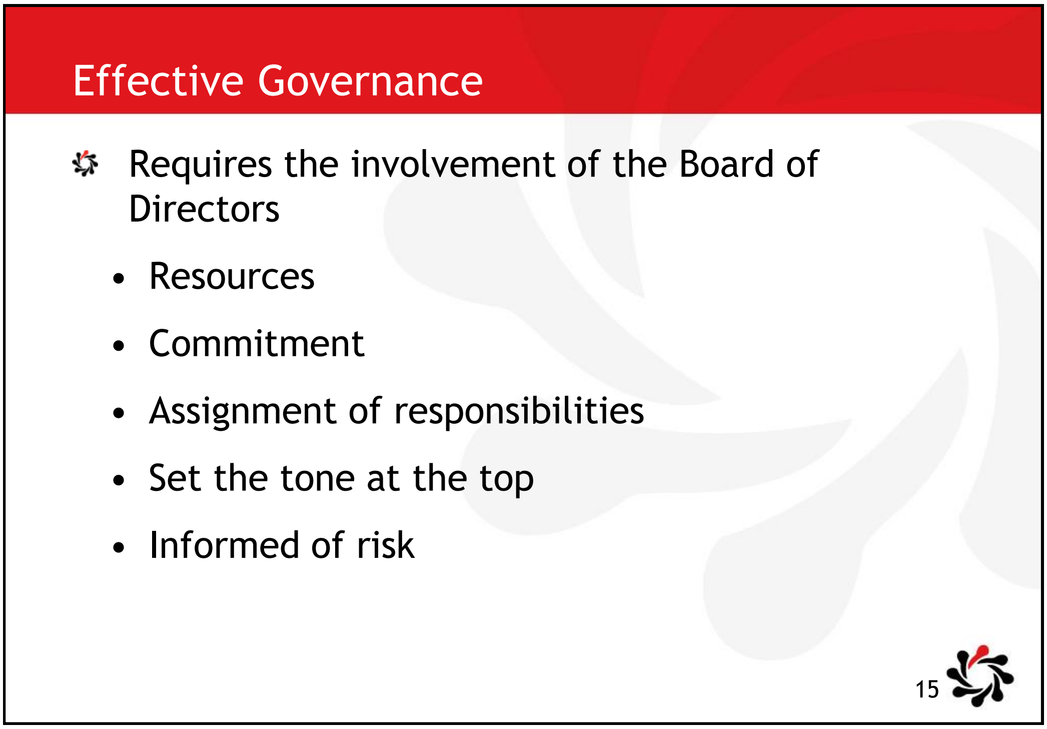
IT BSC

- Future Orientation
- Mission
- Objectives

- Operational Excellence
- Mission
- Objectives

Effective Information Security Governance

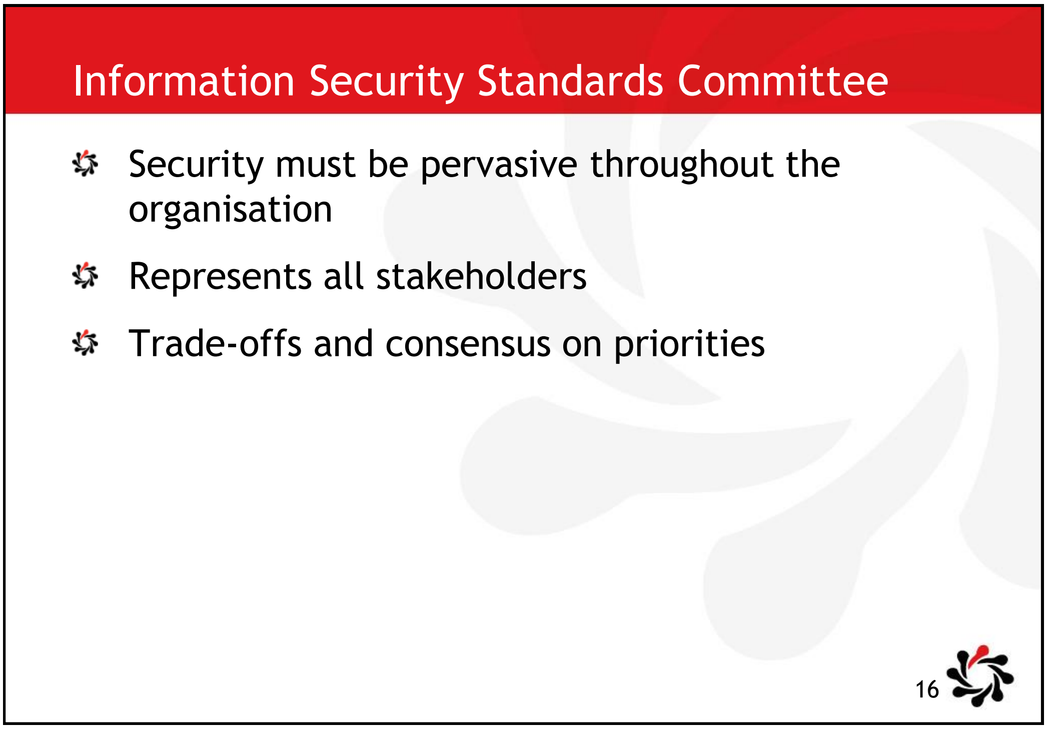
- Consists of:
  - Security strategy
  - Security policies
  - Set of standards for each policy
  - Effective organisational security structure
    - Void of conflicts of interest
  - Institutionalised monitoring program
    - Ensure compliance and feedback



Effective Governance

- Requires the involvement of the Board of Directors
  - Resources
  - Commitment
  - Assignment of responsibilities
  - Set the tone at the top
  - Informed of risk

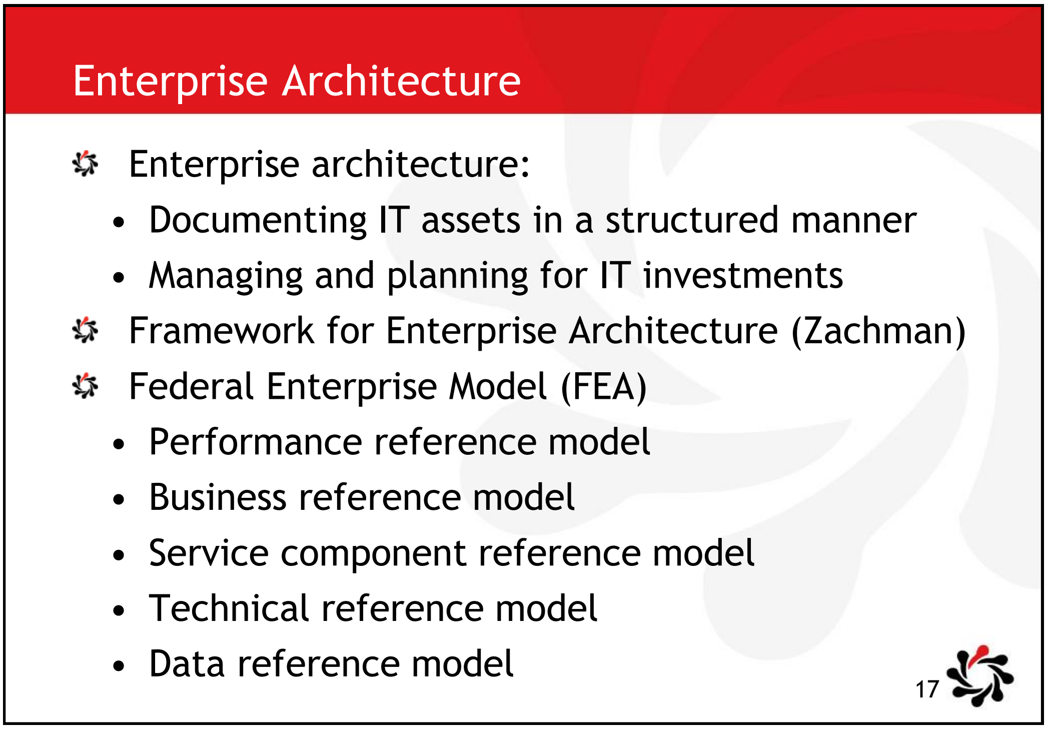
15



Information Security Standards Committee

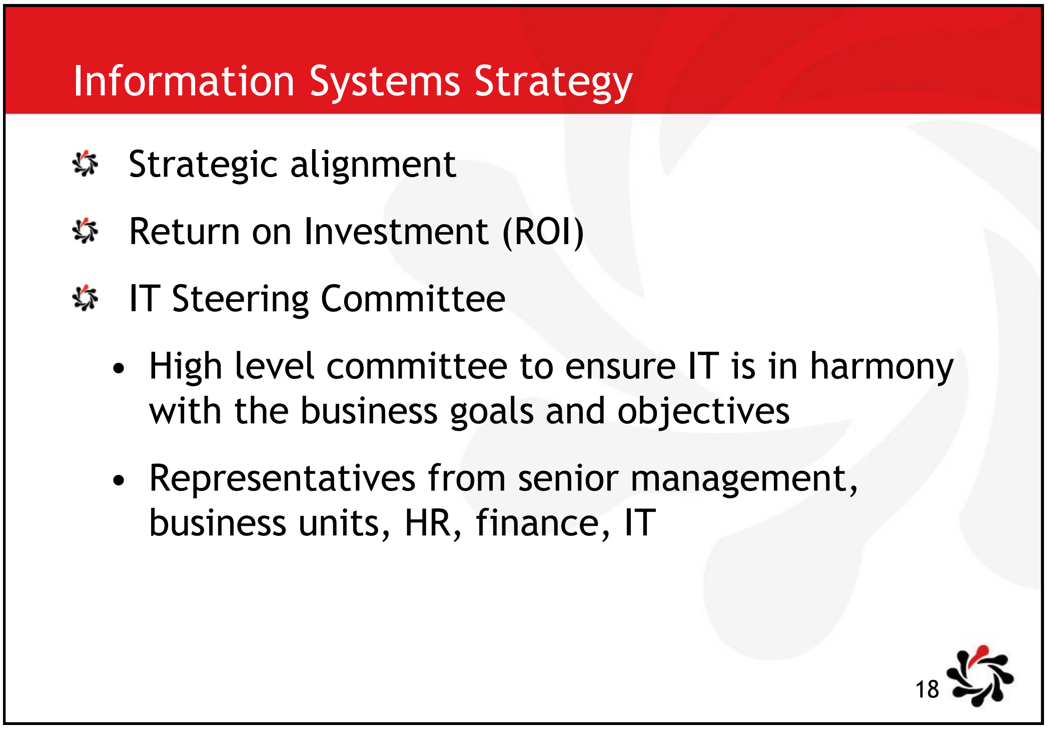
- Security must be pervasive throughout the organisation
- Represents all stakeholders
- Trade-offs and consensus on priorities

16



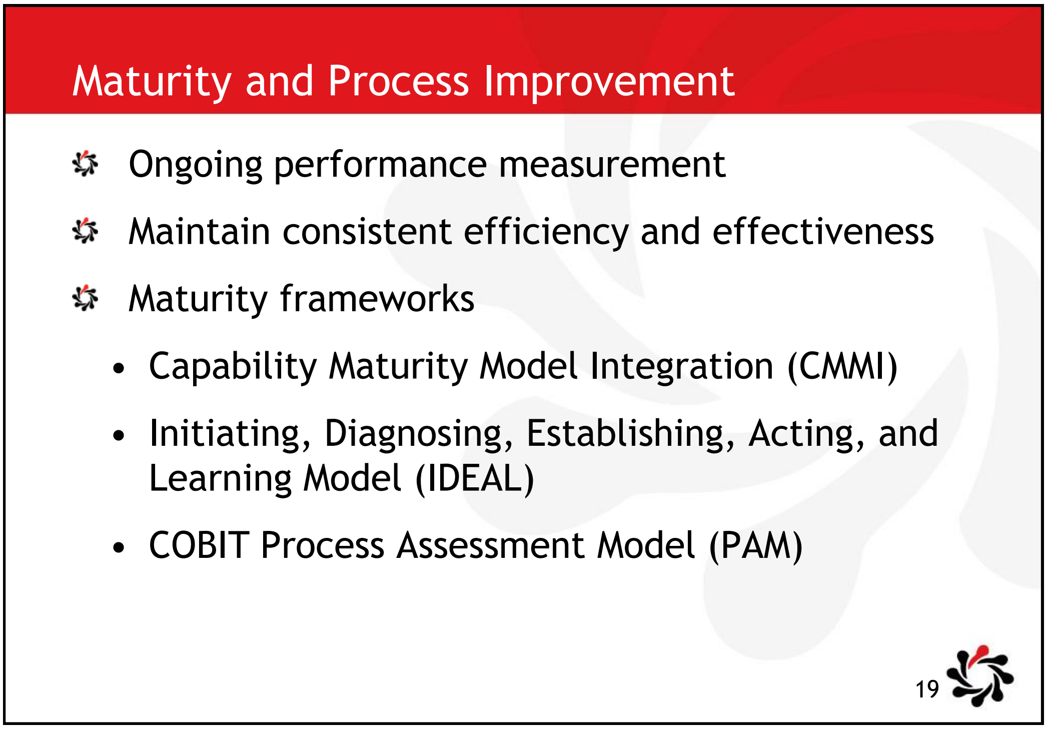
Enterprise Architecture

- Enterprise architecture:
  - Documenting IT assets in a structured manner
  - Managing and planning for IT investments
- Framework for Enterprise Architecture (Zachman)
- Federal Enterprise Model (FEA)
  - Performance reference model
  - Business reference model
  - Service component reference model
  - Technical reference model
  - Data reference model



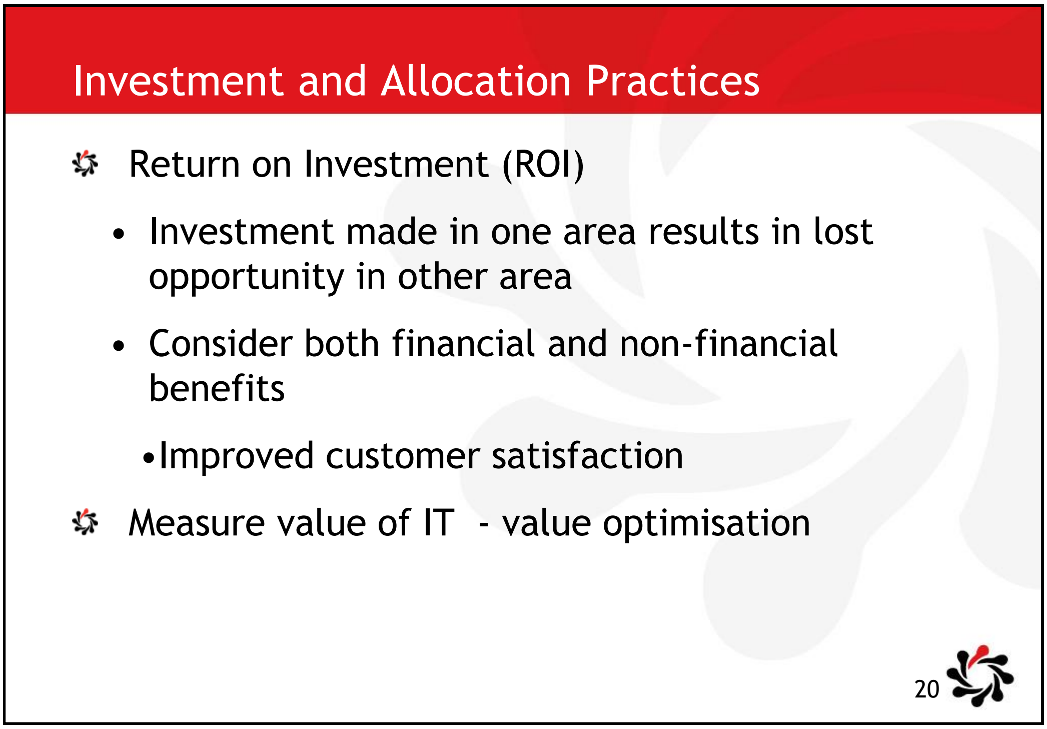
Information Systems Strategy

- Strategic alignment
- Return on Investment (ROI)
- IT Steering Committee
  - High level committee to ensure IT is in harmony with the business goals and objectives
  - Representatives from senior management, business units, HR, finance, IT



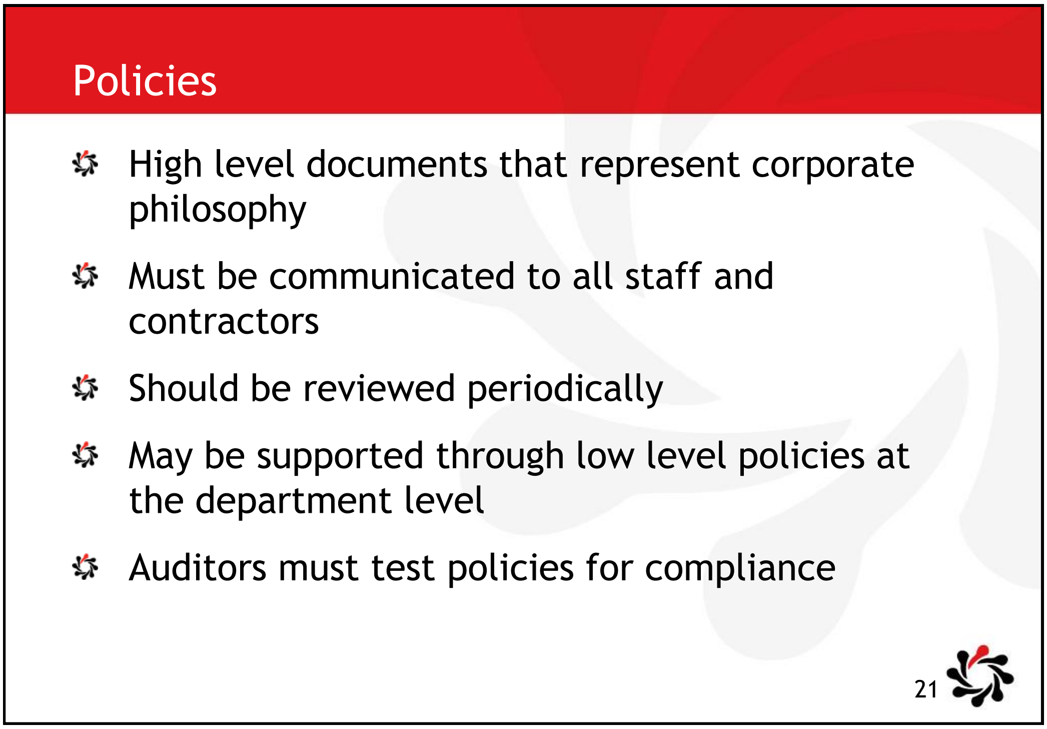
Maturity and Process Improvement

- Ongoing performance measurement
- Maintain consistent efficiency and effectiveness
- Maturity frameworks
  - Capability Maturity Model Integration (CMMI)
  - Initiating, Diagnosing, Establishing, Acting, and Learning Model (IDEAL)
  - COBIT Process Assessment Model (PAM)



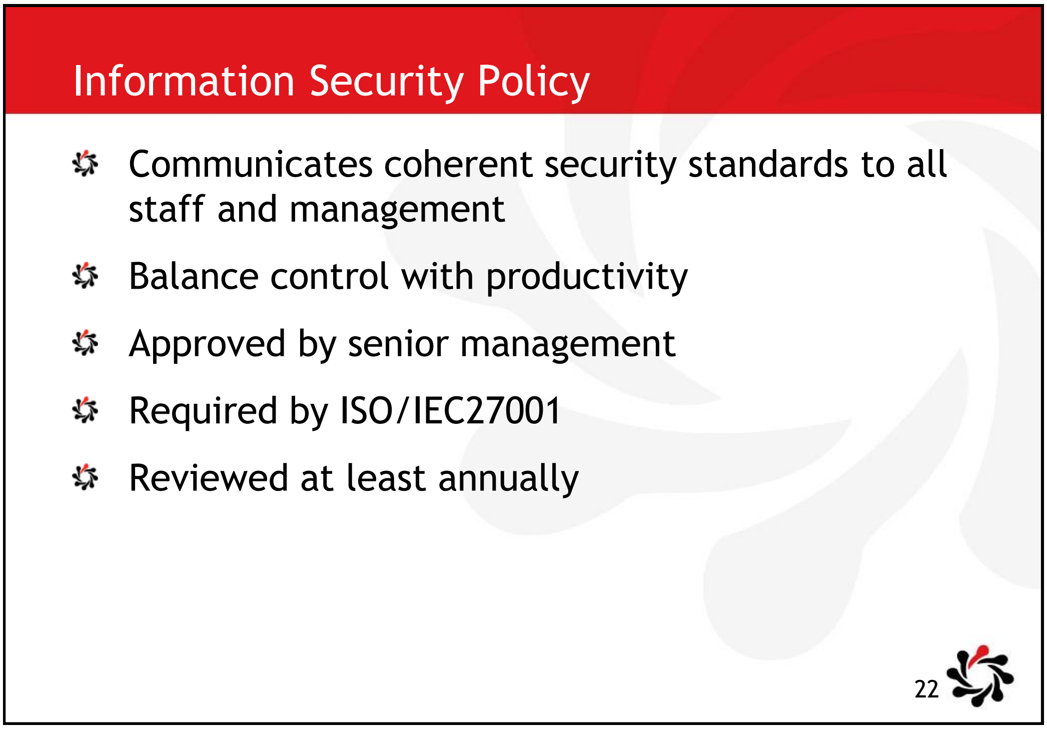
Investment and Allocation Practices

- Return on Investment (ROI)
  - Investment made in one area results in lost opportunity in other area
  - Consider both financial and non-financial benefits
    - Improved customer satisfaction
- Measure value of IT - value optimisation



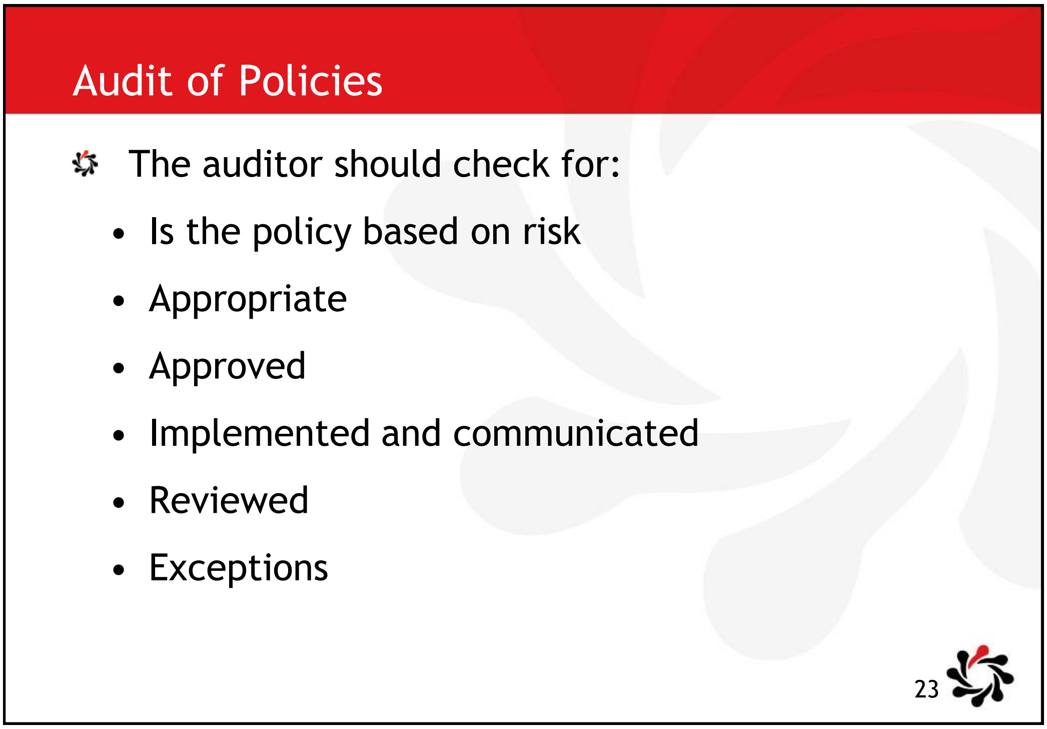
Policies

- High level documents that represent corporate philosophy
- Must be communicated to all staff and contractors
- Should be reviewed periodically
- May be supported through low level policies at the department level
- Auditors must test policies for compliance



Information Security Policy

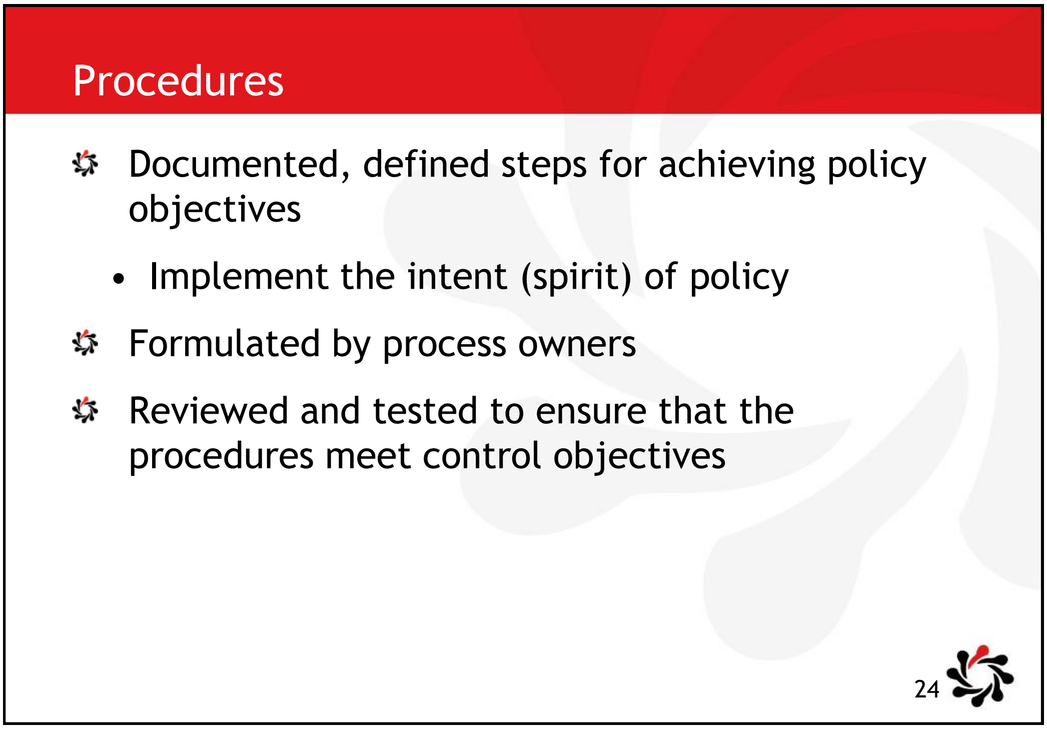
- Communicates coherent security standards to all staff and management
- Balance control with productivity
- Approved by senior management
- Required by ISO/IEC27001
- Reviewed at least annually



Audit of Policies

- The auditor should check for:
  - Is the policy based on risk
  - Appropriate
  - Approved
  - Implemented and communicated
  - Reviewed
  - Exceptions

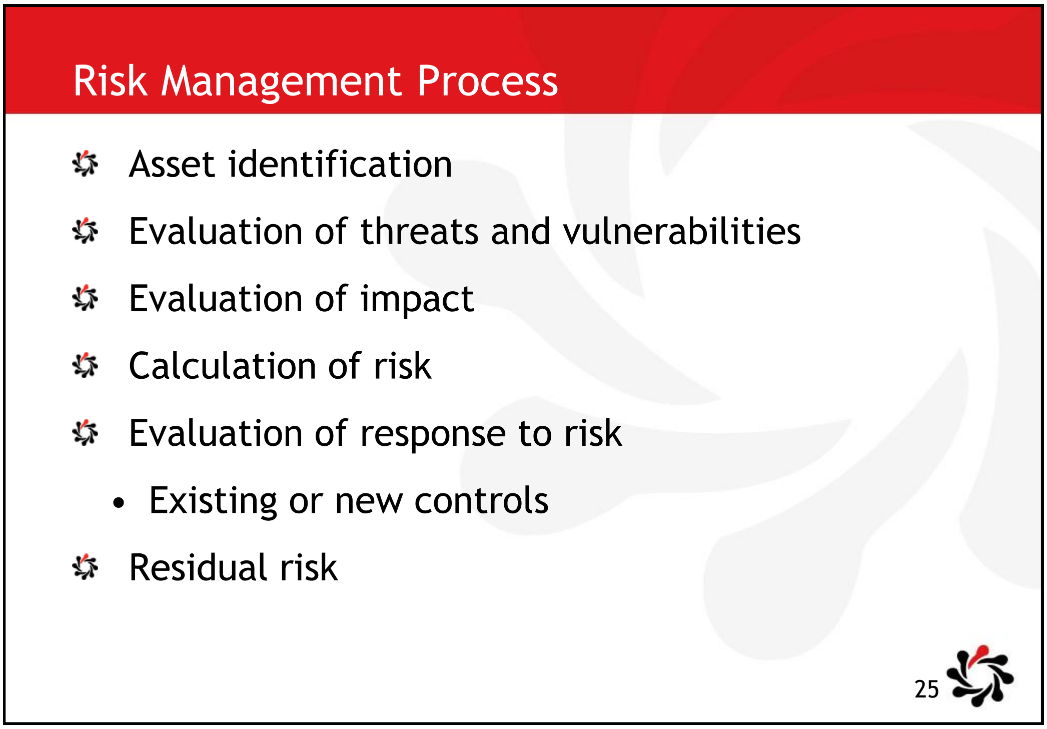
23



Procedures

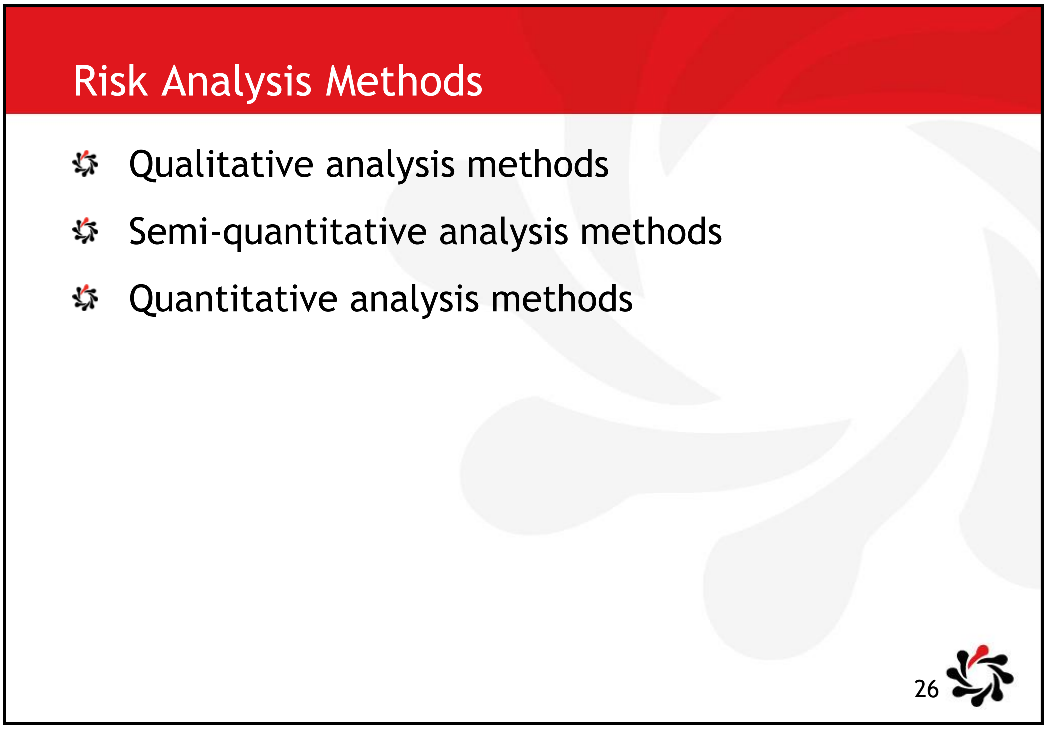
- Documented, defined steps for achieving policy objectives
  - Implement the intent (spirit) of policy
- Formulated by process owners
- Reviewed and tested to ensure that the procedures meet control objectives

24



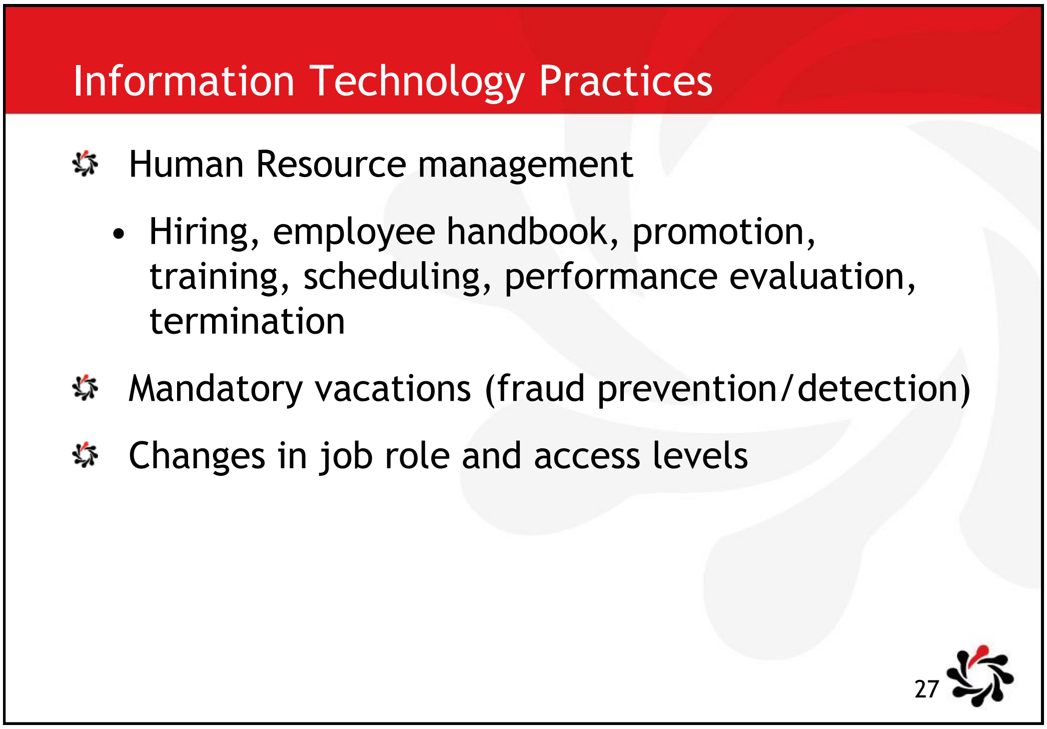
Risk Management Process

- Asset identification
- Evaluation of threats and vulnerabilities
- Evaluation of impact
- Calculation of risk
- Evaluation of response to risk
  - Existing or new controls
- Residual risk



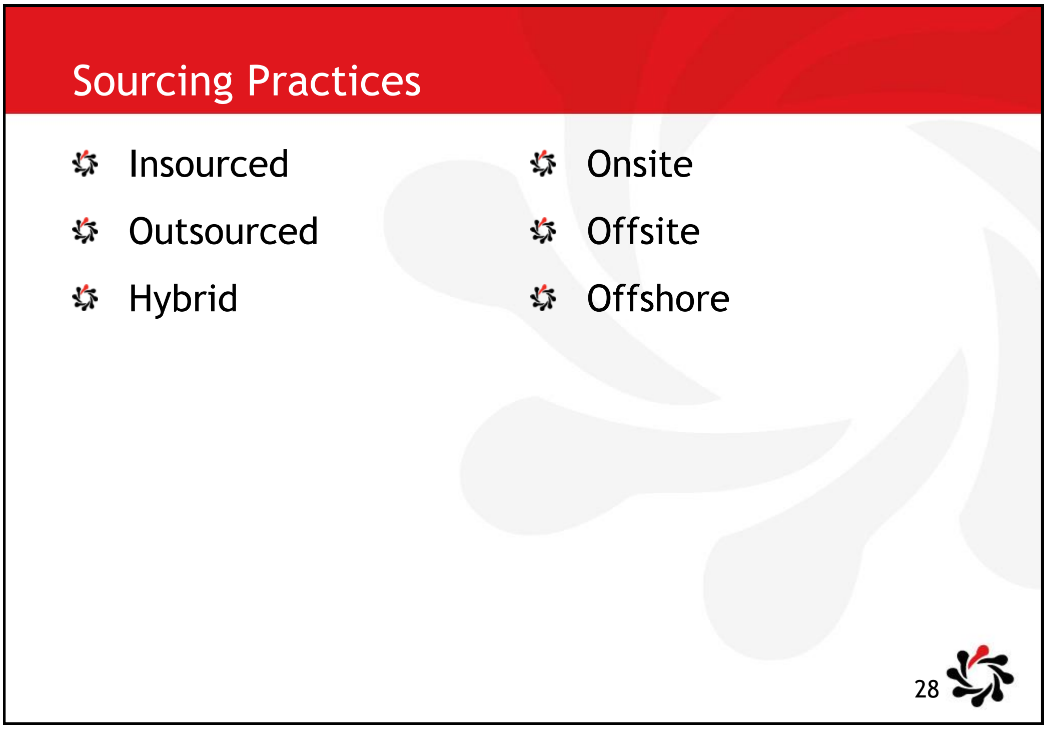
Risk Analysis Methods

- Qualitative analysis methods
- Semi-quantitative analysis methods
- Quantitative analysis methods



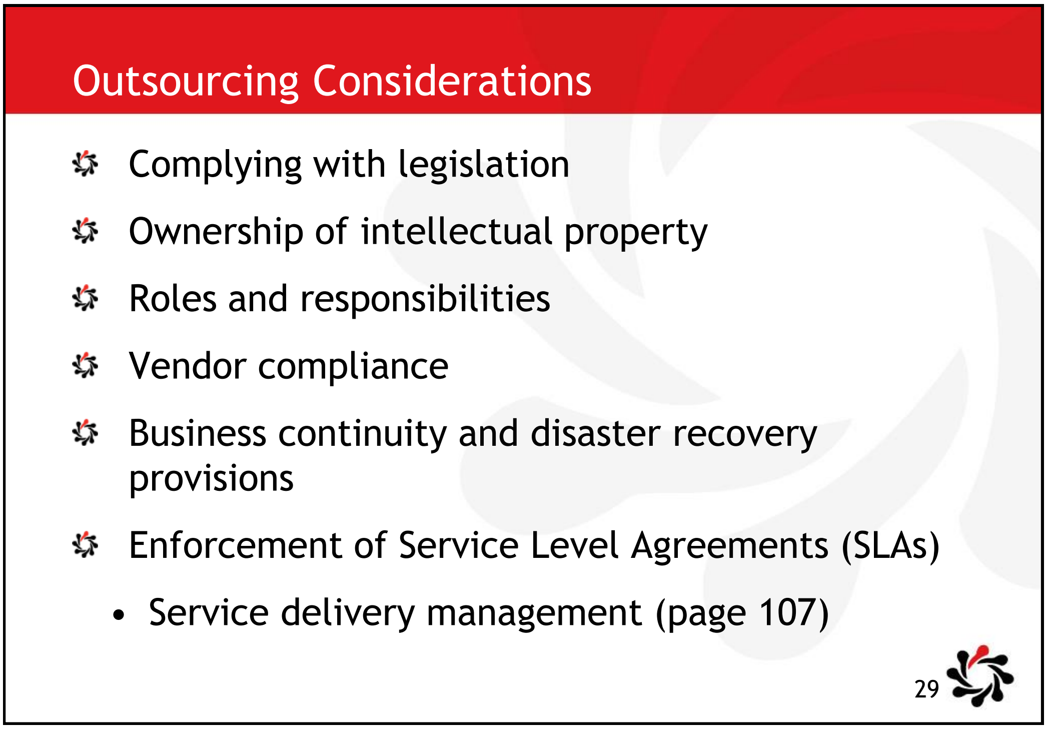
Information Technology Practices

- Human Resource management
  - Hiring, employee handbook, promotion, training, scheduling, performance evaluation, termination
- Mandatory vacations (fraud prevention/detection)
- Changes in job role and access levels



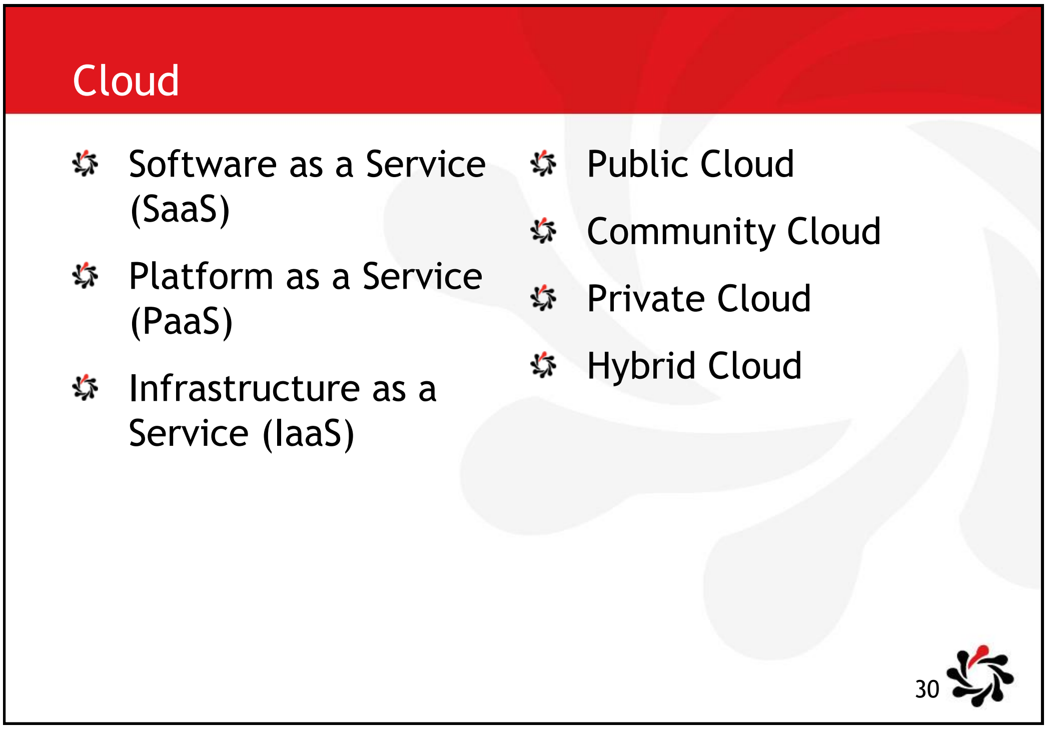
Sourcing Practices

- Insourced
- Outsourced
- Hybrid
- Onsite
- Offsite
- Offshore



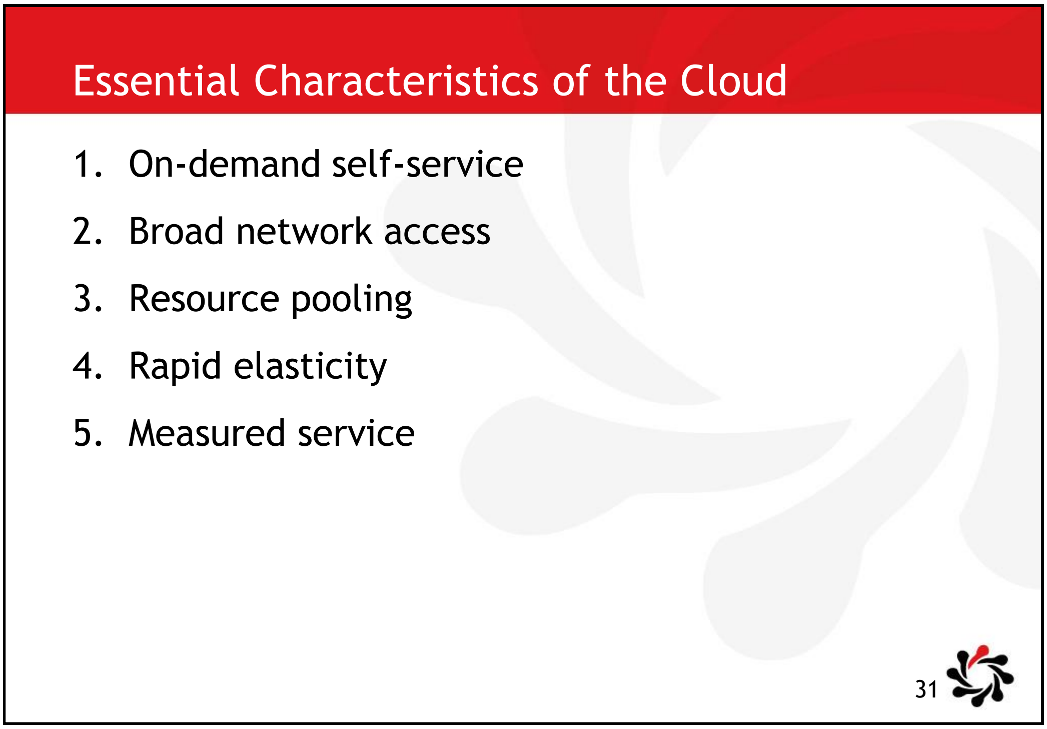
Outsourcing Considerations

- Complying with legislation
- Ownership of intellectual property
- Roles and responsibilities
- Vendor compliance
- Business continuity and disaster recovery provisions
- Enforcement of Service Level Agreements (SLAs)
  - Service delivery management (page 107)



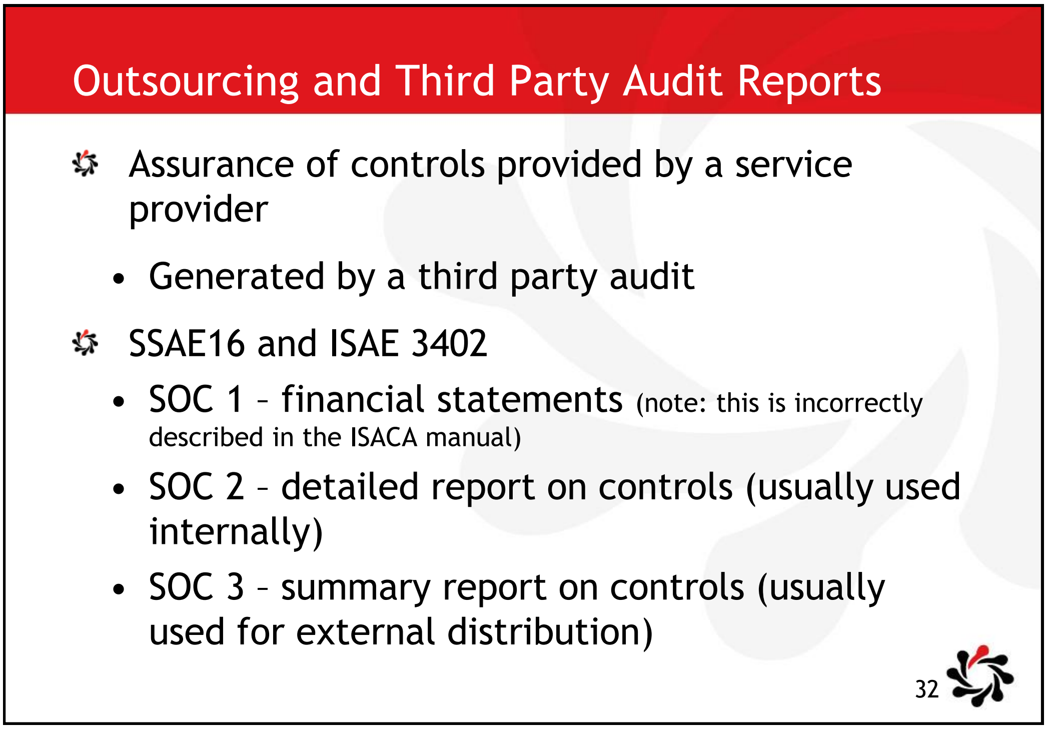
Cloud

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Public Cloud
- Community Cloud
- Private Cloud
- Hybrid Cloud



Essential Characteristics of the Cloud

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

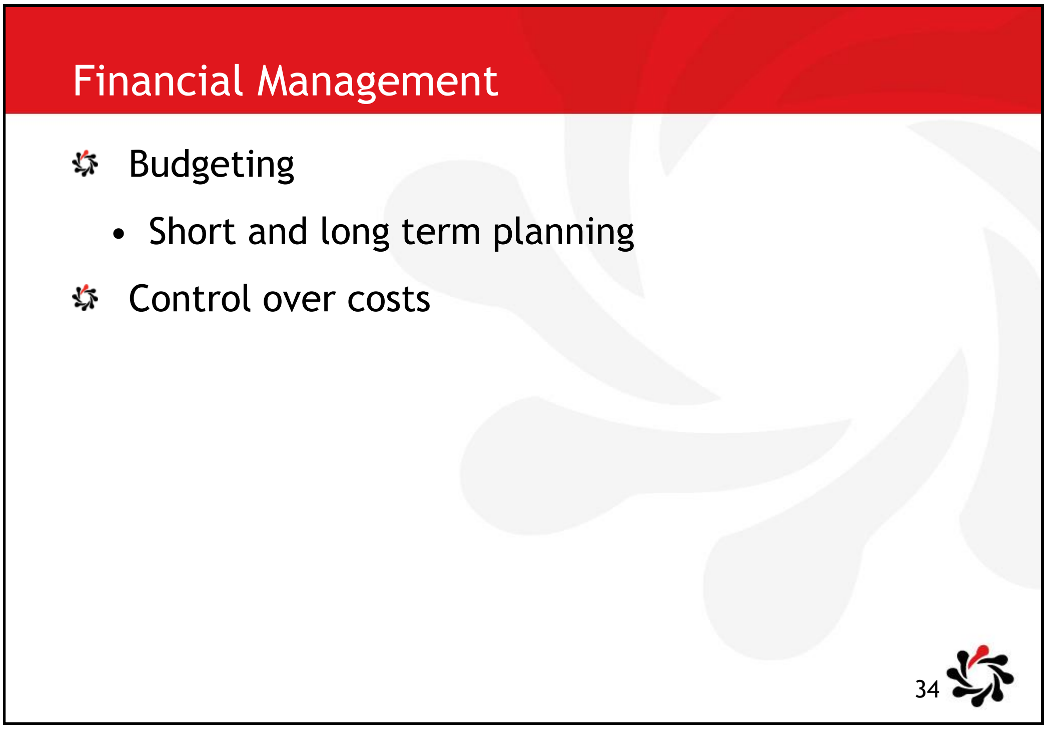


Outsourcing and Third Party Audit Reports

- Assurance of controls provided by a service provider
  - Generated by a third party audit
- SSAE16 and ISAE 3402
  - SOC 1 – financial statements (note: this is incorrectly described in the ISACA manual)
  - SOC 2 – detailed report on controls (usually used internally)
  - SOC 3 – summary report on controls (usually used for external distribution)

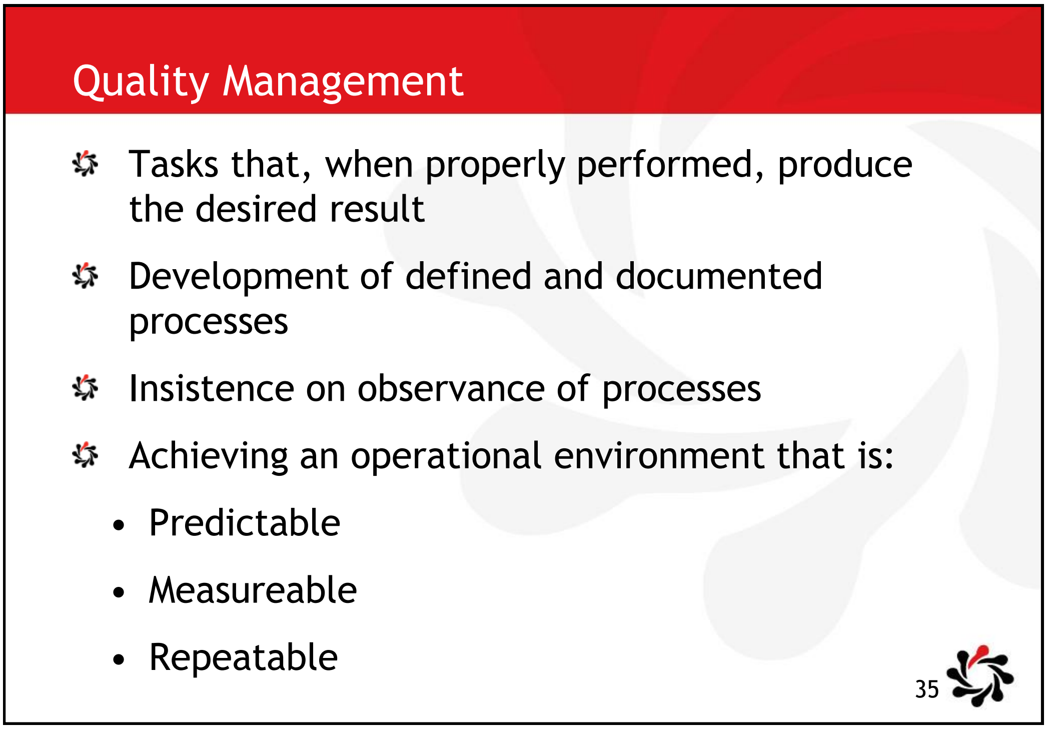
Monitoring and Review of Third Party Services

- Regular audits and reporting
- Monitoring performance levels
- Incident management reports
- Audit trails
- Resolve issues
- Change control process



Financial Management

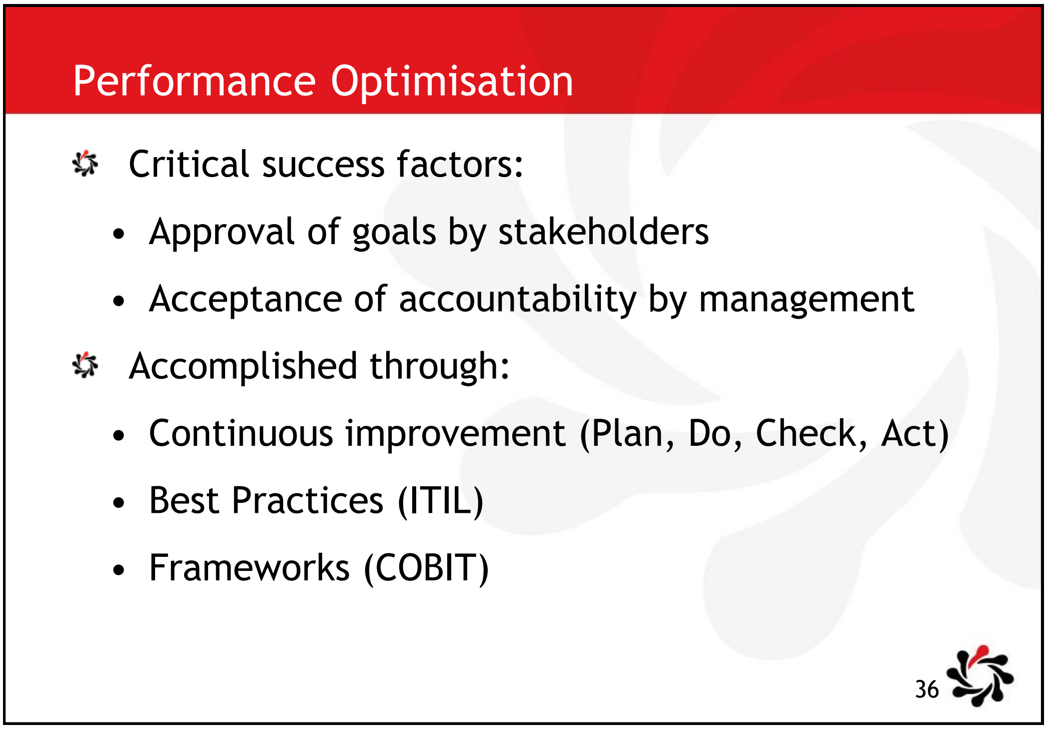
- Budgeting
  - Short and long term planning
- Control over costs



Quality Management

- Tasks that, when properly performed, produce the desired result
- Development of defined and documented processes
- Insistence on observance of processes
- Achieving an operational environment that is:
  - Predictable
  - Measureable
  - Repeatable

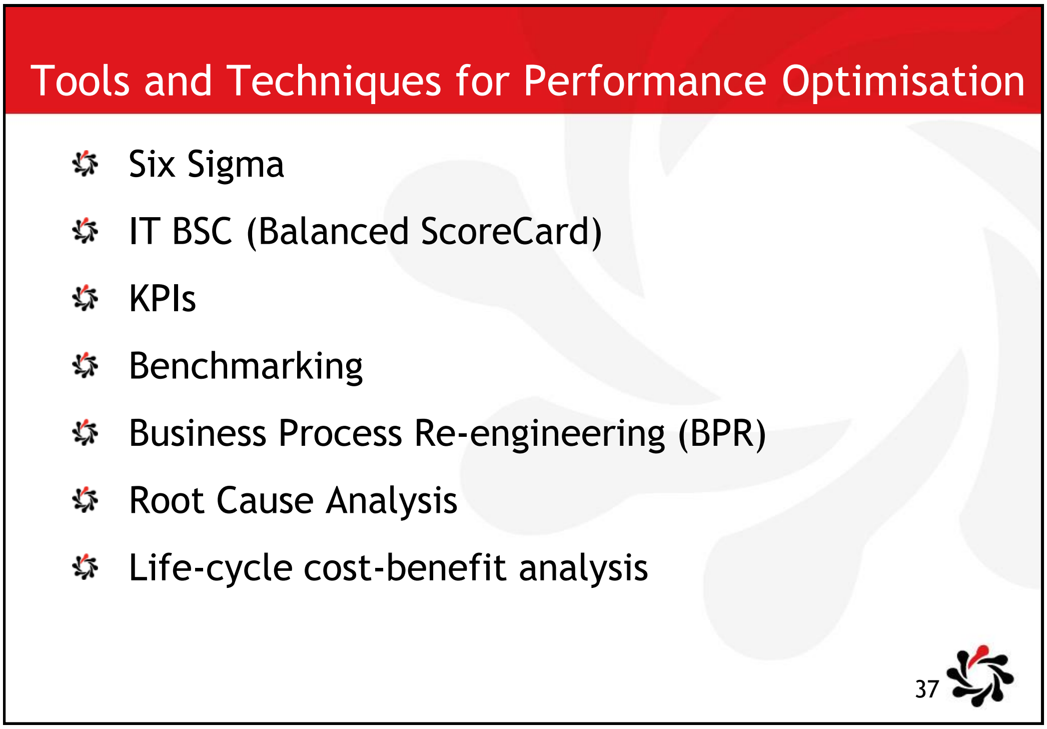
35



Performance Optimisation

- Critical success factors:
  - Approval of goals by stakeholders
  - Acceptance of accountability by management
- Accomplished through:
  - Continuous improvement (Plan, Do, Check, Act)
  - Best Practices (ITIL)
  - Frameworks (COBIT)

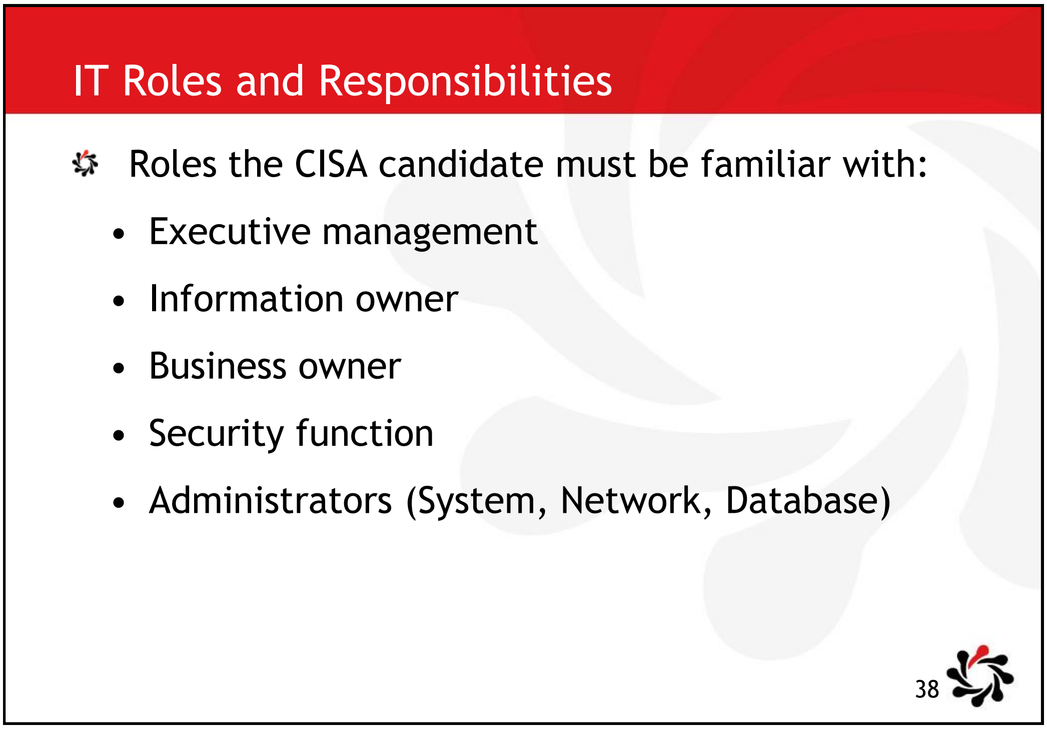
36



Tools and Techniques for Performance Optimisation

- Six Sigma
- IT BSC (Balanced ScoreCard)
- KPIs
- Benchmarking
- Business Process Re-engineering (BPR)
- Root Cause Analysis
- Life-cycle cost-benefit analysis

37



IT Roles and Responsibilities

- Roles the CISA candidate must be familiar with:
  - Executive management
  - Information owner
  - Business owner
  - Security function
  - Administrators (System, Network, Database)

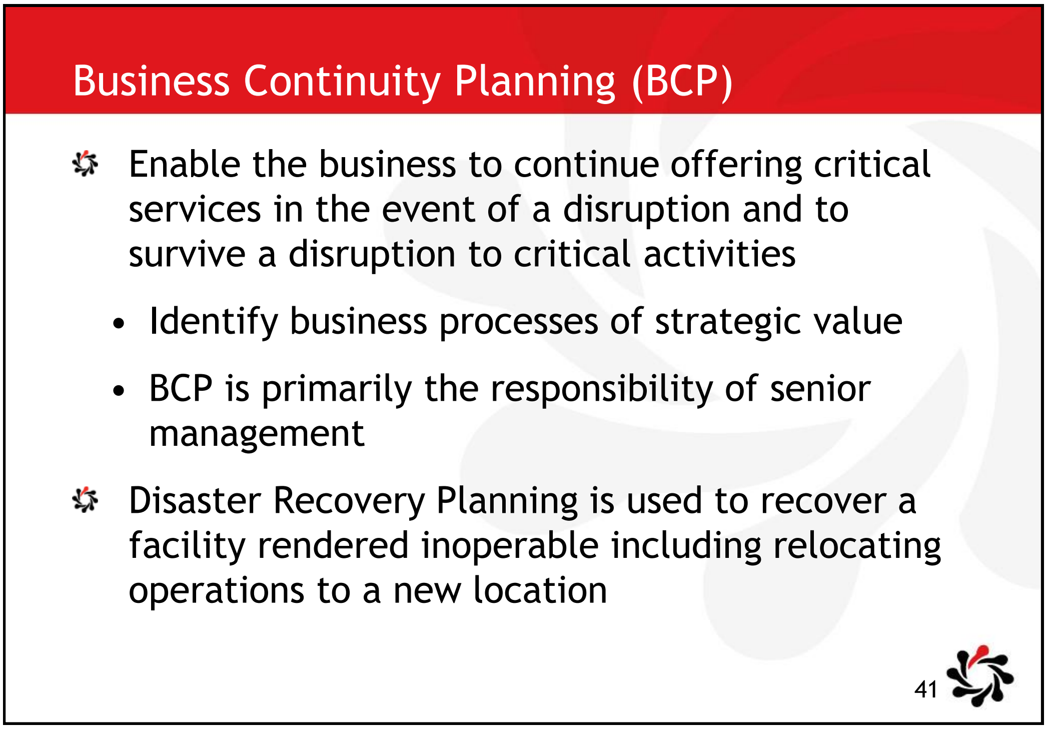
38

Separation/Segregation of Duties

- Roles that should be separated and which require compensating controls
  - Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be properly segregated
  - Authorisations, audit trails, reconciliation
- Privileged users
- Remote logging

Auditing IT Governance Structure and Implementation

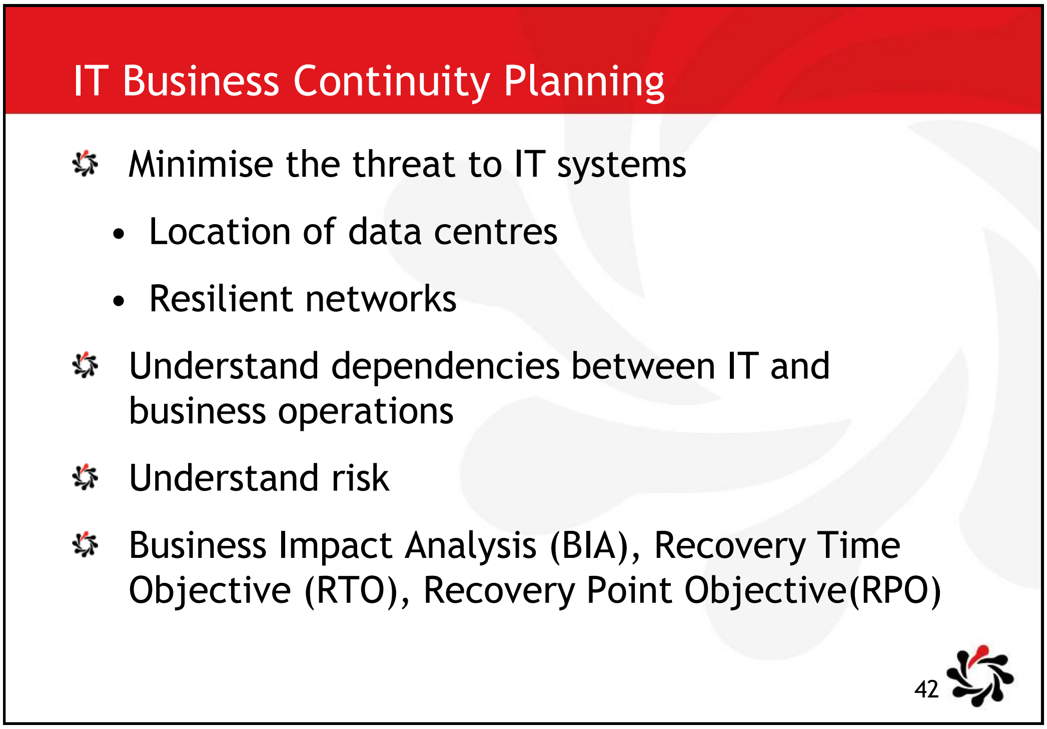
- Significant indicators of potential problems include:
  - Unfavourable end-user attitudes/high turnover
  - Excessive costs/budget overruns
  - Extensive exception reports
  - Slow response to user requests
  - Lack of training/succession plans



Business Continuity Planning (BCP)

- Enable the business to continue offering critical services in the event of a disruption and to survive a disruption to critical activities
  - Identify business processes of strategic value
  - BCP is primarily the responsibility of senior management
- Disaster Recovery Planning is used to recover a facility rendered inoperable including relocating operations to a new location

41



IT Business Continuity Planning

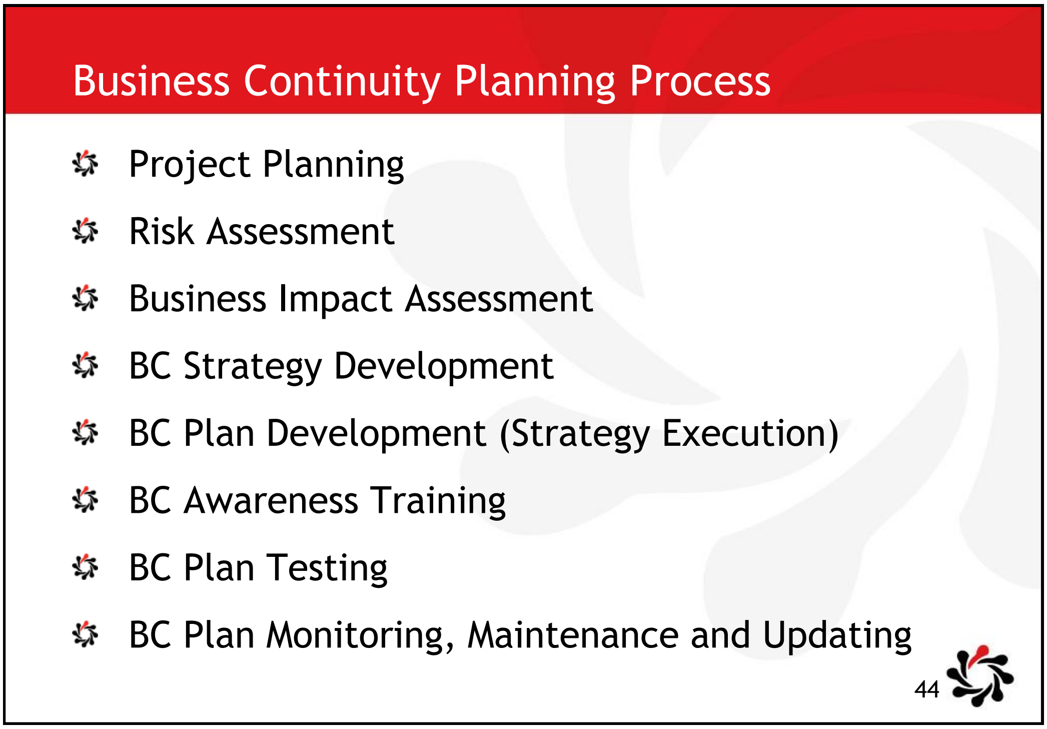
- Minimise the threat to IT systems
  - Location of data centres
  - Resilient networks
- Understand dependencies between IT and business operations
- Understand risk
- Business Impact Analysis (BIA), Recovery Time Objective (RTO), Recovery Point Objective(RPO)

42

Disruptive Events

- Natural events
- Pandemic
- Damage to reputation or brand
- Unanticipated/unforeseeable events (black swan events)

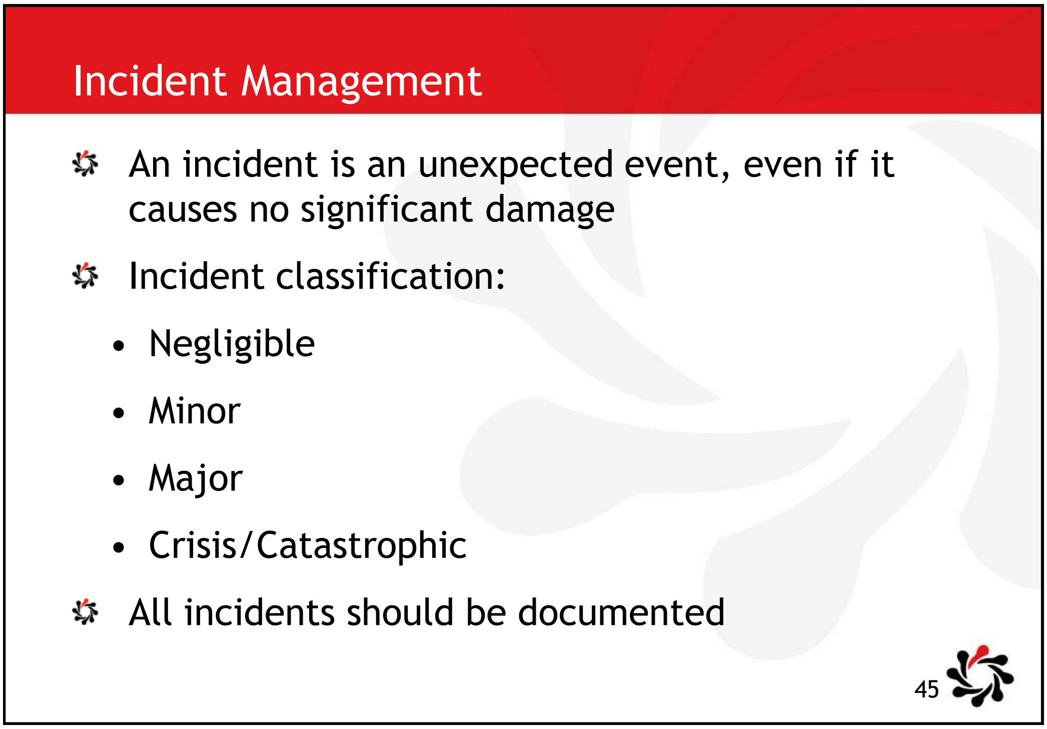
43



Business Continuity Planning Process

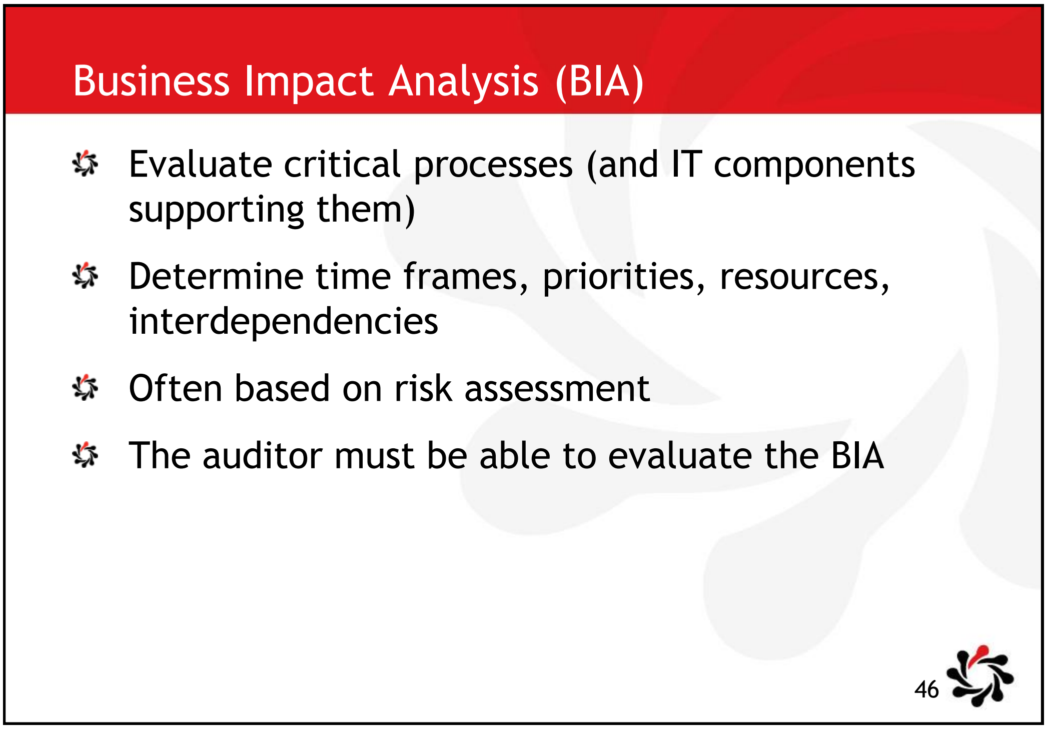
- Project Planning
- Risk Assessment
- Business Impact Assessment
- BC Strategy Development
- BC Plan Development (Strategy Execution)
- BC Awareness Training
- BC Plan Testing
- BC Plan Monitoring, Maintenance and Updating

44



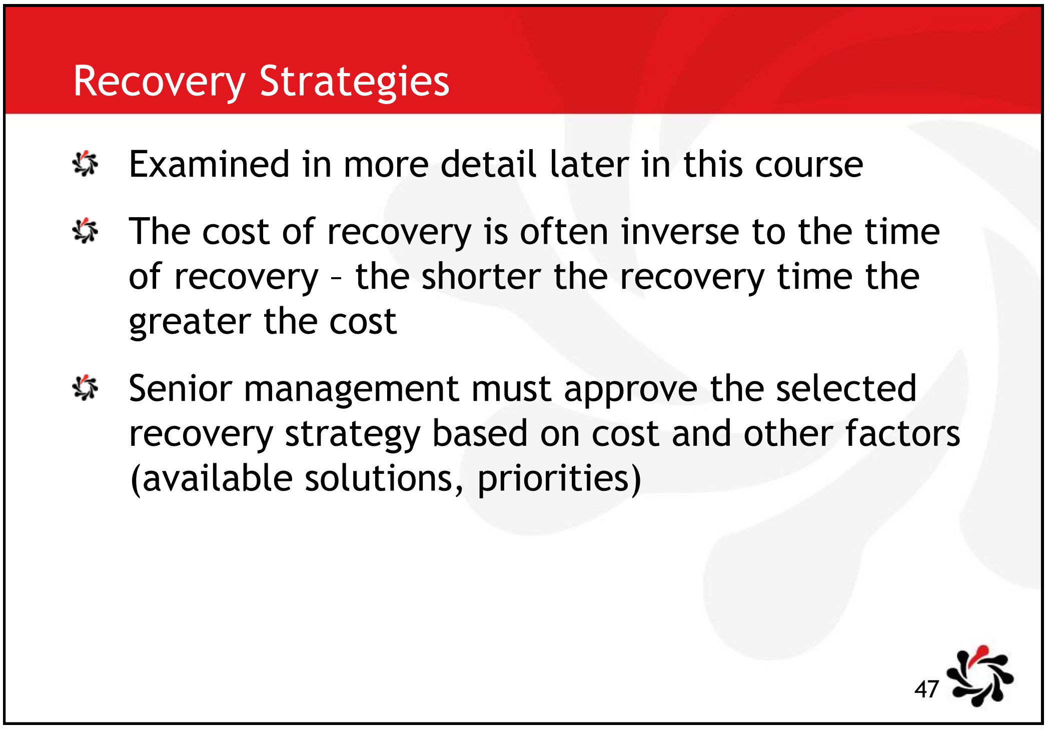
Incident Management

- An incident is an unexpected event, even if it causes no significant damage
- Incident classification:
  - Negligible
  - Minor
  - Major
  - Crisis/Catastrophic
- All incidents should be documented



Business Impact Analysis (BIA)

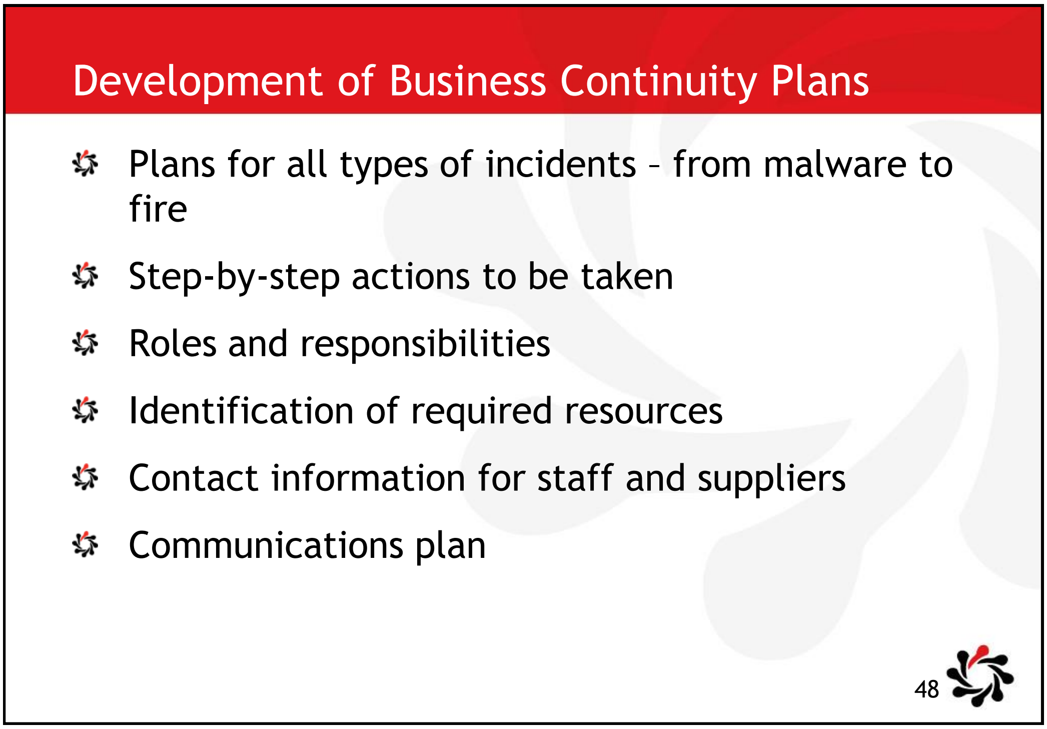
- Evaluate critical processes (and IT components supporting them)
- Determine time frames, priorities, resources, interdependencies
- Often based on risk assessment
- The auditor must be able to evaluate the BIA



Recovery Strategies

- Examined in more detail later in this course
- The cost of recovery is often inverse to the time of recovery – the shorter the recovery time the greater the cost
- Senior management must approve the selected recovery strategy based on cost and other factors (available solutions, priorities)

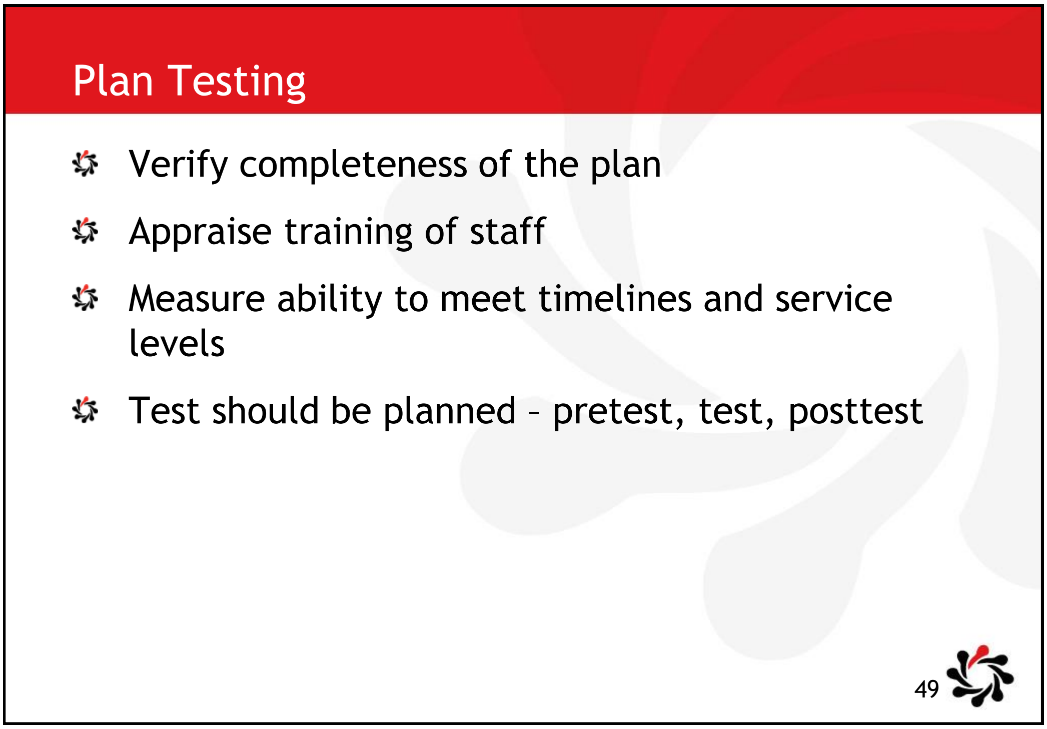
47



Development of Business Continuity Plans

- Plans for all types of incidents – from malware to fire
- Step-by-step actions to be taken
- Roles and responsibilities
- Identification of required resources
- Contact information for staff and suppliers
- Communications plan

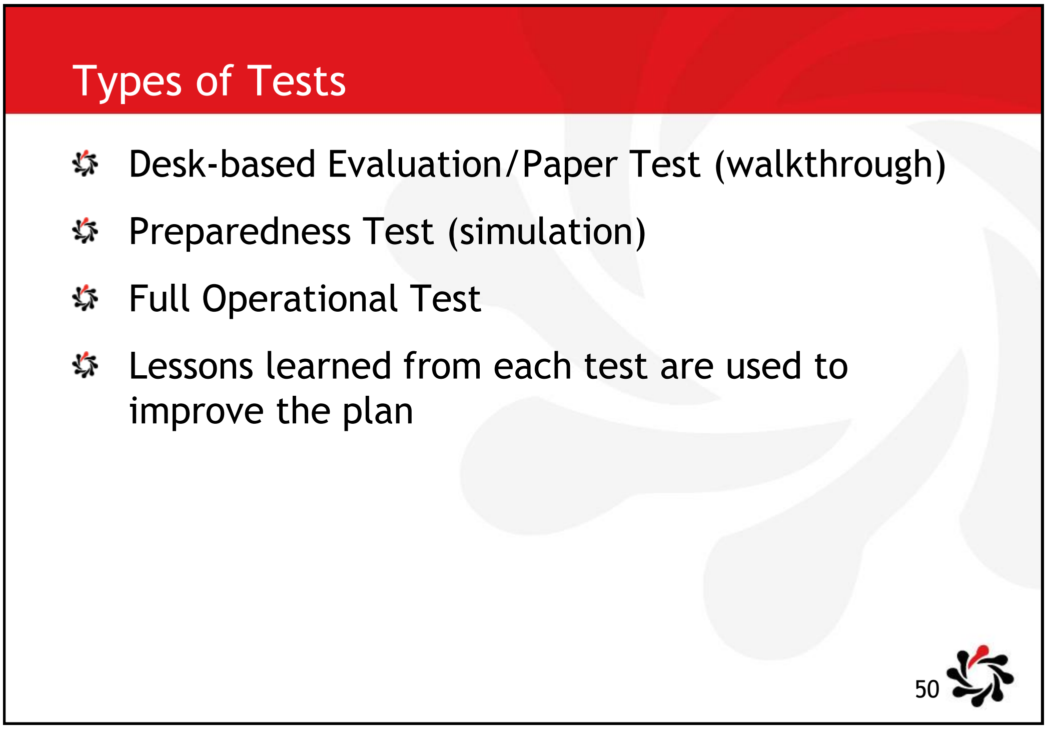
48



Plan Testing

- Verify completeness of the plan
- Appraise training of staff
- Measure ability to meet timelines and service levels
- Test should be planned – pretest, test, posttest

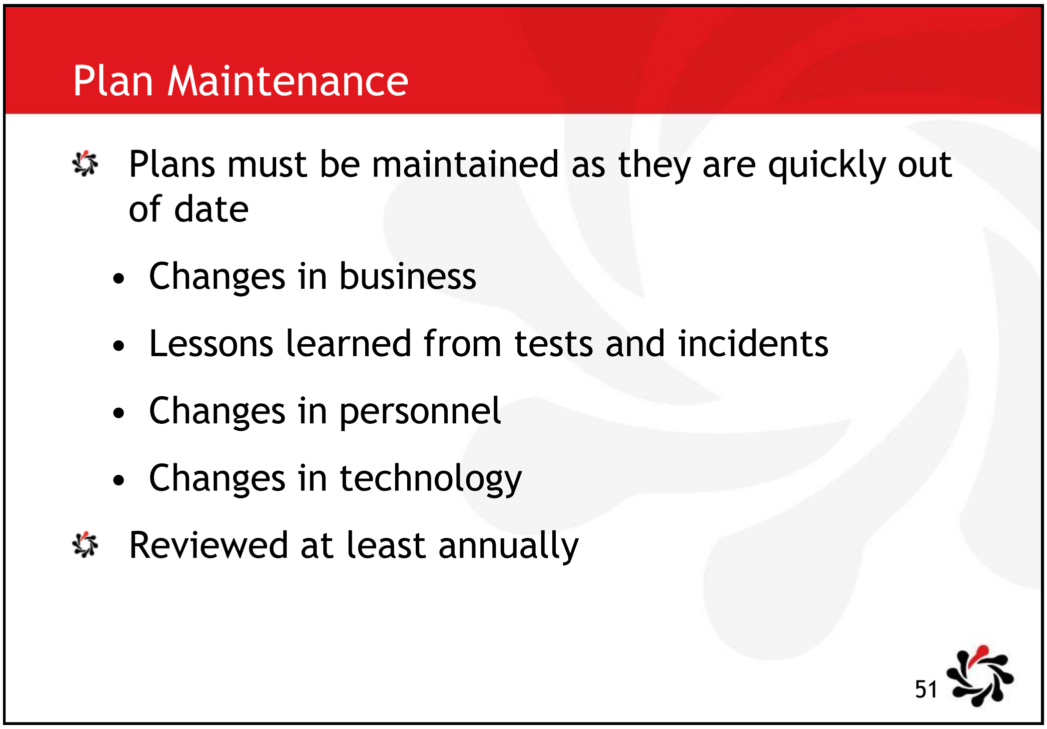
49



Types of Tests

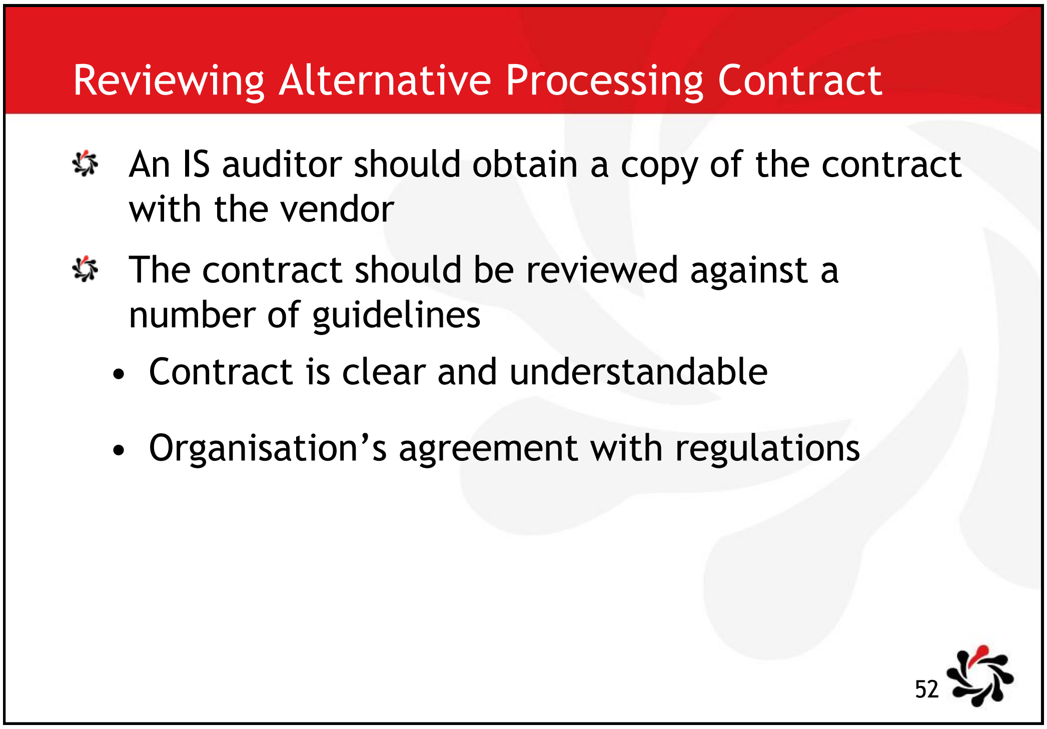
- Desk-based Evaluation/Paper Test (walkthrough)
- Preparedness Test (simulation)
- Full Operational Test
- Lessons learned from each test are used to improve the plan

50



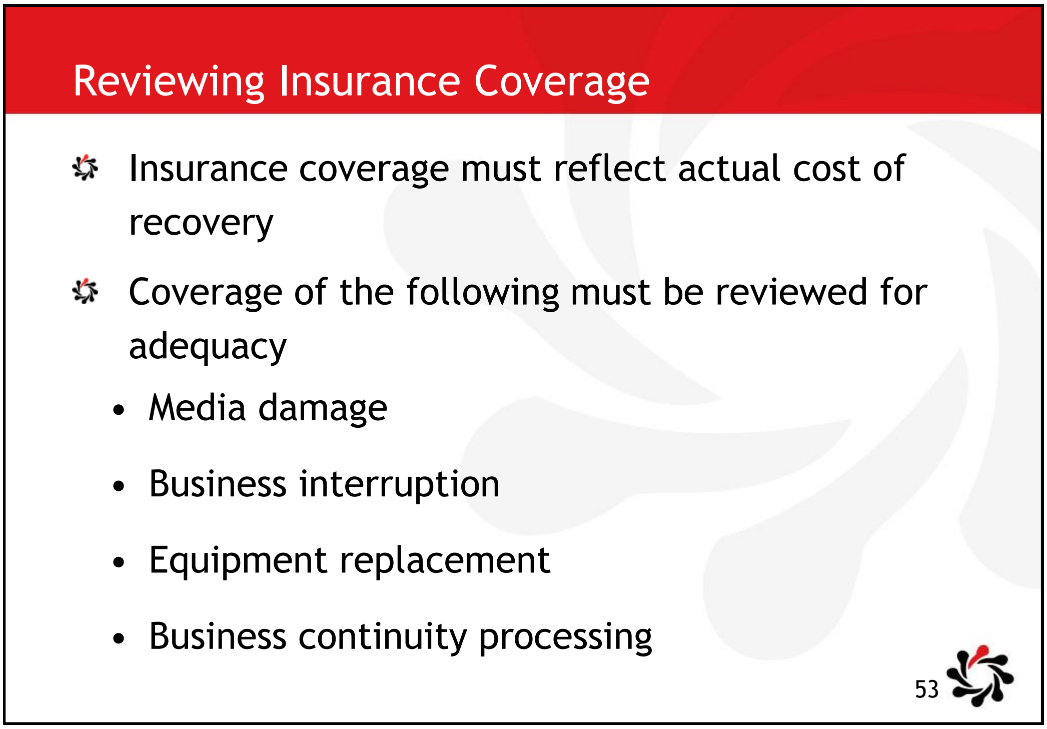
Plan Maintenance

- Plans must be maintained as they are quickly out of date
  - Changes in business
  - Lessons learned from tests and incidents
  - Changes in personnel
  - Changes in technology
- Reviewed at least annually



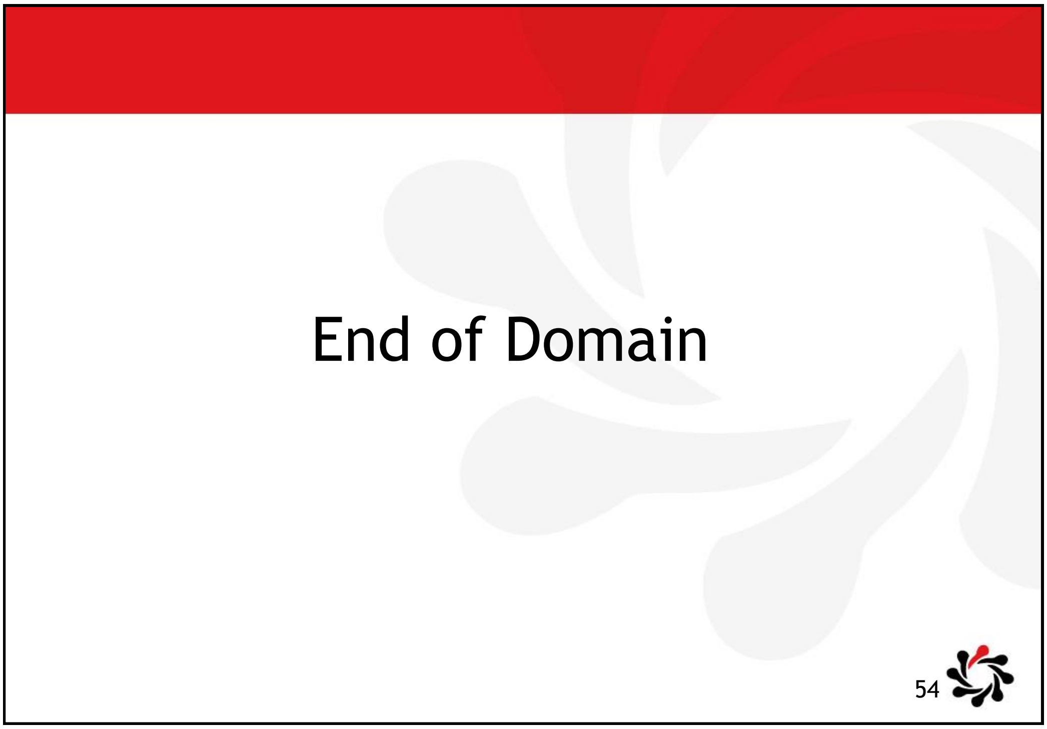
Reviewing Alternative Processing Contract

- 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

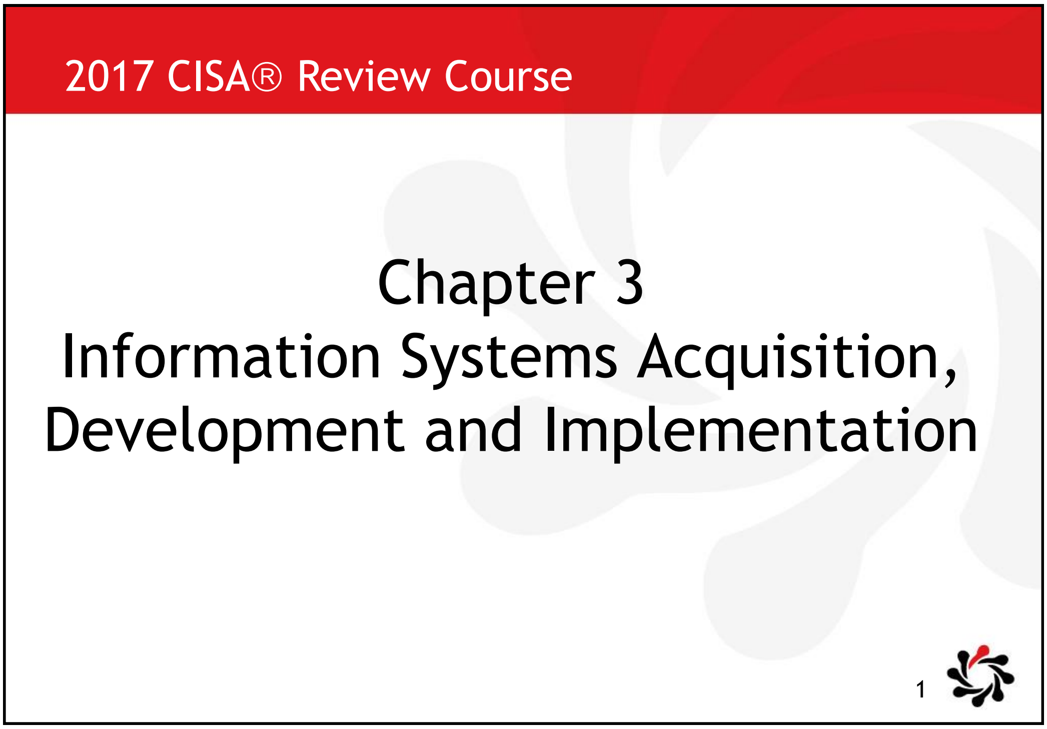


Reviewing Insurance Coverage

- 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

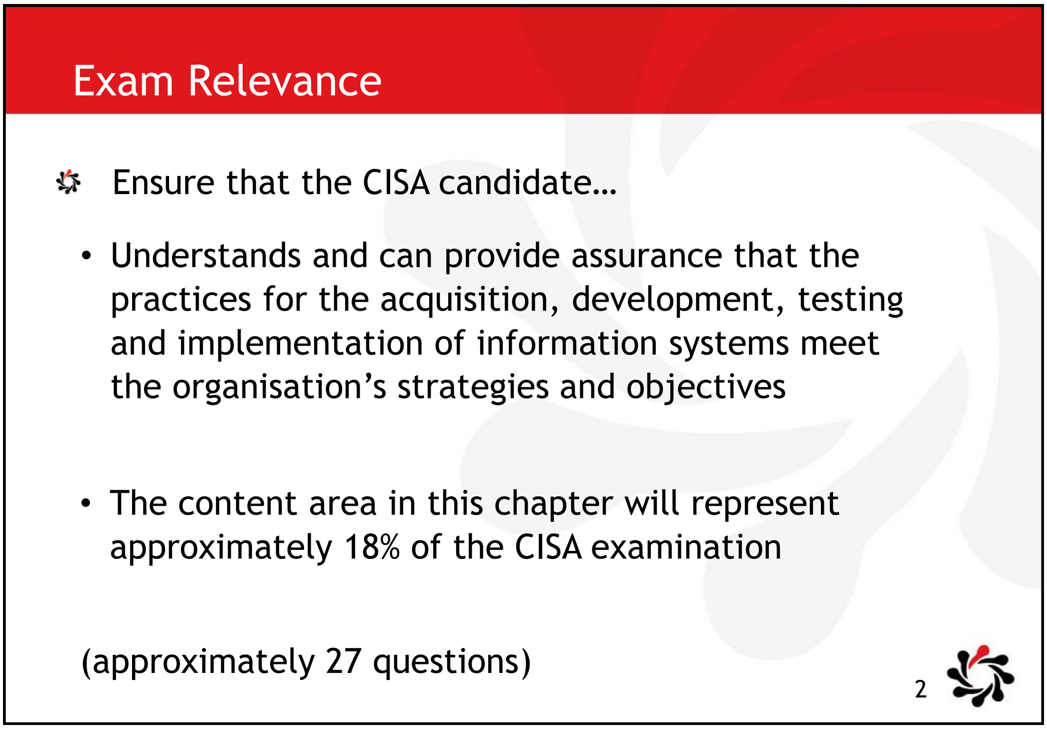


End of Domain



2017 CISA® Review Course

Chapter 3
Information Systems Acquisition, Development and Implementation



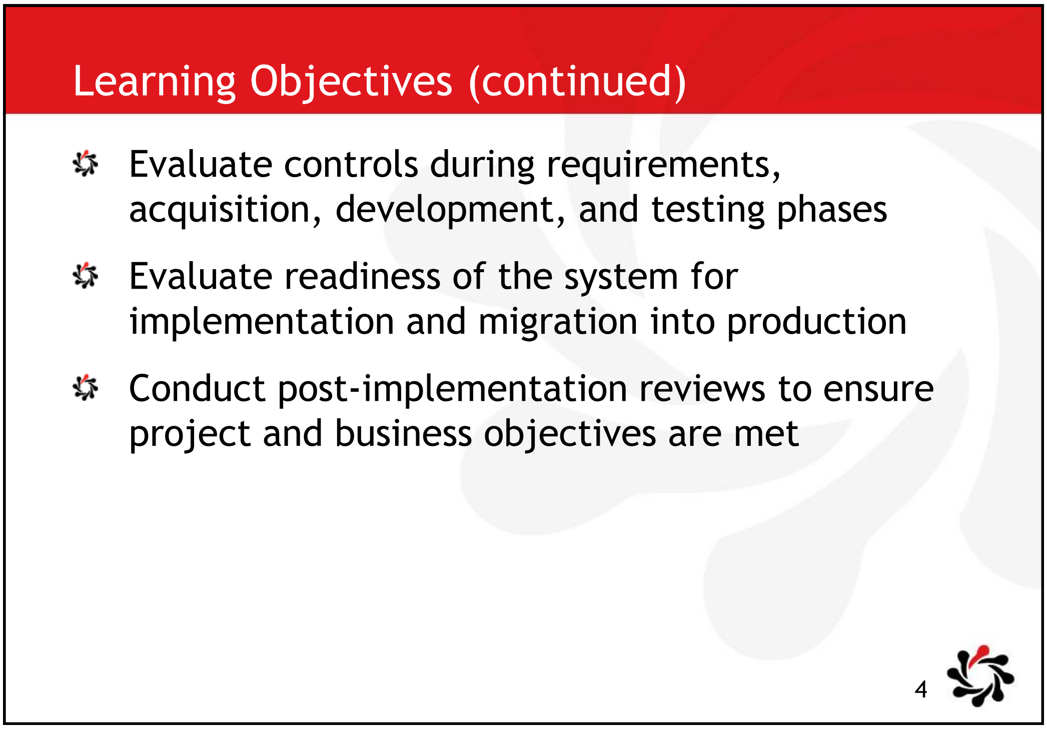
Exam Relevance

- 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 organisation's strategies and objectives
  - The content area in this chapter will represent approximately 18% of the CISA examination

(approximately 27 questions)

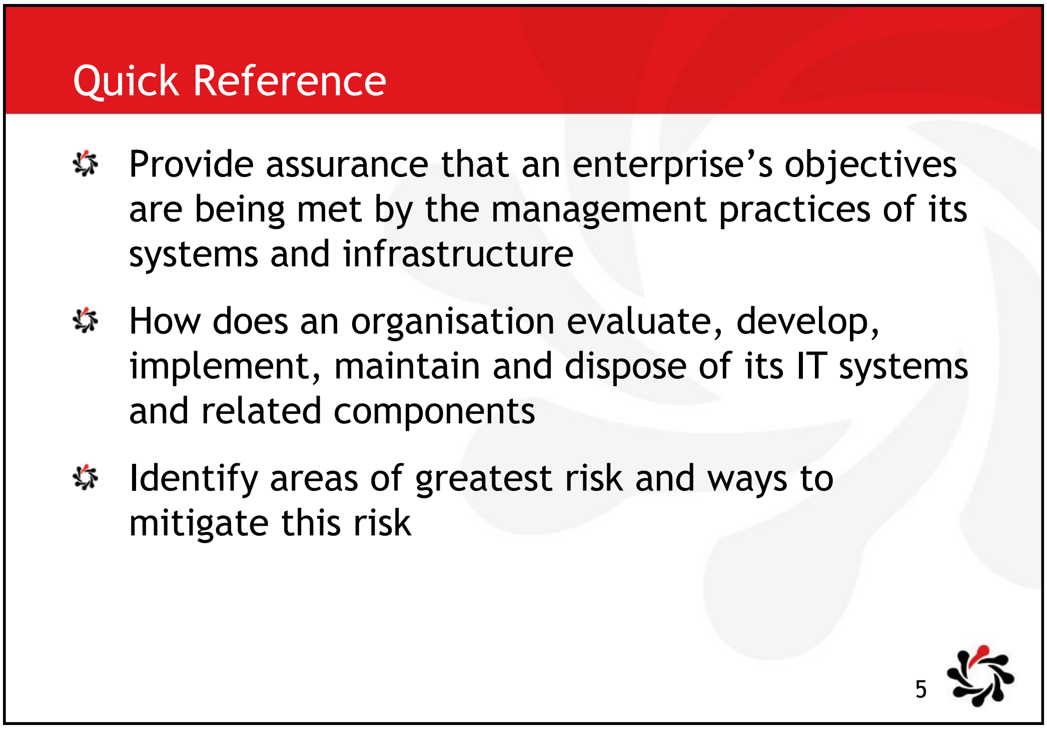
Learning Objectives

- Evaluate Business Case for IT investments
  - Meets business objectives
- Evaluate IT supplier selection and contract management
- Evaluate project management framework
  - Cost-effective, manage risk
- Conduct project reviews
  - Documentation, timely and accurate status



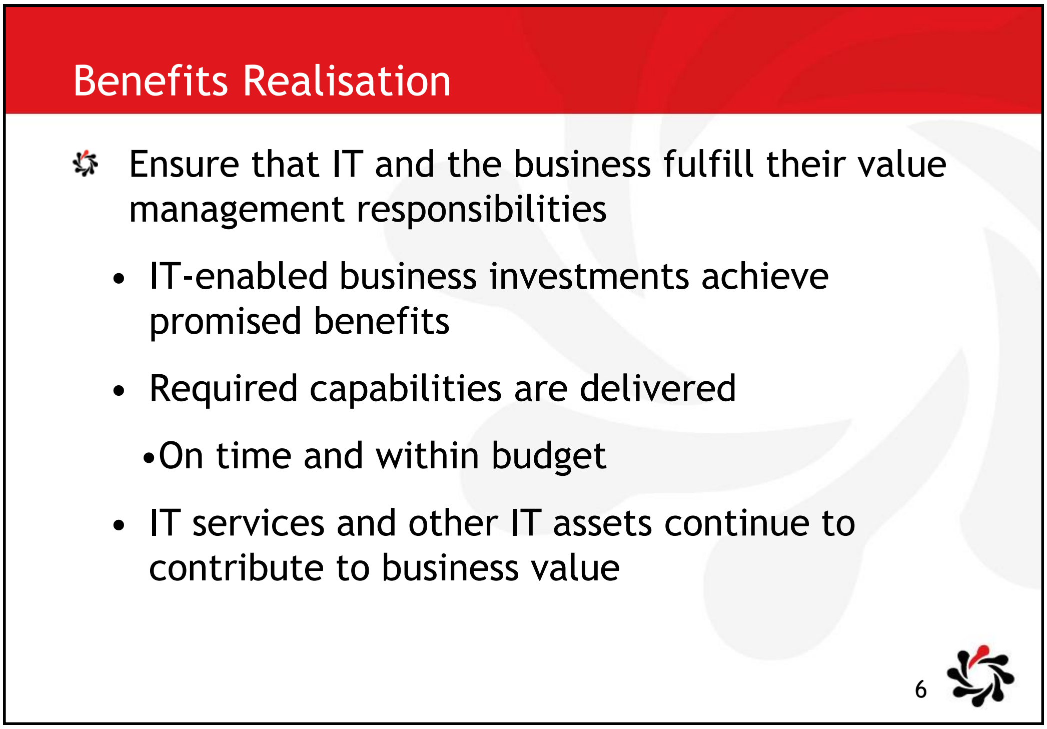
Learning Objectives (continued)

- Evaluate controls 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



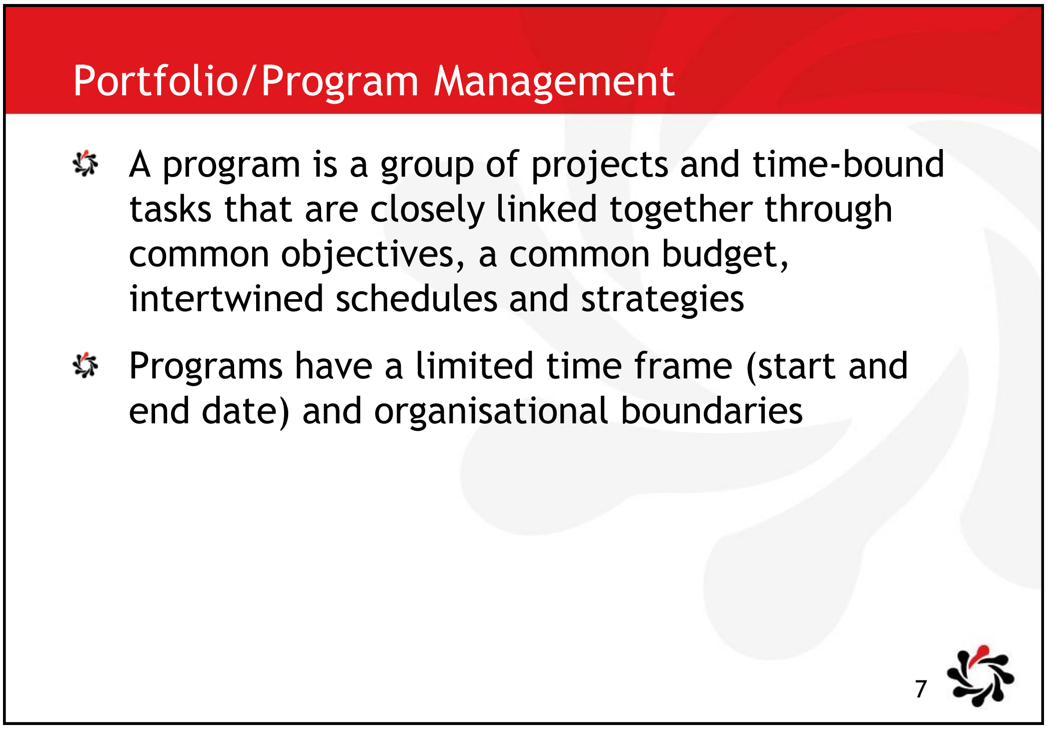
Quick Reference

- Provide assurance that an enterprise’s objectives are being met by the management practices of its systems and infrastructure
- How does an organisation evaluate, develop, implement, maintain and dispose of its IT systems and related components
- Identify areas of greatest risk and ways to mitigate this risk



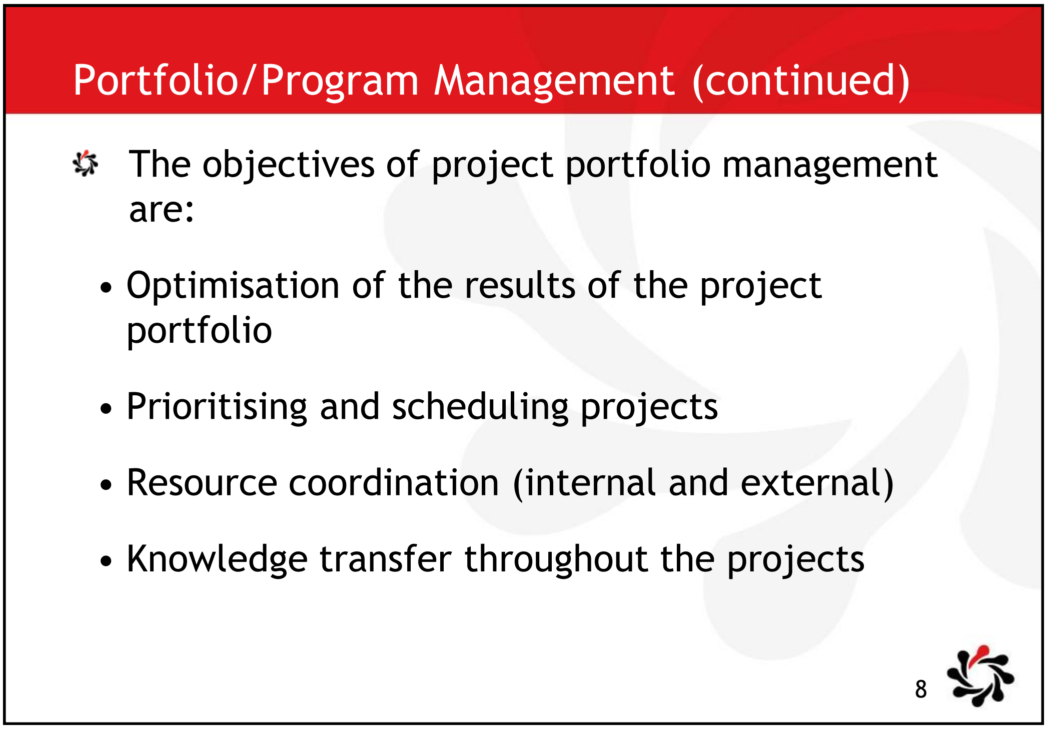
Benefits Realisation

- Ensure that IT and the business fulfill their value management responsibilities
  - IT-enabled business investments achieve promised benefits
  - Required capabilities are delivered
    - On time and within budget
  - IT services and other IT assets continue to contribute to business value



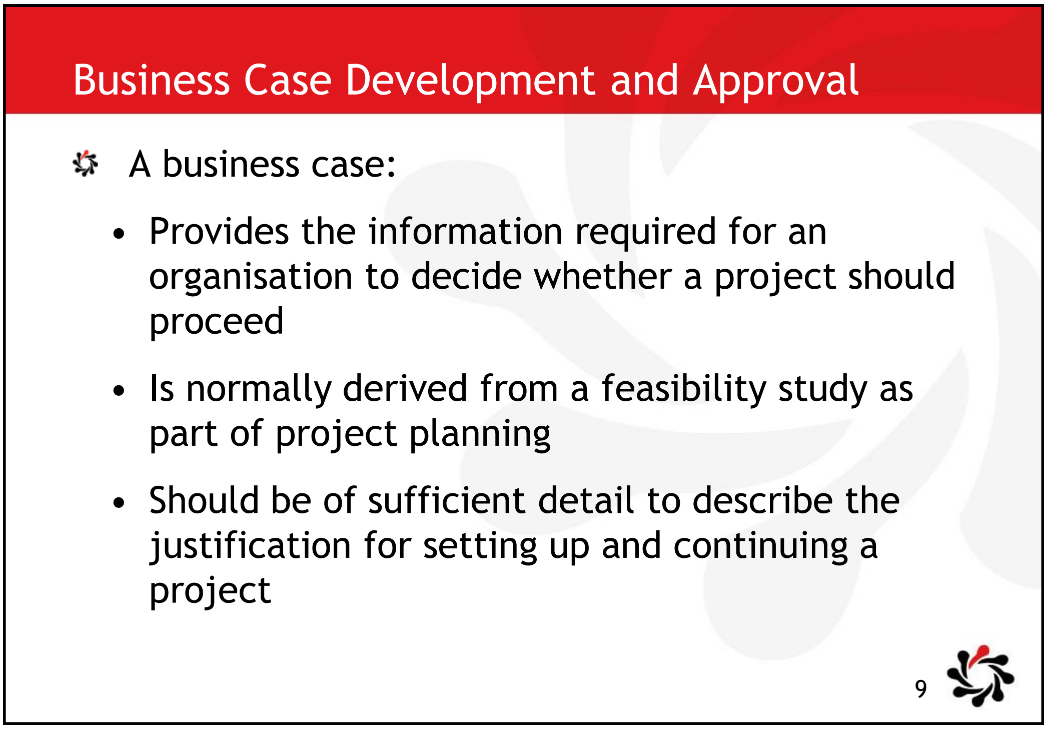
Portfolio/Program Management

- 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



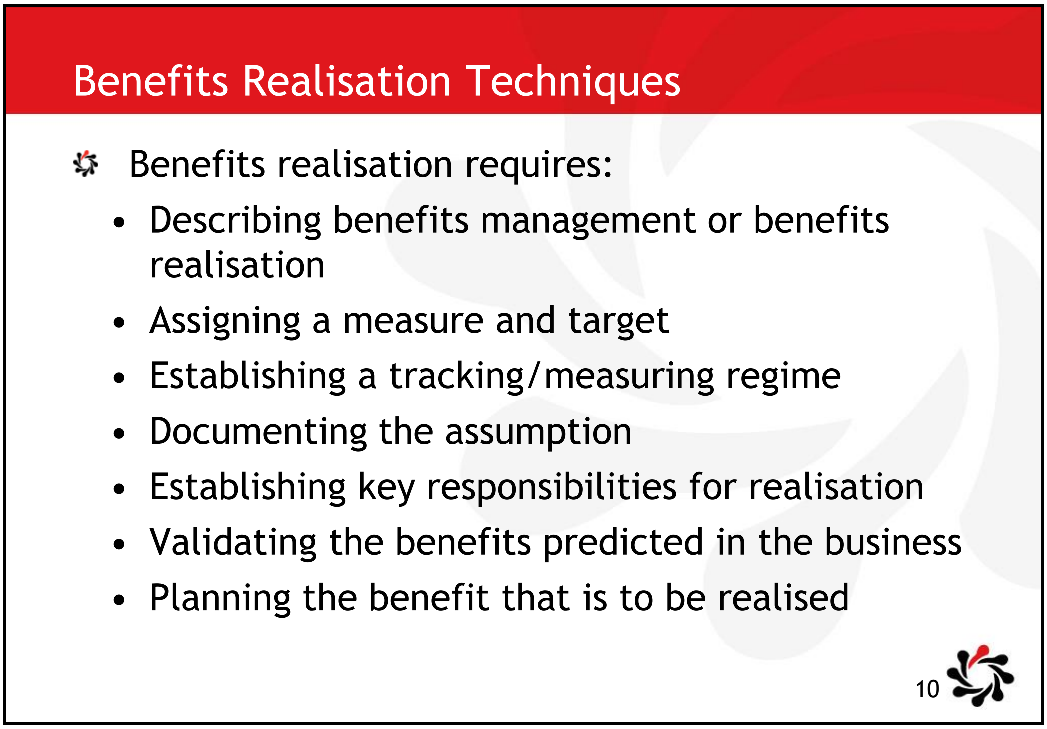
Portfolio/Program Management (continued)

- 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



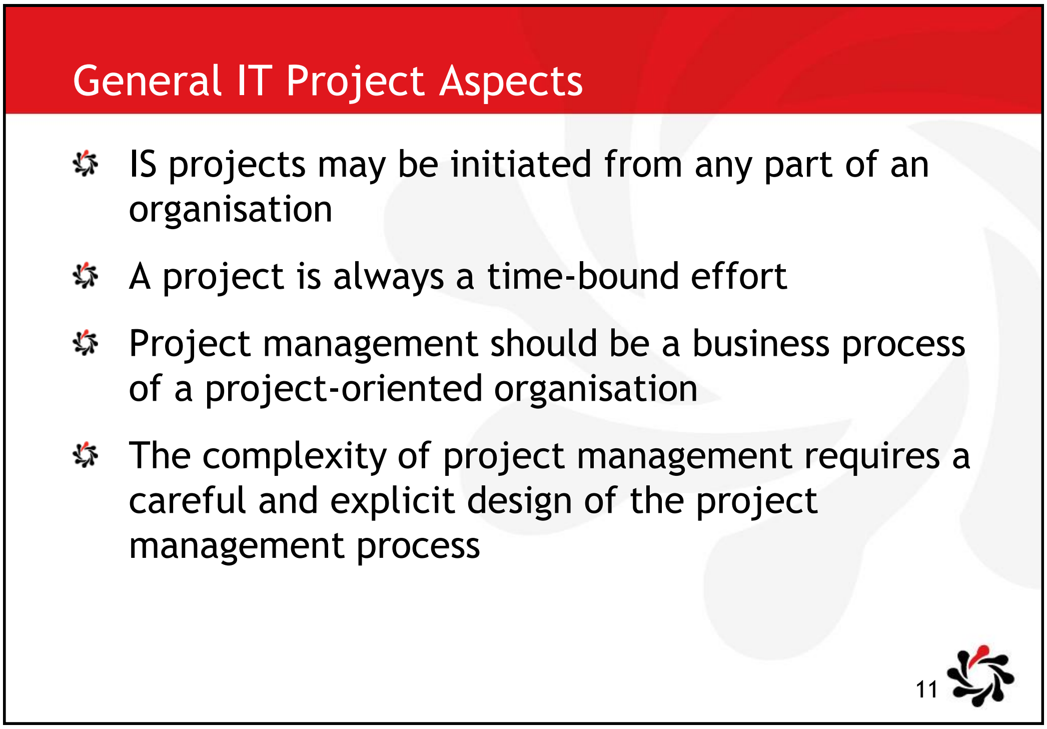
Business Case Development and Approval

- 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

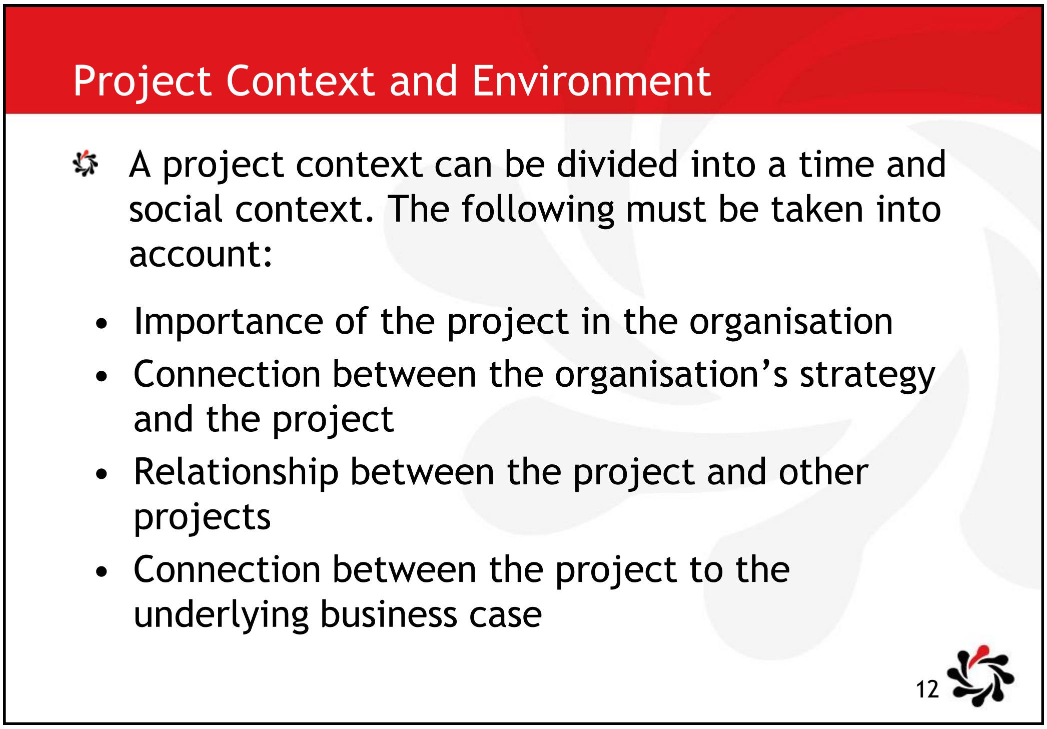
- Benefits realisation requires:
  - Describing benefits management or benefits realisation
  - Assigning a measure and target
  - Establishing a tracking/measuring regime
  - Documenting the assumption
  - Establishing key responsibilities for realisation
  - Validating the benefits predicted in the 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

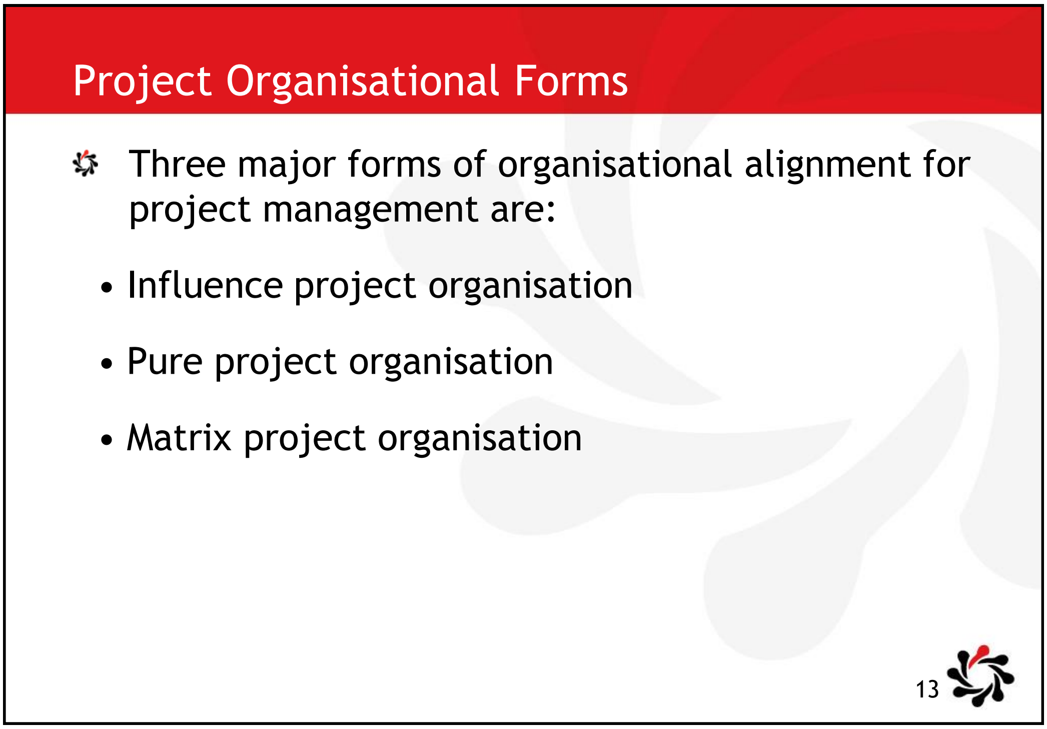
11



Project Context and Environment

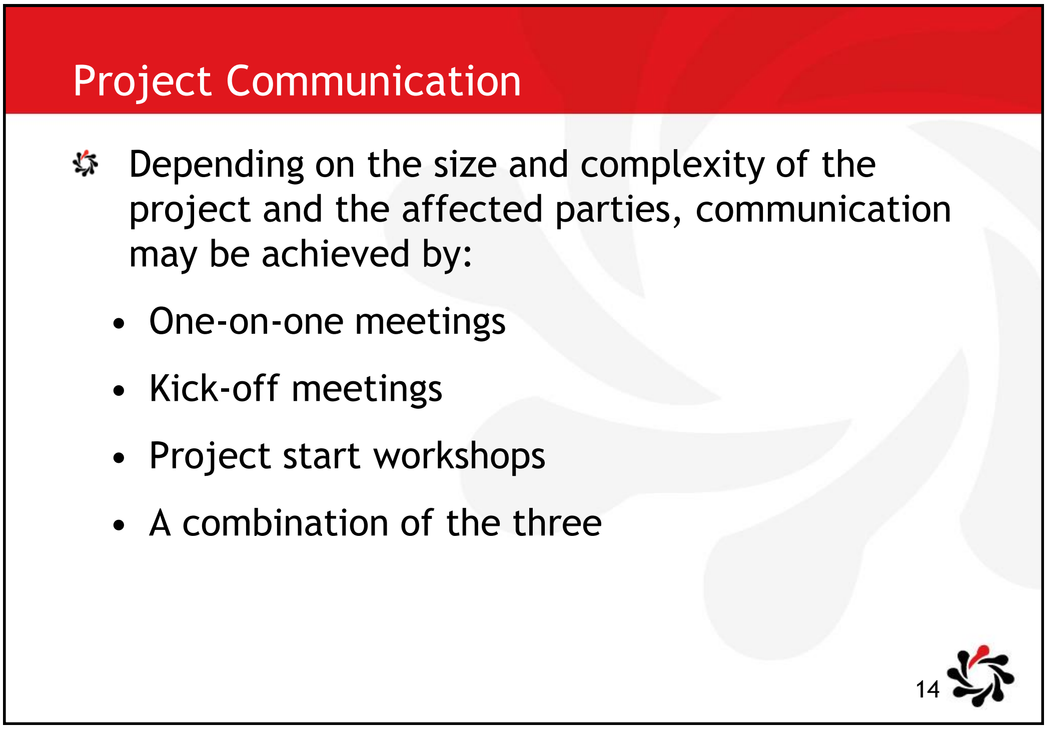
- A project context can be divided into a time and social context. The following must be taken into account:
  - Importance of the project in the organisation
  - Connection between the organisation’s strategy and the project
  - Relationship between the project and other projects
  - Connection between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

12



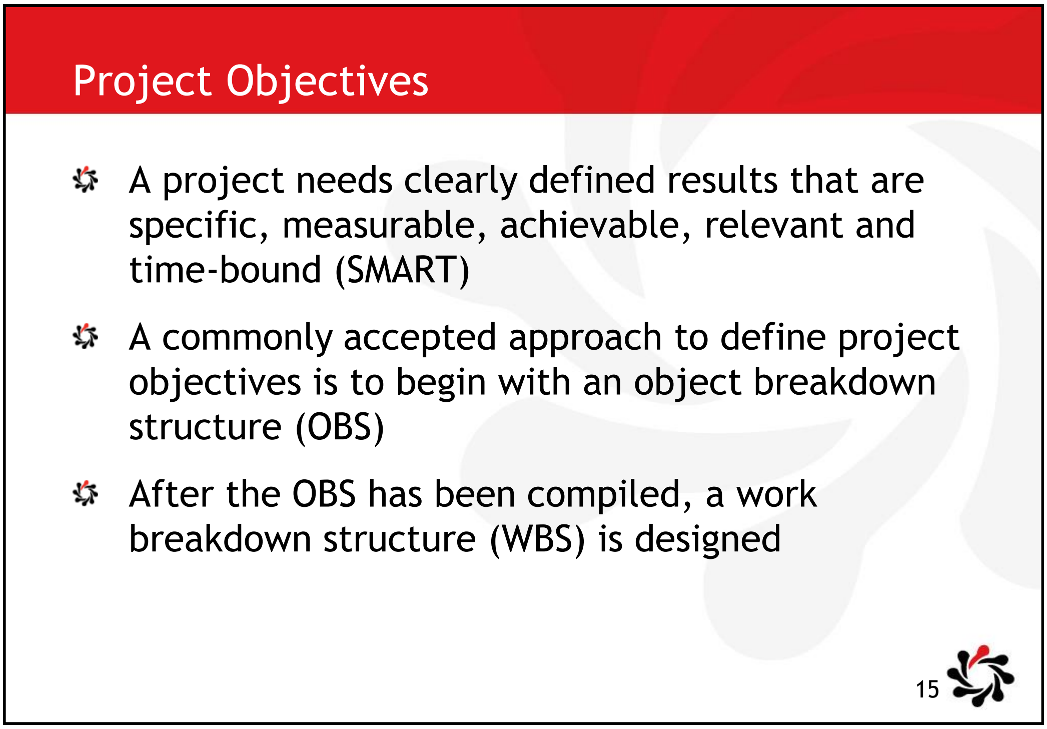
Project Organisational Forms

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



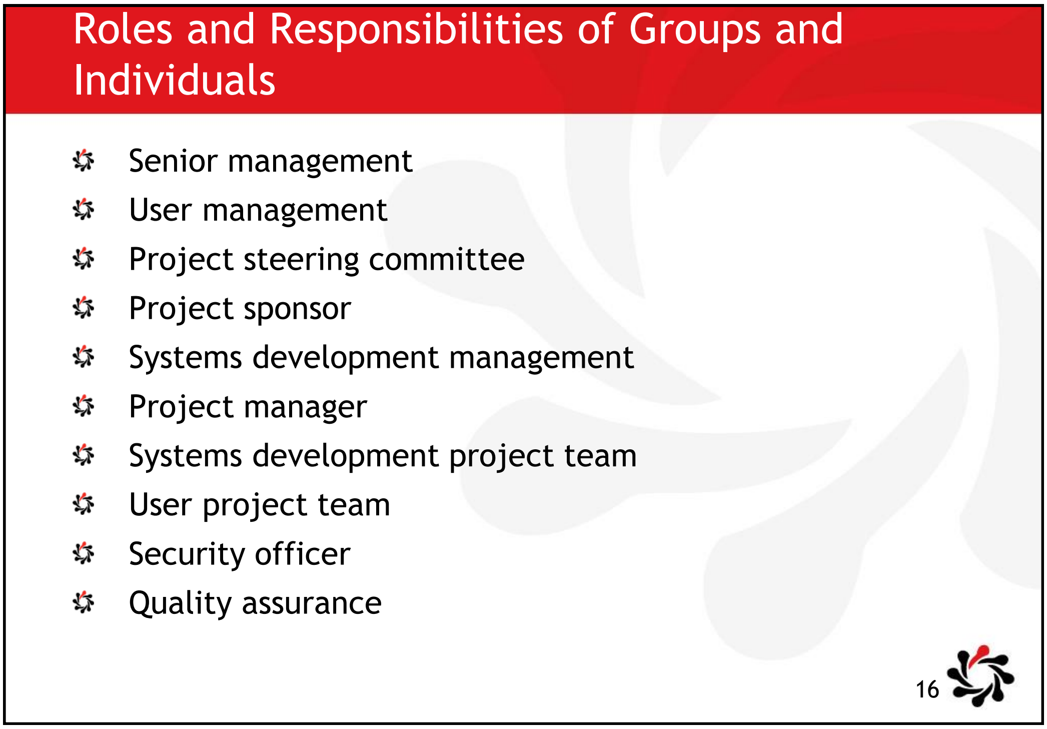
Project Communication

- 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



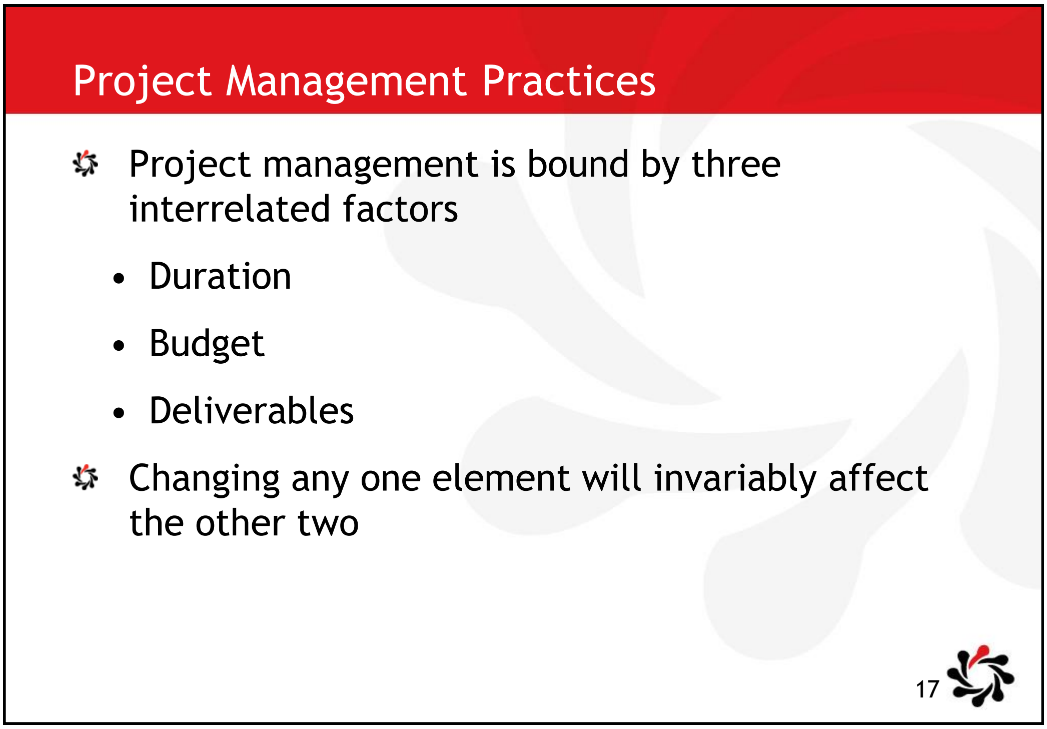
Project Objectives

- 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



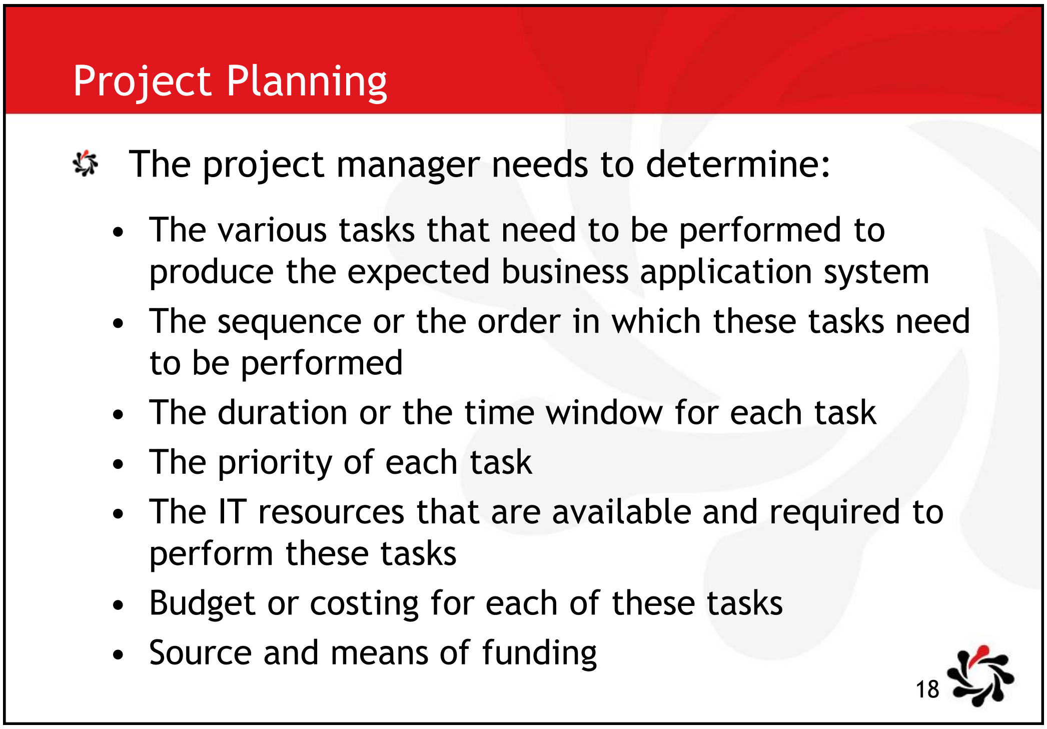
Roles and Responsibilities of Groups and Individuals

- 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



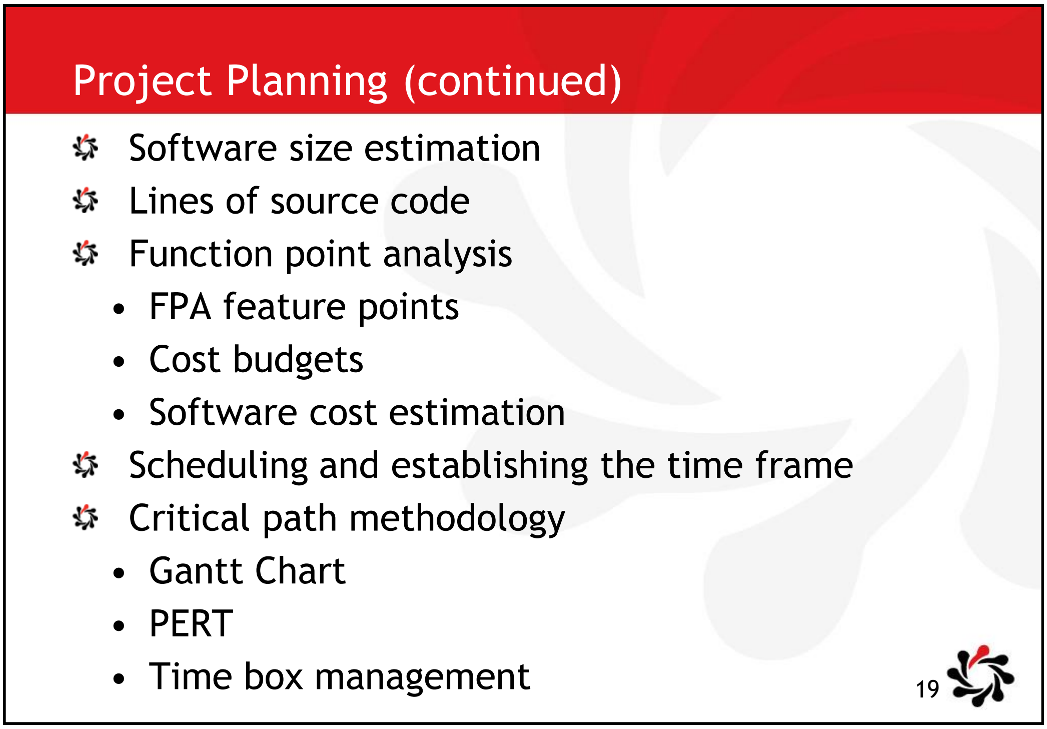
Project Management Practices

- Project management is bound by three interrelated factors
  - Duration
  - Budget
  - Deliverables
- Changing any one element will invariably affect the other two



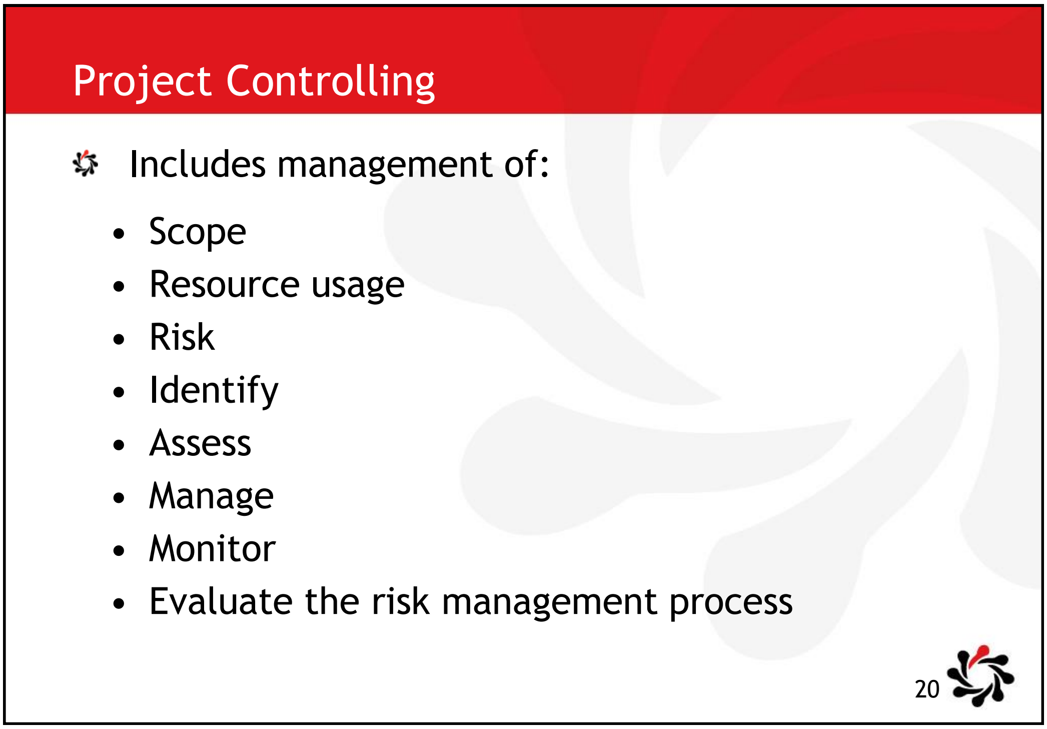
Project Planning

- 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



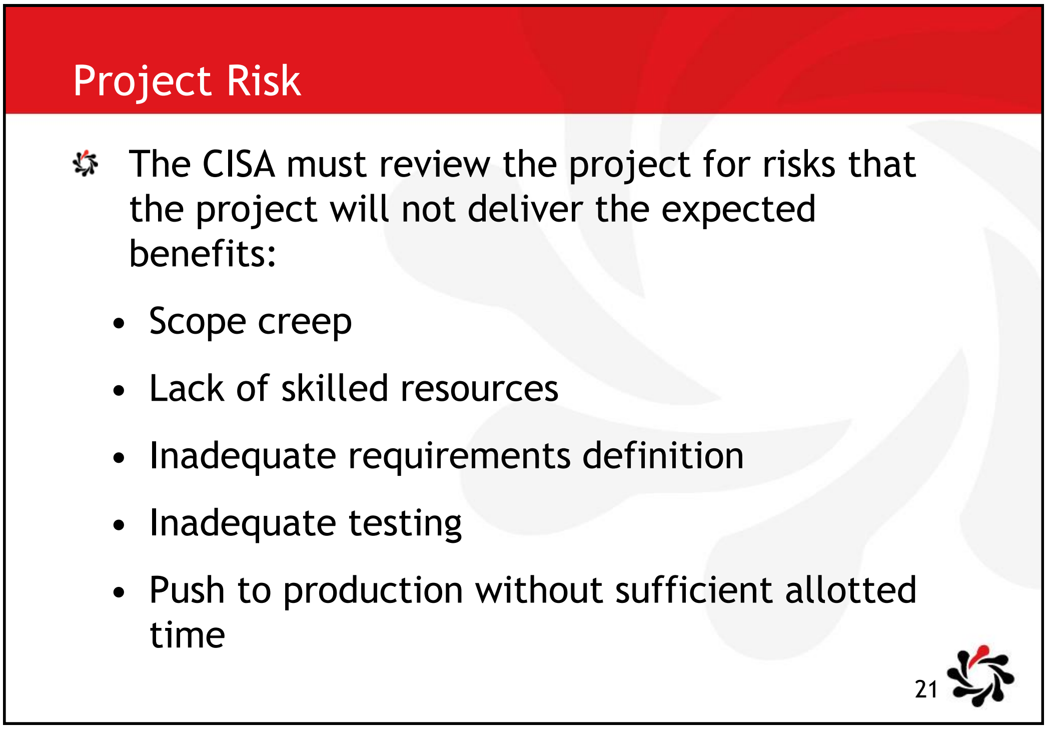
Project Planning (continued)

- 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



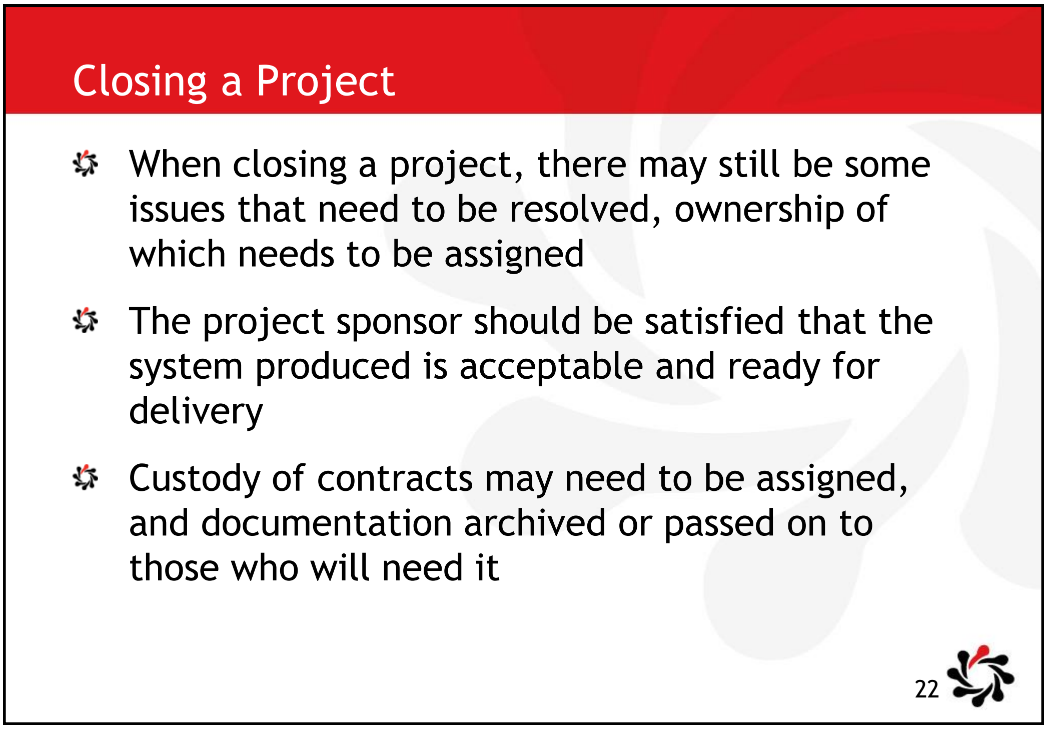
Project Controlling

- Includes management of:
  - Scope
  - Resource usage
  - Risk
  - Identify
  - Assess
  - Manage
  - Monitor
  - Evaluate the risk management process



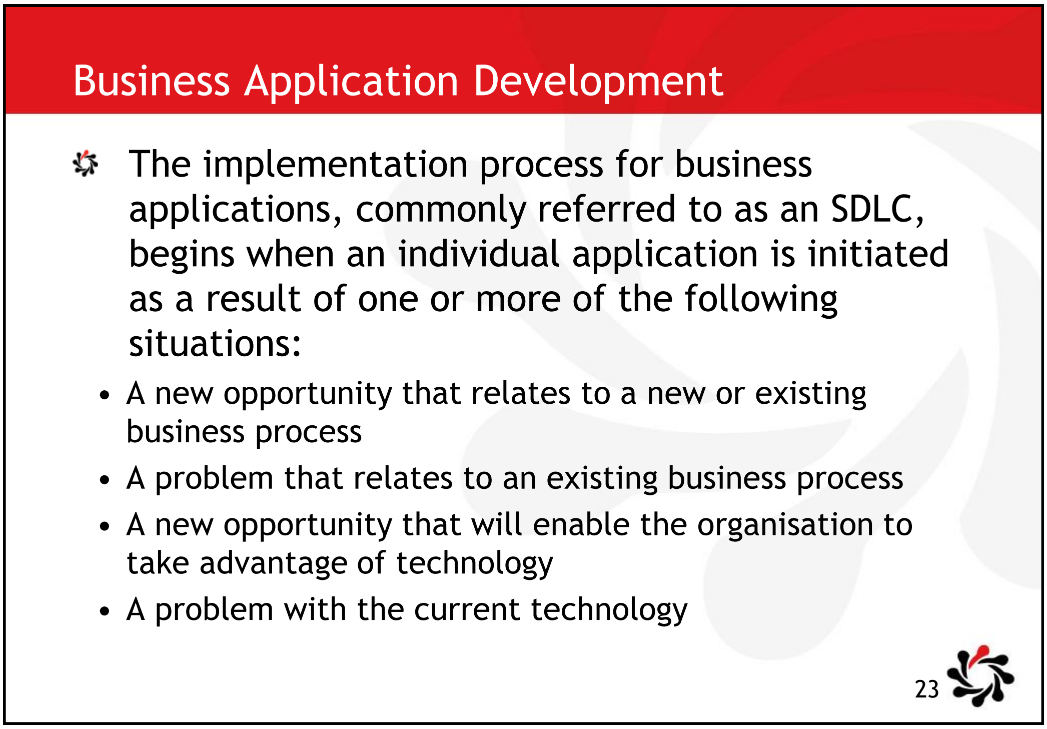
Project Risk

- 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



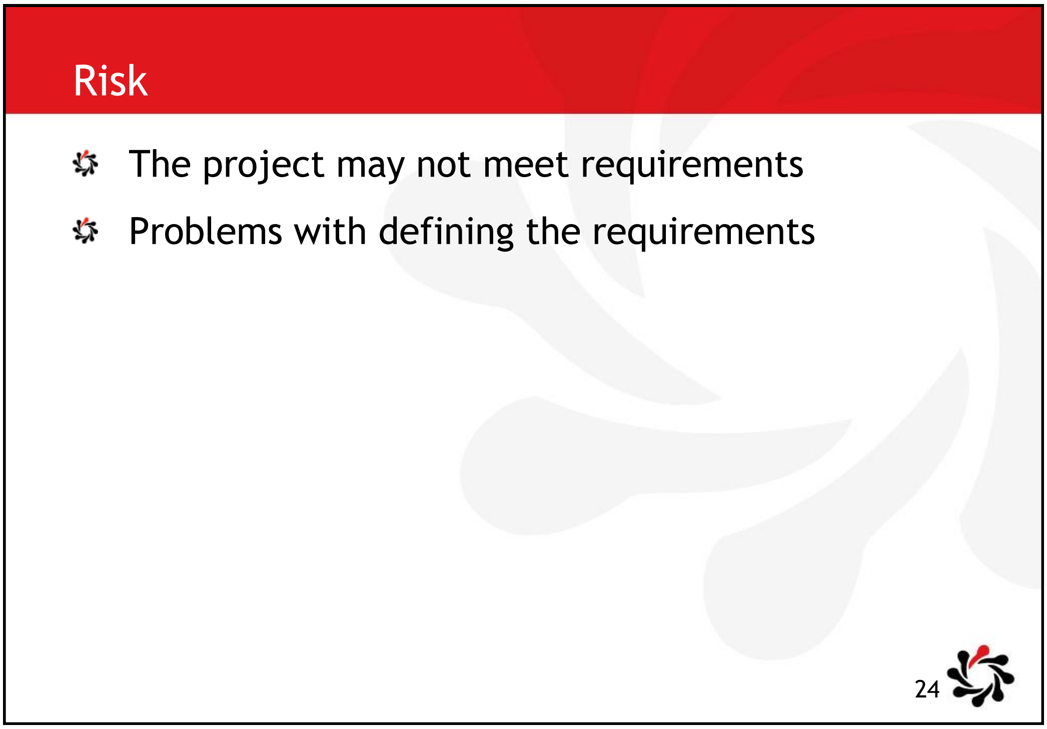
Closing a Project

- 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



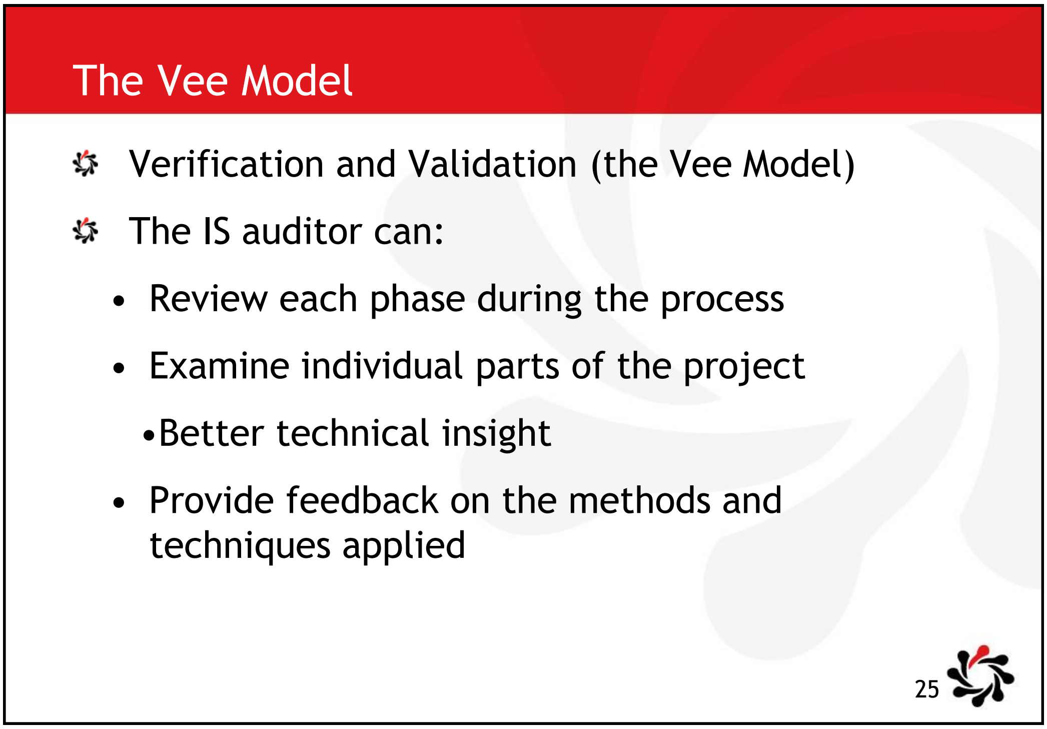
Business Application Development

- 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



Risk

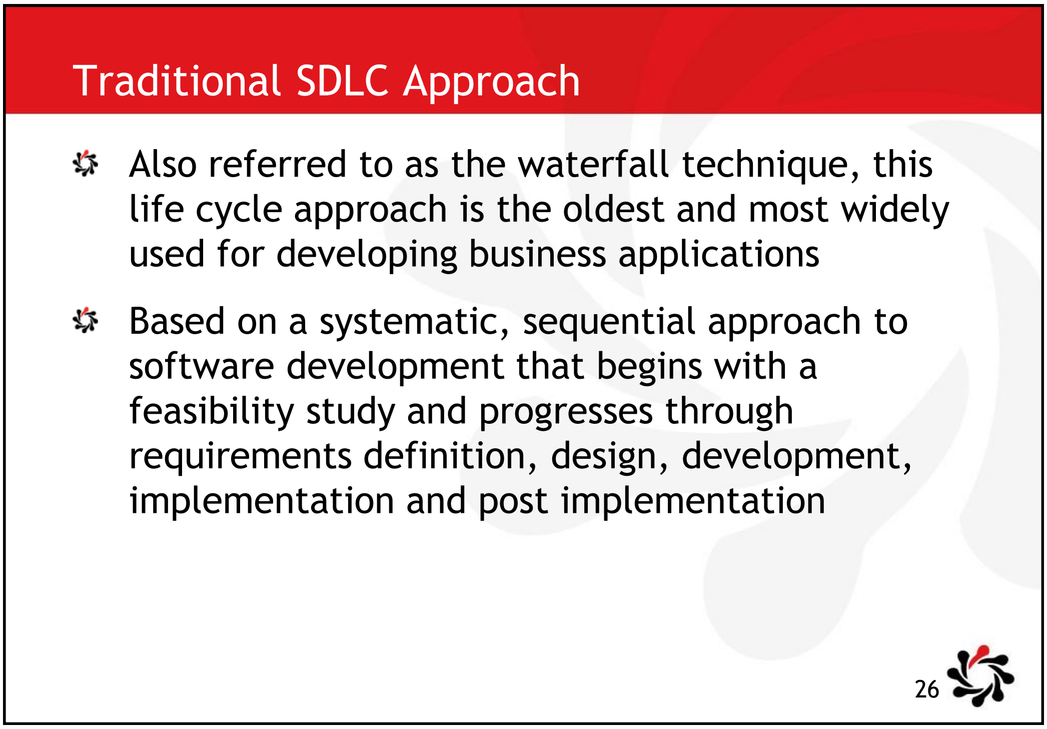
- The project may not meet requirements
- Problems with defining the requirements



The Vee Model

- Verification and Validation (the Vee Model)
- The IS auditor can:
  - Review each phase during the process
  - Examine individual parts of the project
    - Better technical insight
  - Provide feedback on the methods and techniques applied

25



Traditional SDLC Approach

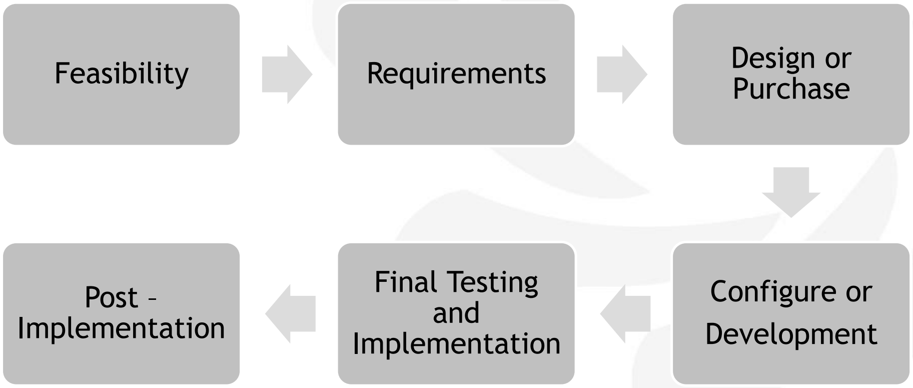
- Also referred to as the waterfall technique, this life cycle approach is the oldest and most widely used for developing business applications
- Based on a systematic, sequential approach to software development that begins with a feasibility study and progresses through requirements definition, design,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

26

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

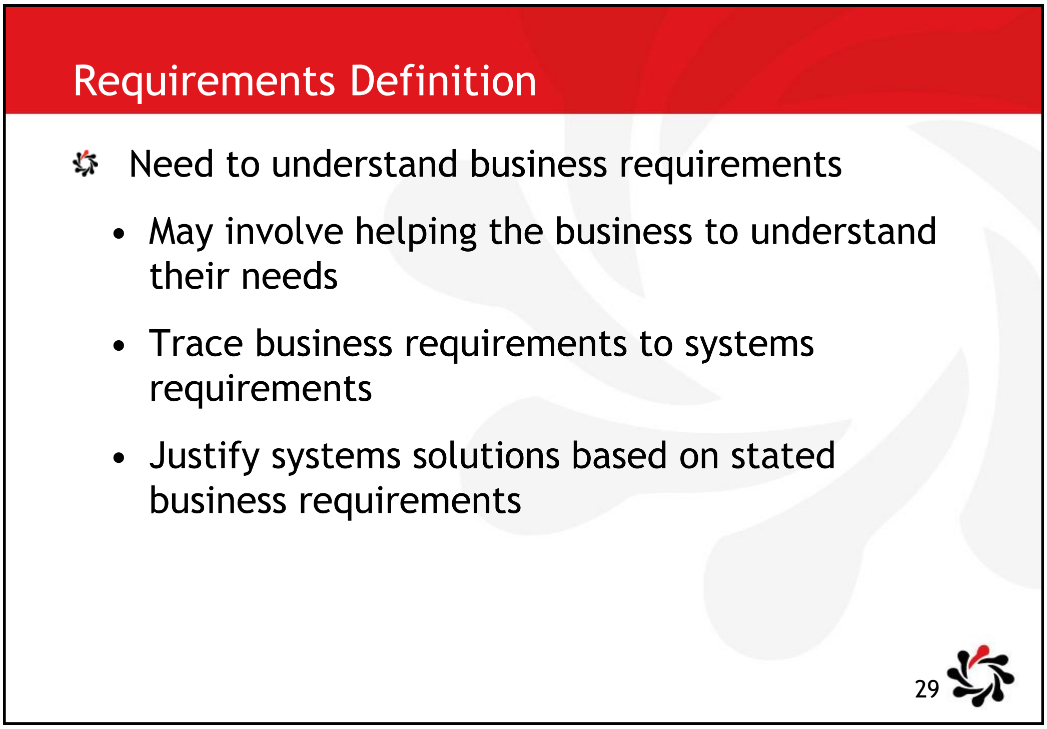
Requirements

Design or Purchase

Configure or Development

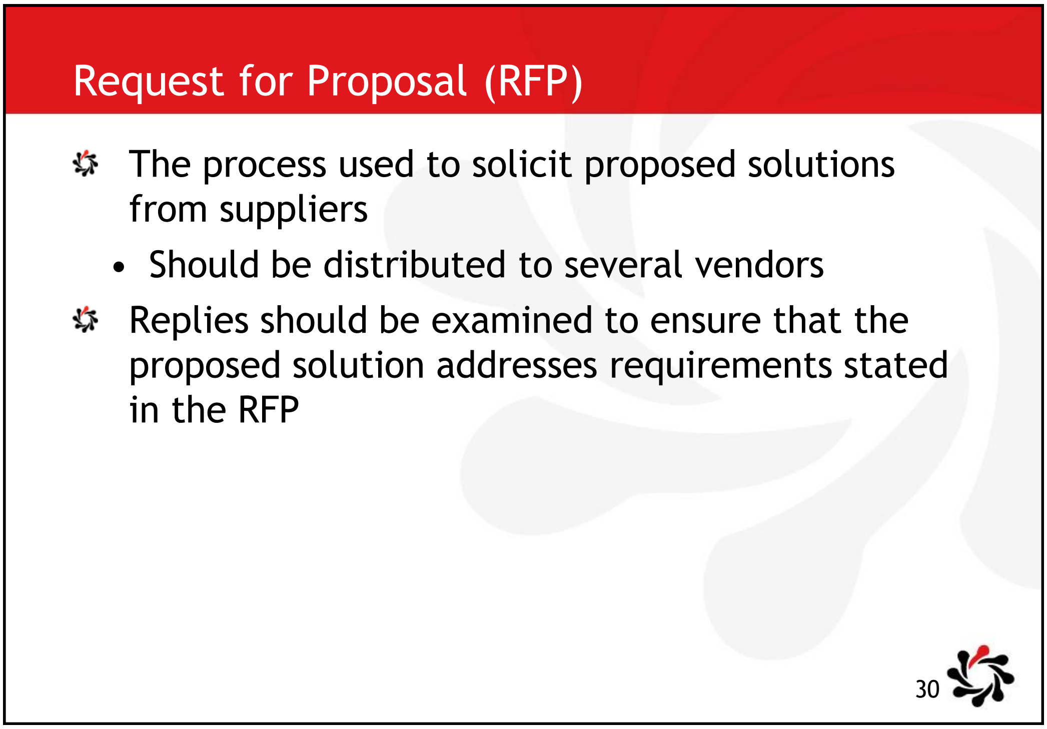
Final Testing and Implementation

Post - Implementation



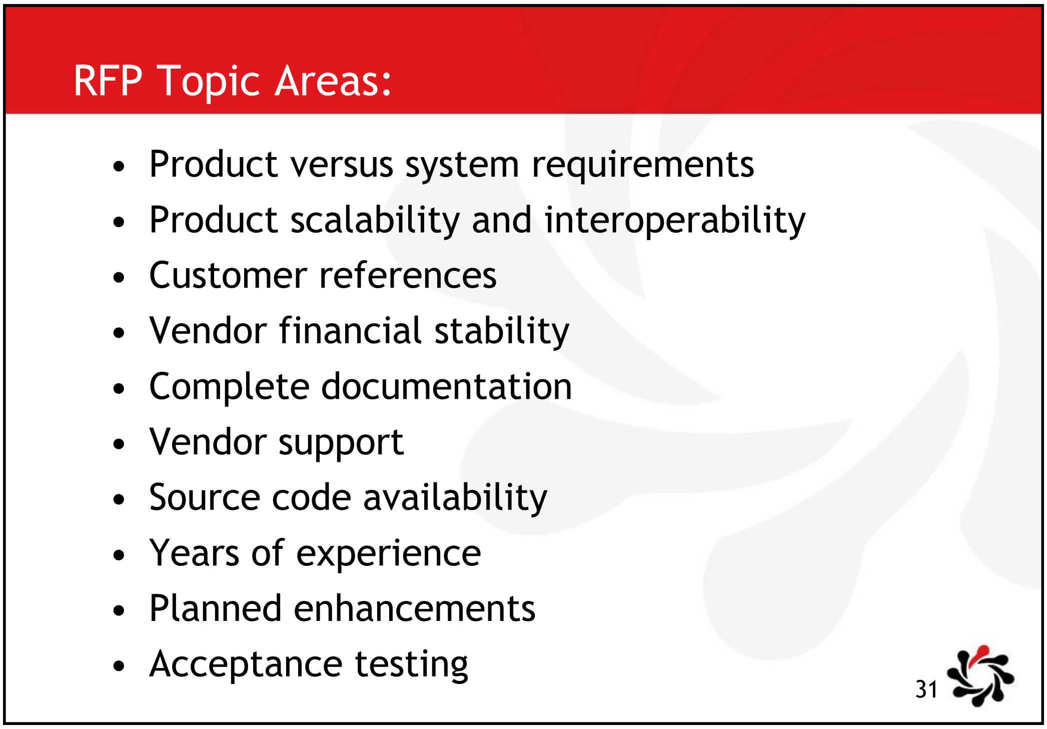
Requirements Definition

- 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



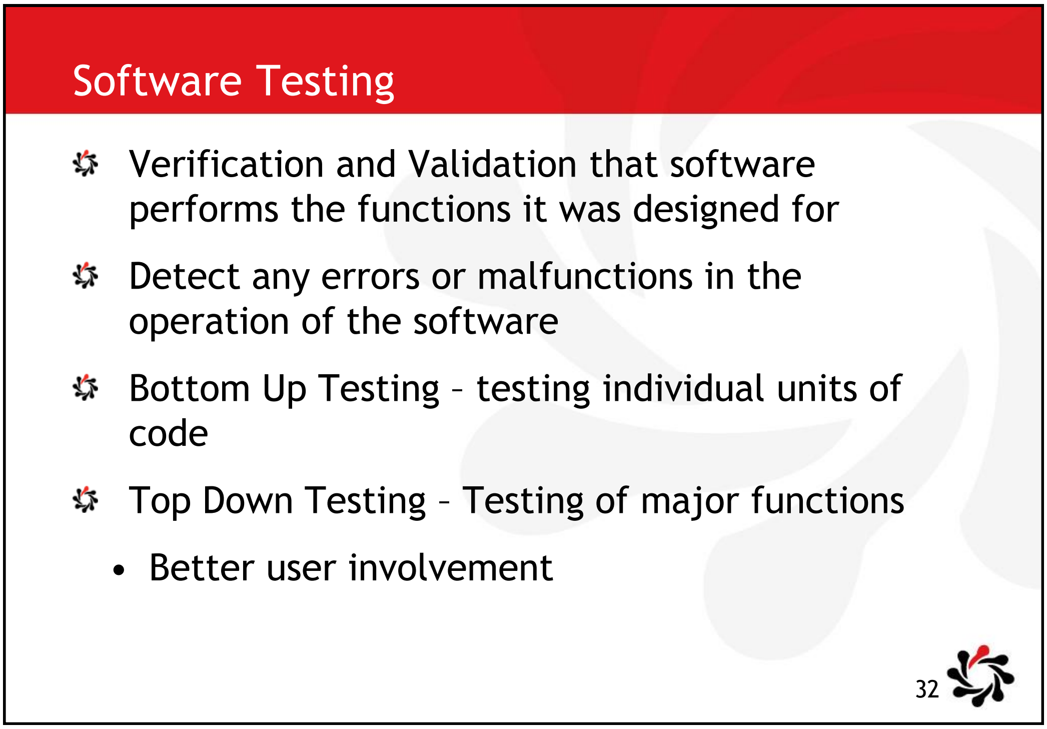
Request for Proposal (RFP)

- The process used to solicit proposed solutions from suppliers
  - Should be distributed to several vendors
- Replies should be examined to ensure that the proposed solution addresses requirements stated in the RFP



RFP Topic Areas:

- Product versus system requirements
- Product scalability and interoperability
- Customer references
- Vendor financial stability
- Complete documentation
- Vendor support
- Source code availability
- Years of experience
- Planned enhancements
- Acceptance testing



Software Testing

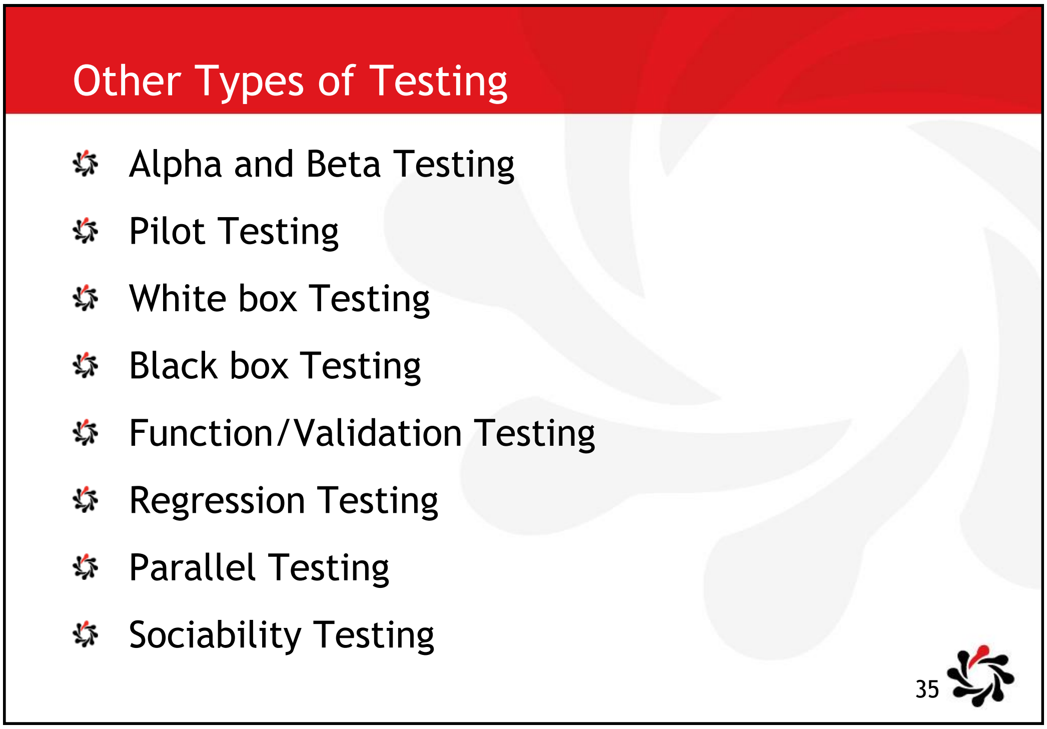
- Verification and Validation that software performs the functions it was designed for
- Detect any errors or malfunctions in the operation of the software
- Bottom Up Testing – testing individual units of code
- Top Down Testing – Testing of major functions
  - Better user involvement

Types of Tests

- Unit Testing
- Interface or Integration Testing
- System Testing
- Final Acceptance Testing (User Acceptance Testing)
  - Quality assurance
    - Documentation
    - Coding Standards

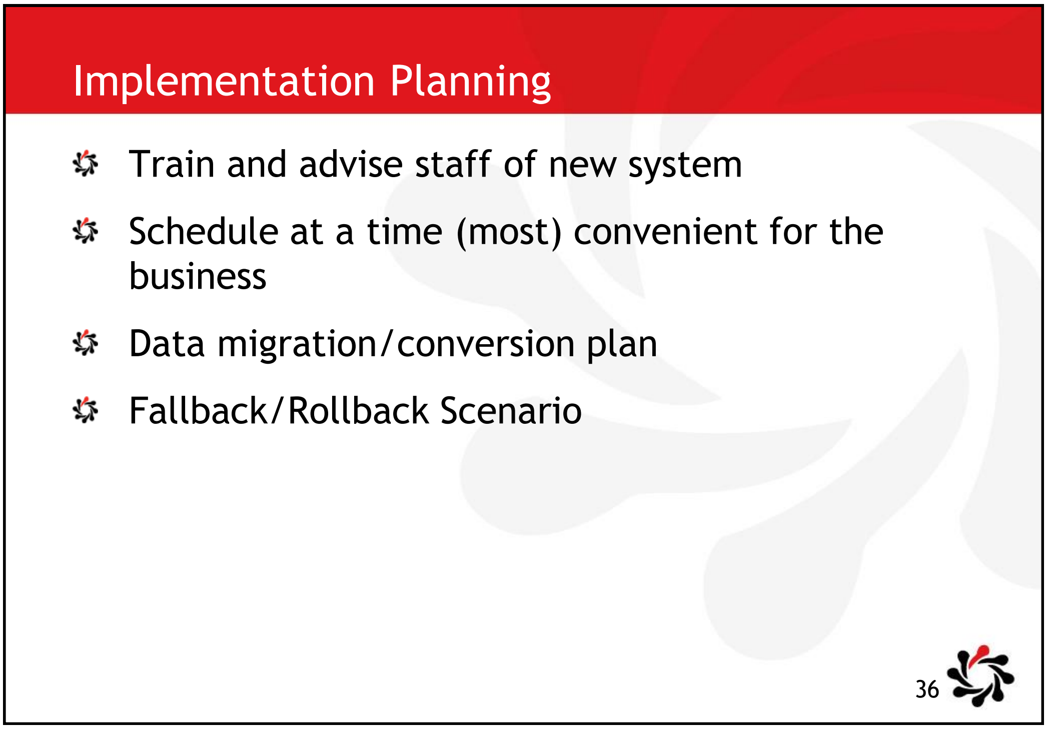
Testing (continued)

- Testing should first be done in a secure area separate from production
- Integrated Test Facilities (ITF) tests the system under production-like conditions.
  - Load Tests
  - May use (sanitised) production data



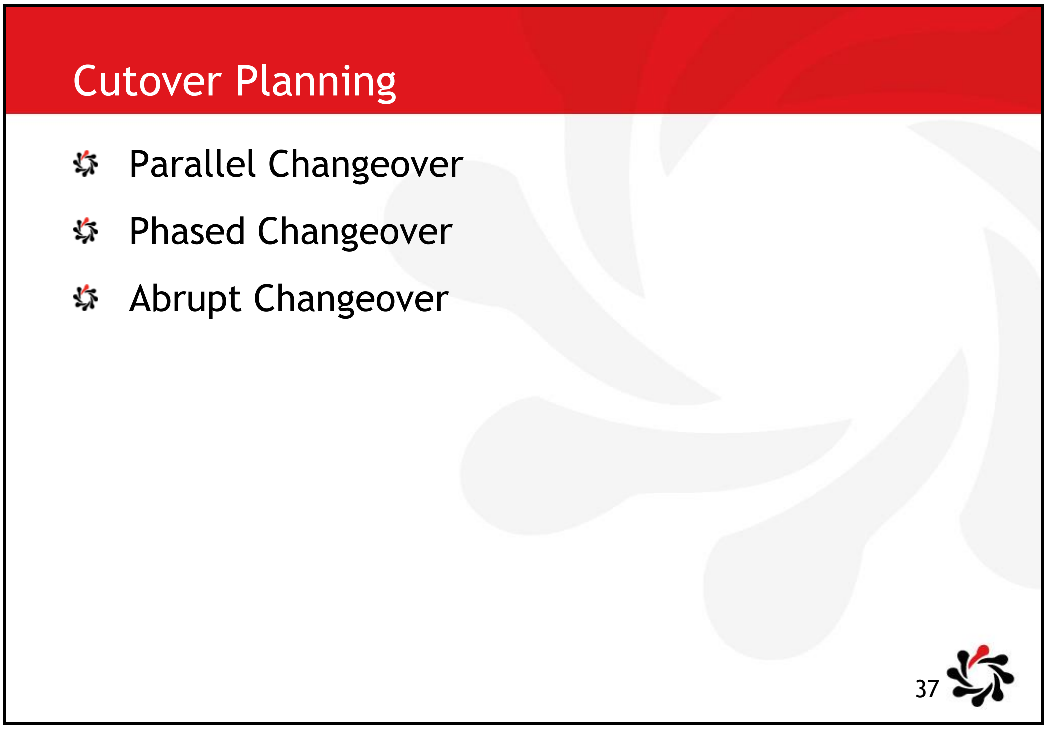
Other Types of Testing

- Alpha and Beta Testing
- Pilot Testing
- White box Testing
- Black box Testing
- Function/Validation Testing
- Regression Testing
- Parallel Testing
- Sociability Testing



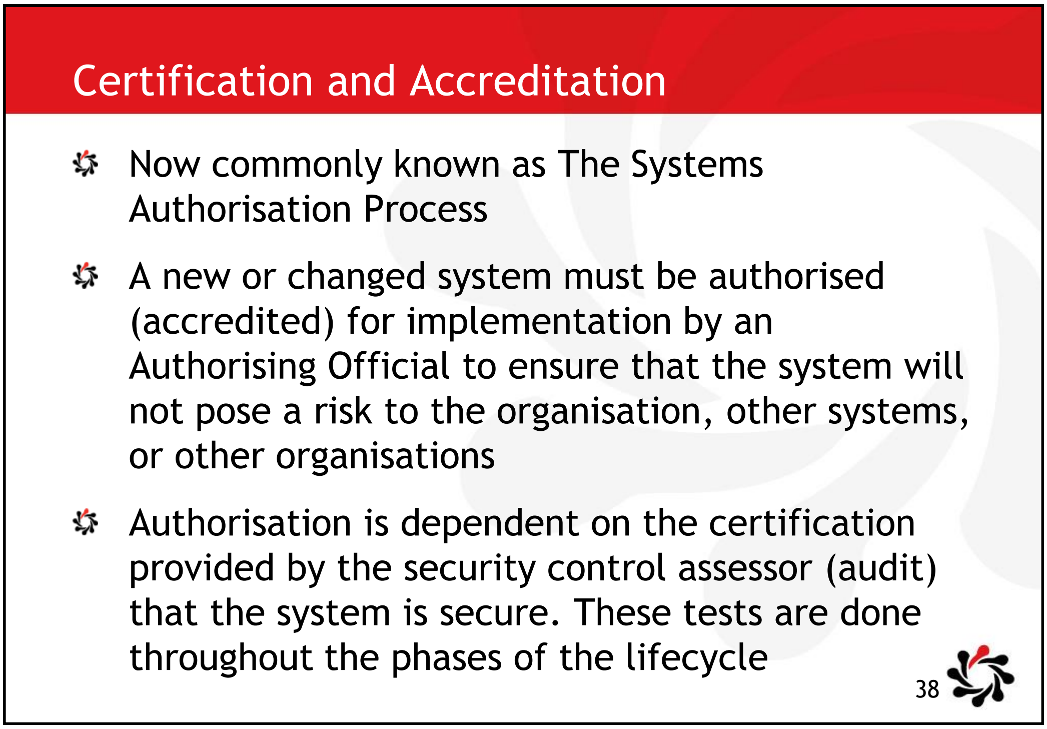
Implementation Planning

- Train and advise staff of new system
- Schedule at a time (most) convenient for the business
- Data migration/conversion plan
- Fallback/Rollback Scenario



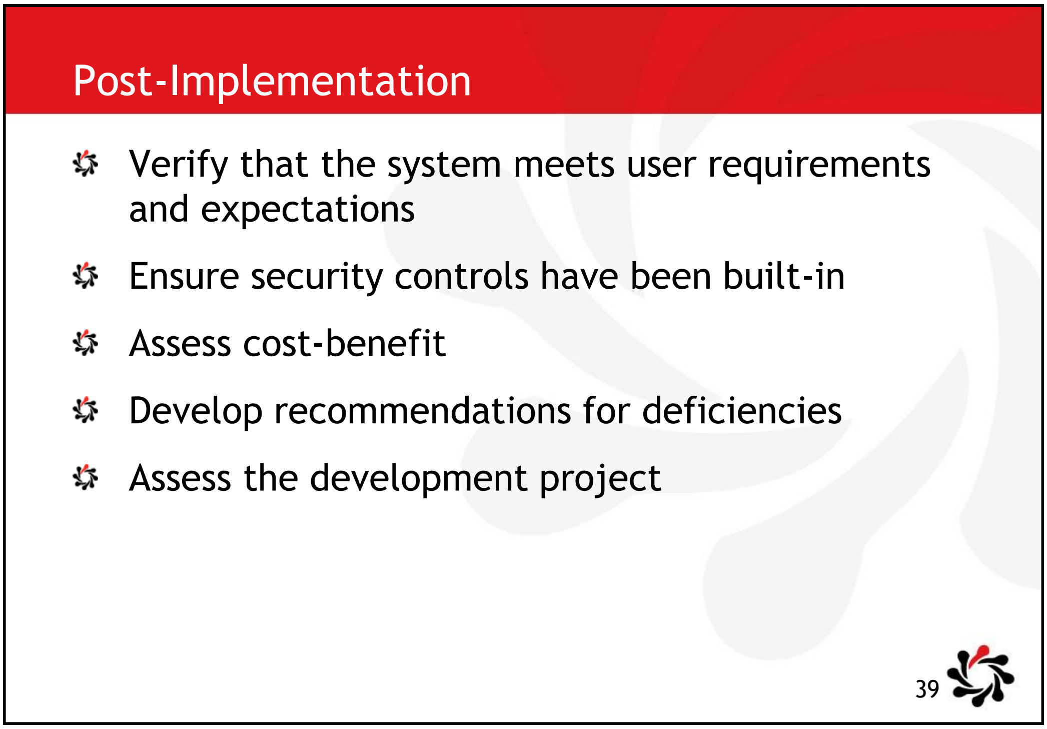
Cutover Planning

- Parallel Changeover
- Phased Changeover
- Abrupt Changeover



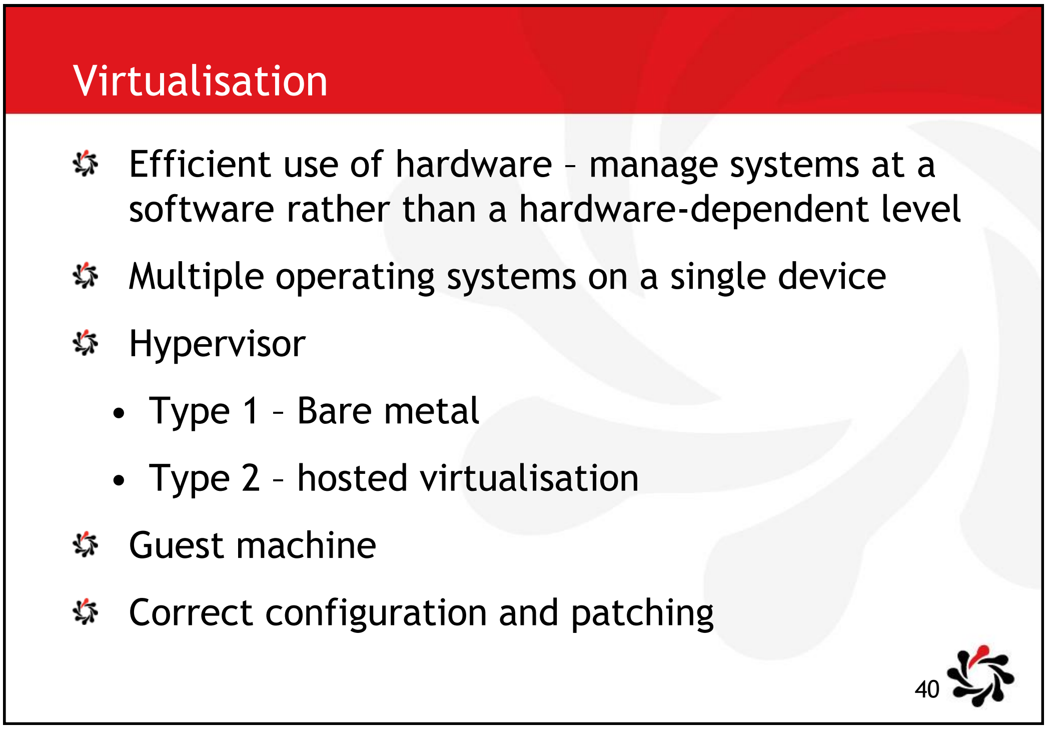
Certification and Accreditation

- Now commonly known as The Systems Authorisation Process
- A new or changed system must be authorised (accredited) for implementation by an Authorising Official to ensure that the system will not pose a risk to the organisation, other systems, or other organisations
- Authorisation is dependent on the certification provided by the security control assessor (audit) that the system is secure. These tests are done throughout the phases of the lifecycle



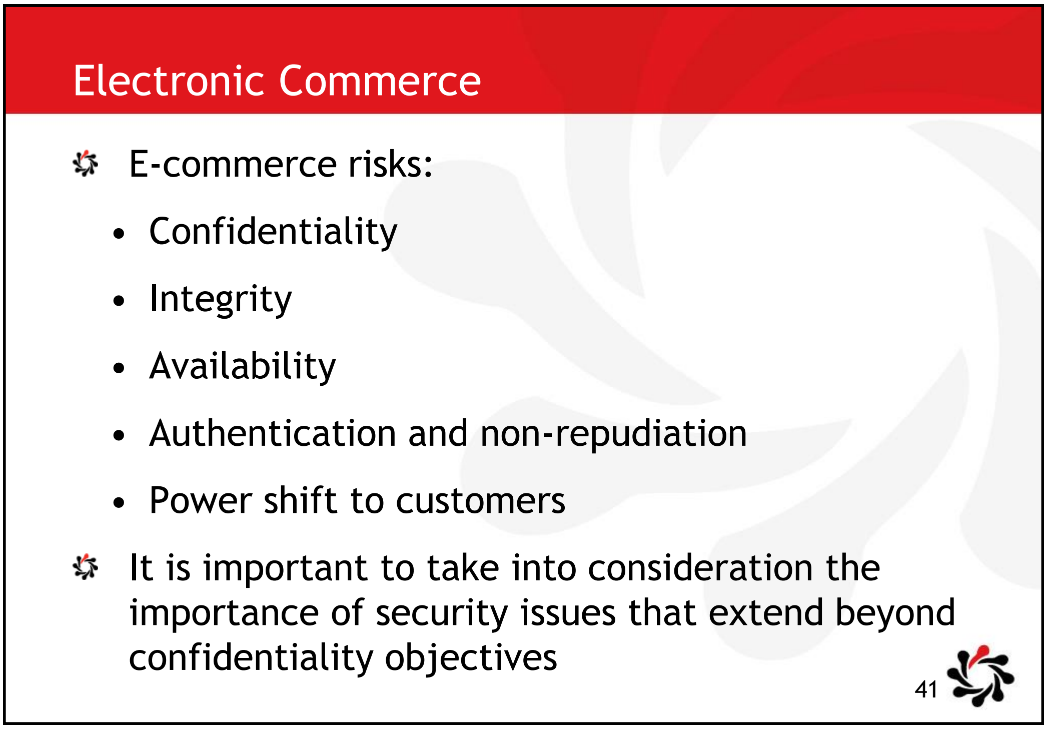
Post-Implementation

- Verify that the system meets user requirements and expectations
- Ensure security controls have been built-in
- Assess cost-benefit
- Develop recommendations for deficiencies
- Assess the development project



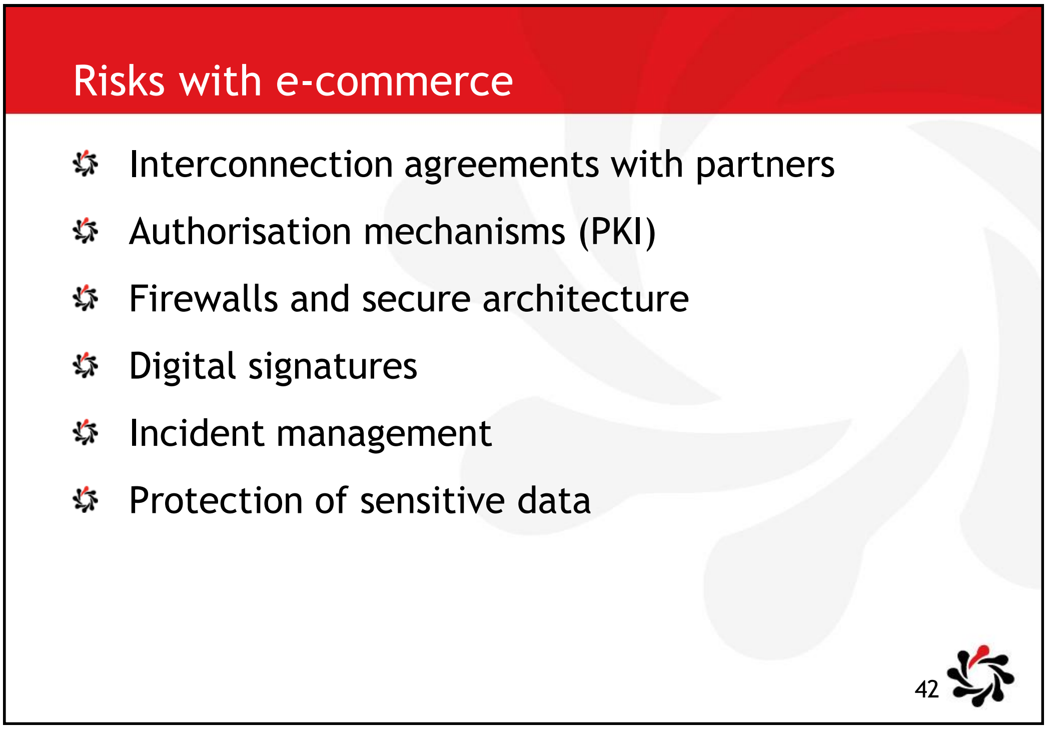
Virtualisation

- Efficient use of hardware – manage systems at a software rather than a hardware-dependent level
- Multiple operating systems on a single device
- Hypervisor
  - Type 1 – Bare metal
  - Type 2 – hosted virtualisation
- Guest machine
- Correct configuration and patching



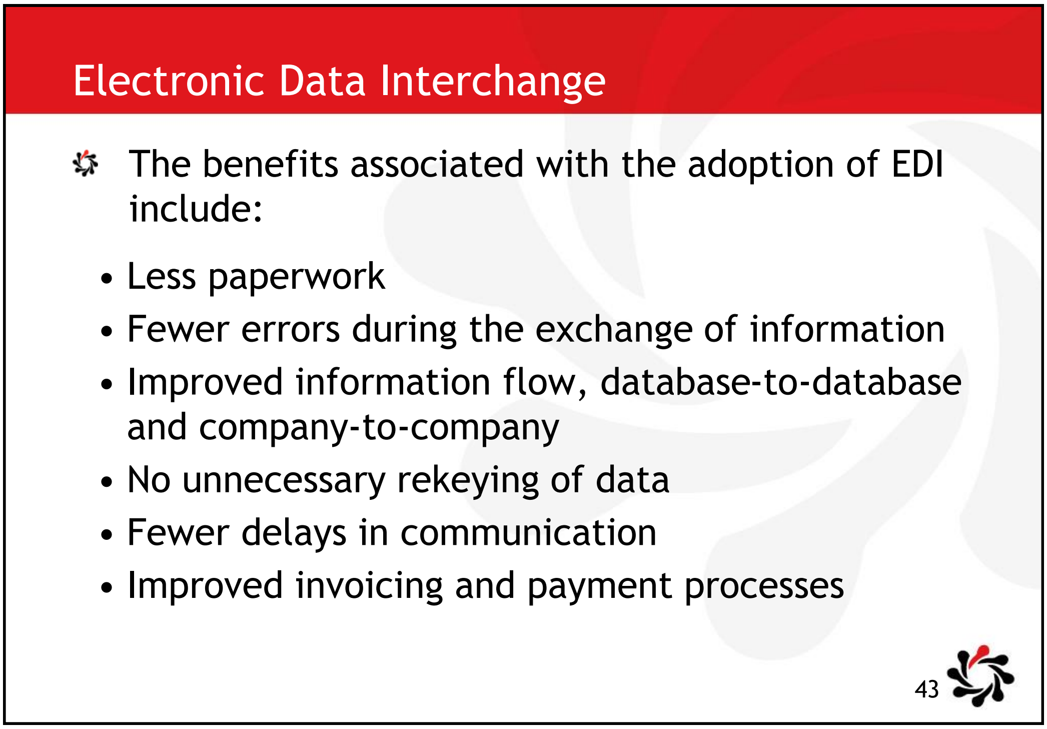
Electronic Commerce

- 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



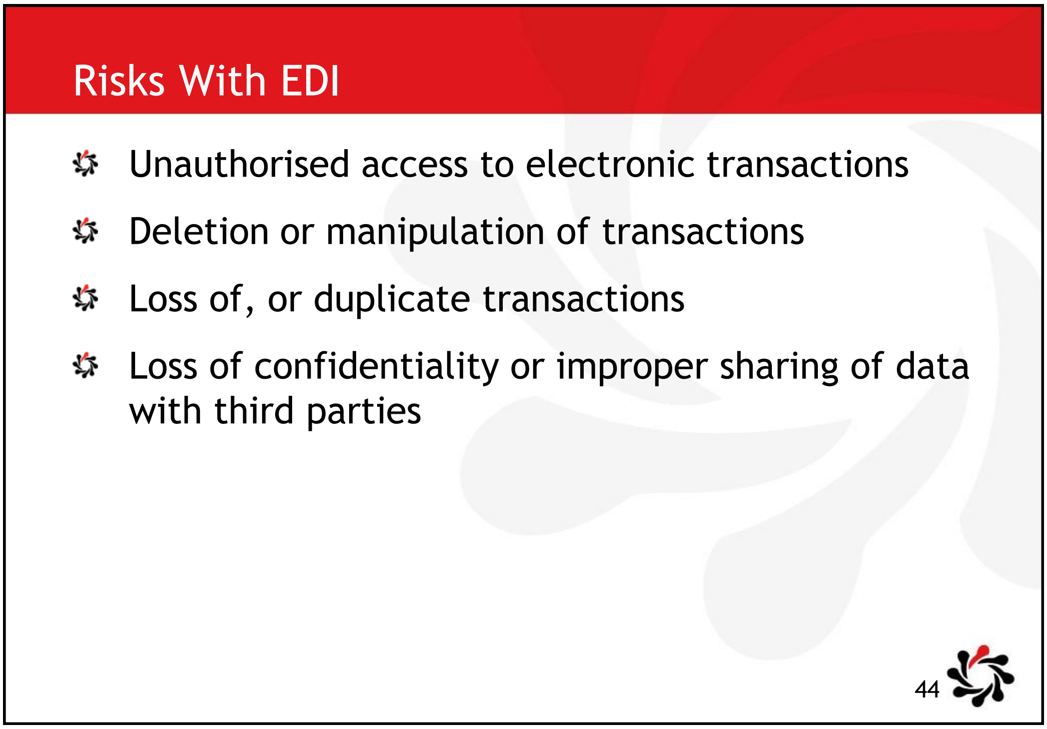
Risks with e-commerce

- Interconnection agreements with partners
- Authorisation mechanisms (PKI)
- Firewalls and secure architecture
- Digital signatures
- Incident management
- Protection of sensitive data



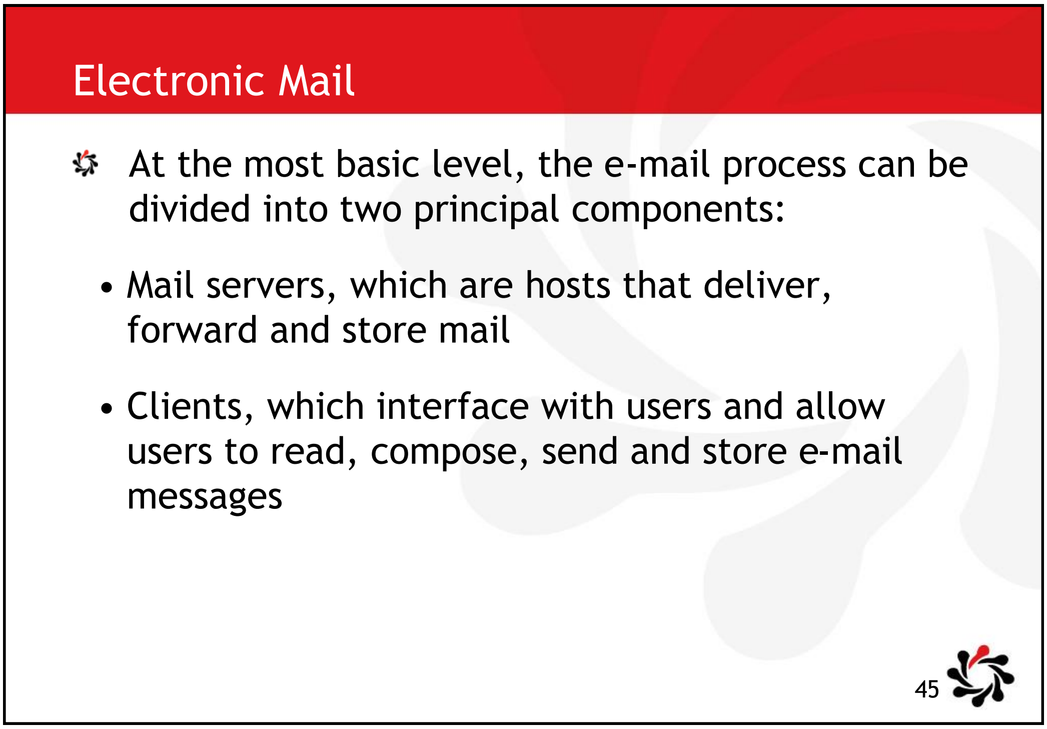
Electronic Data Interchange

- 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



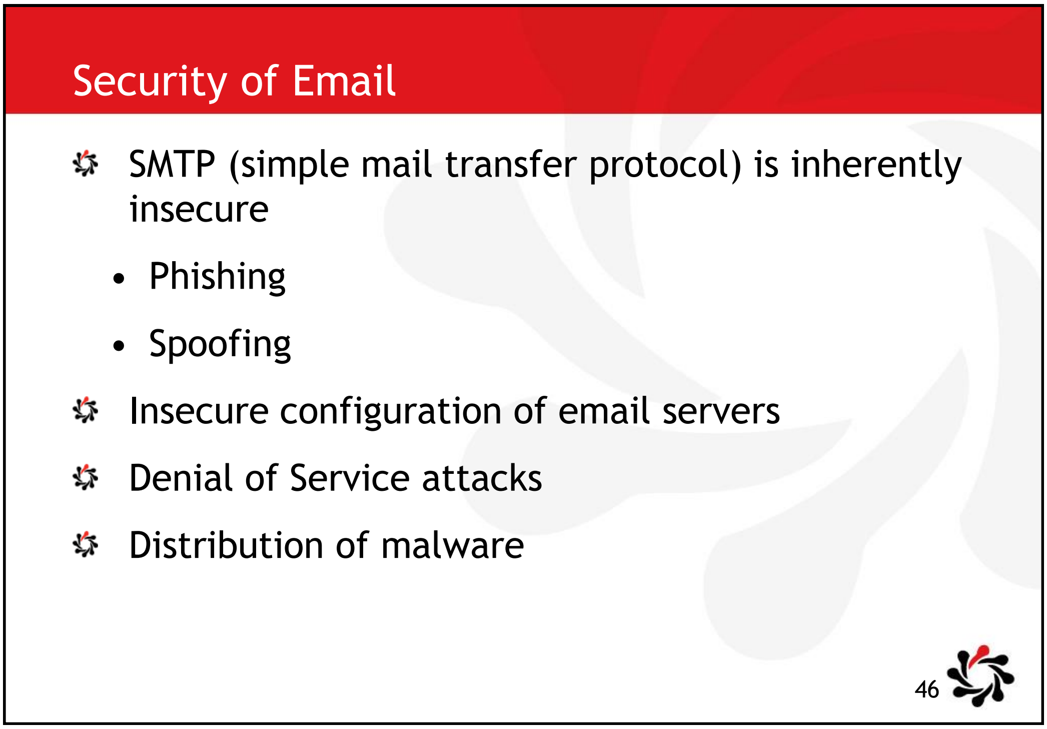
Risks With EDI

- Unauthorised access to electronic transactions
- Deletion or manipulation of transactions
- Loss of, or duplicate transactions
- Loss of confidentiality or improper sharing of data with third parties



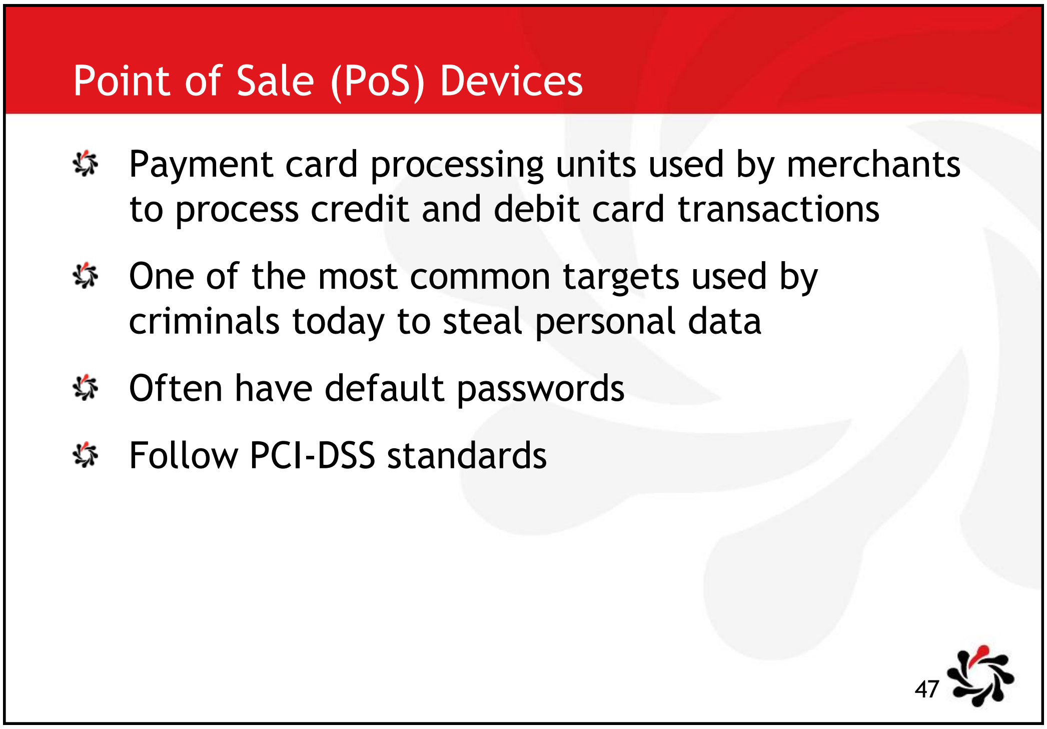
Electronic Mail

- 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



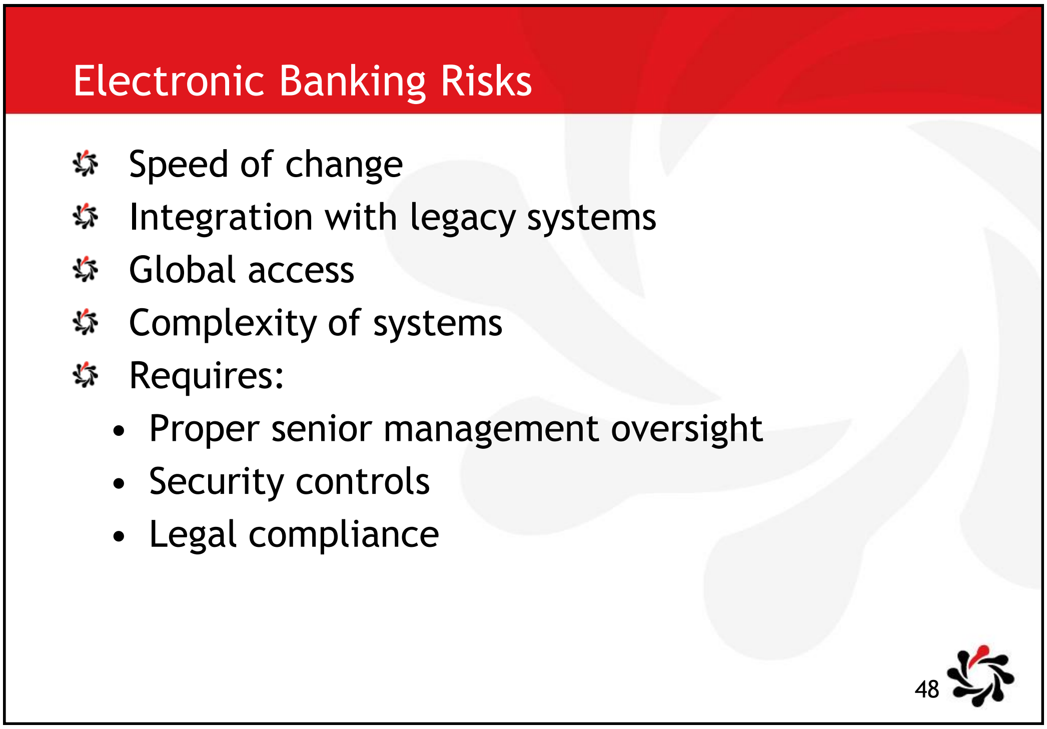
Security of Email

- SMTP (simple mail transfer protocol) is inherently insecure
  - Phishing
  - Spoofing
- Insecure configuration of email servers
- Denial of Service attacks
- Distribution of malware



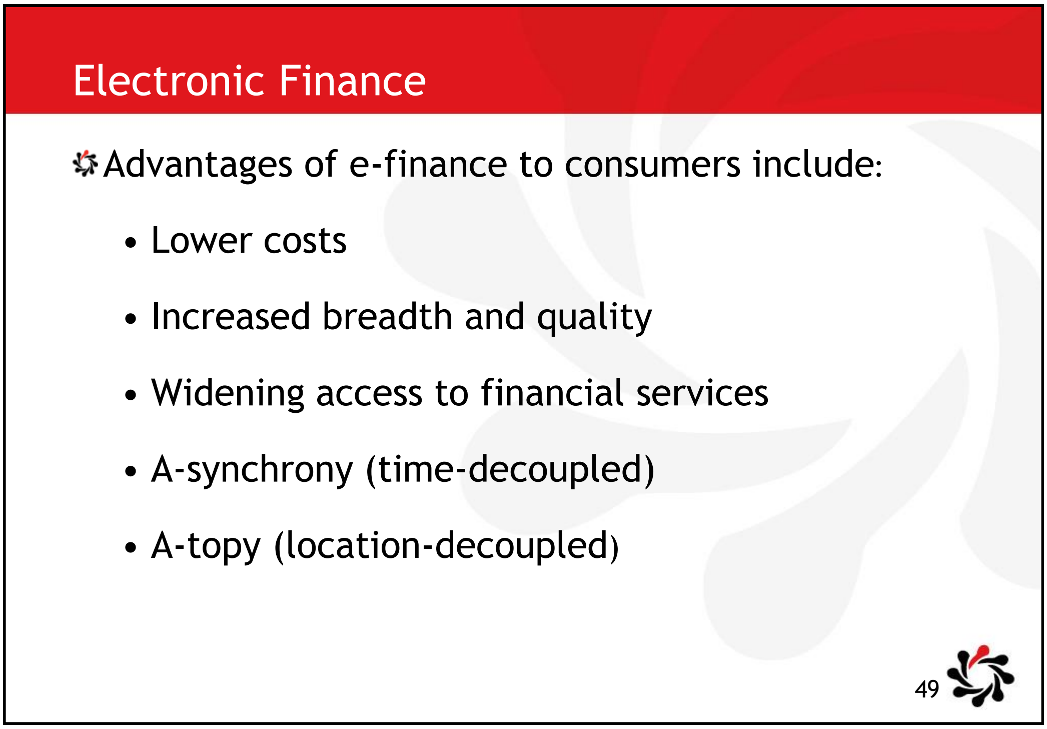
Point of Sale (PoS) Devices

- Payment card processing units used by merchants to process credit and debit card transactions
- One of the most common targets used by criminals today to steal personal data
- Often have default passwords
- Follow PCI-DSS standards



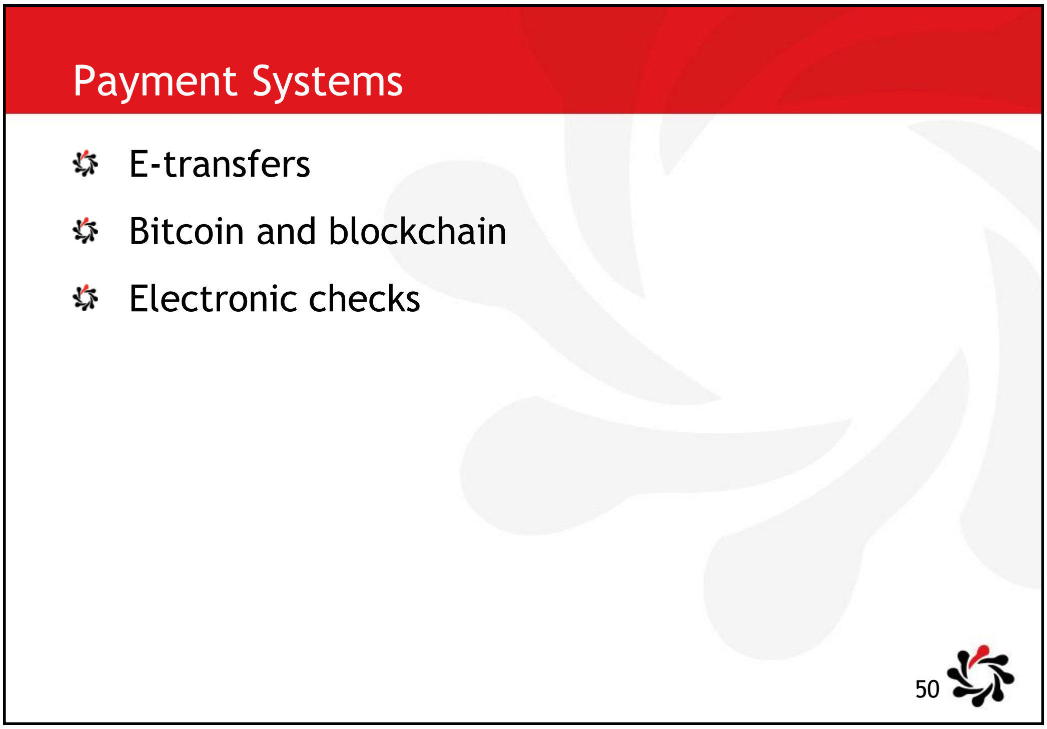
Electronic Banking Risks

- Speed of change
- Integration with legacy systems
- Global access
- Complexity of systems
- Requires:
  - Proper senior management oversight
  - Security controls
  - Legal compliance



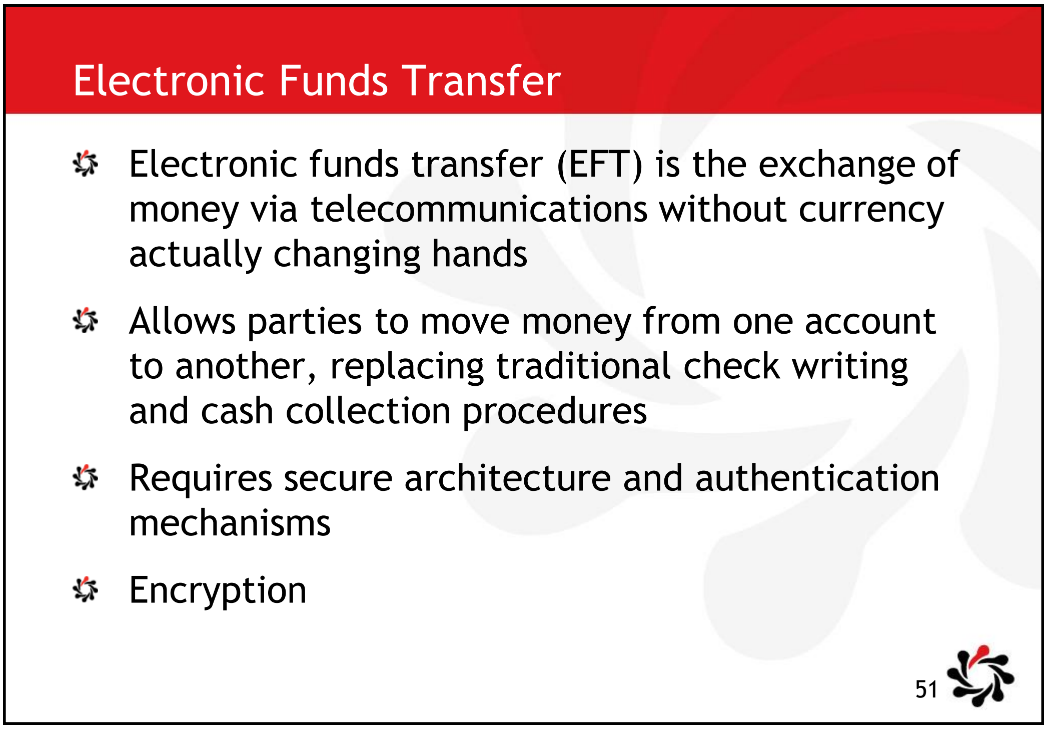
Electronic Finance

- 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)



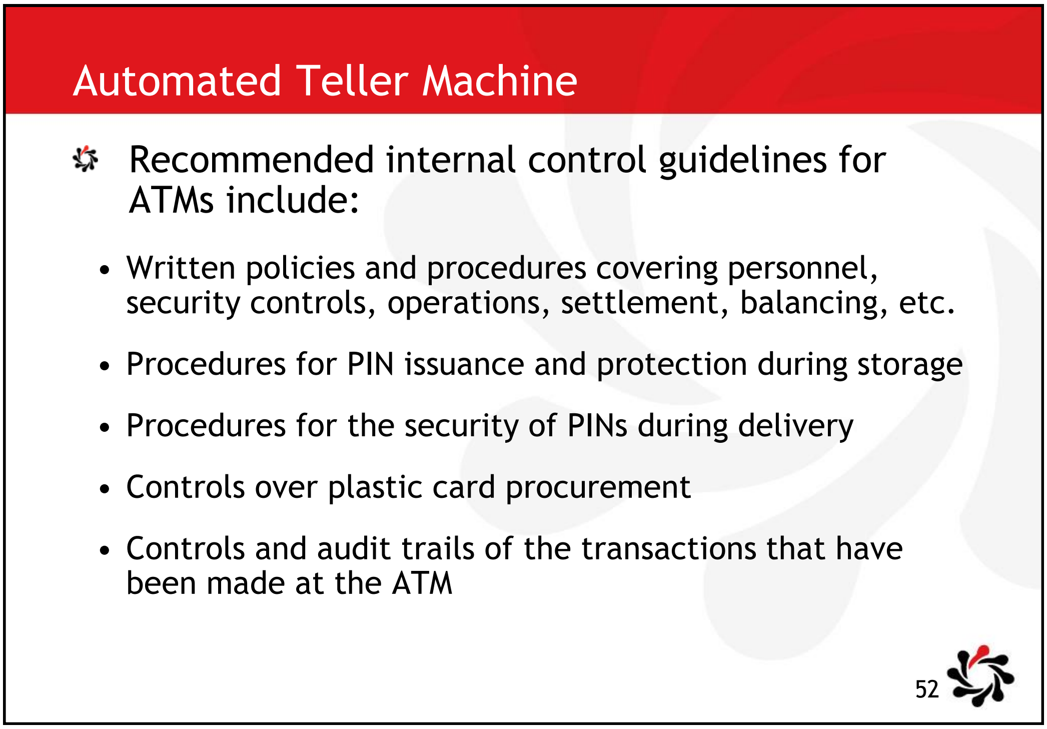
Payment Systems

- E-transfers
- Bitcoin and blockchain
- Electronic checks



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
- Requires secure architecture and authentication mechanisms
- Encryption



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

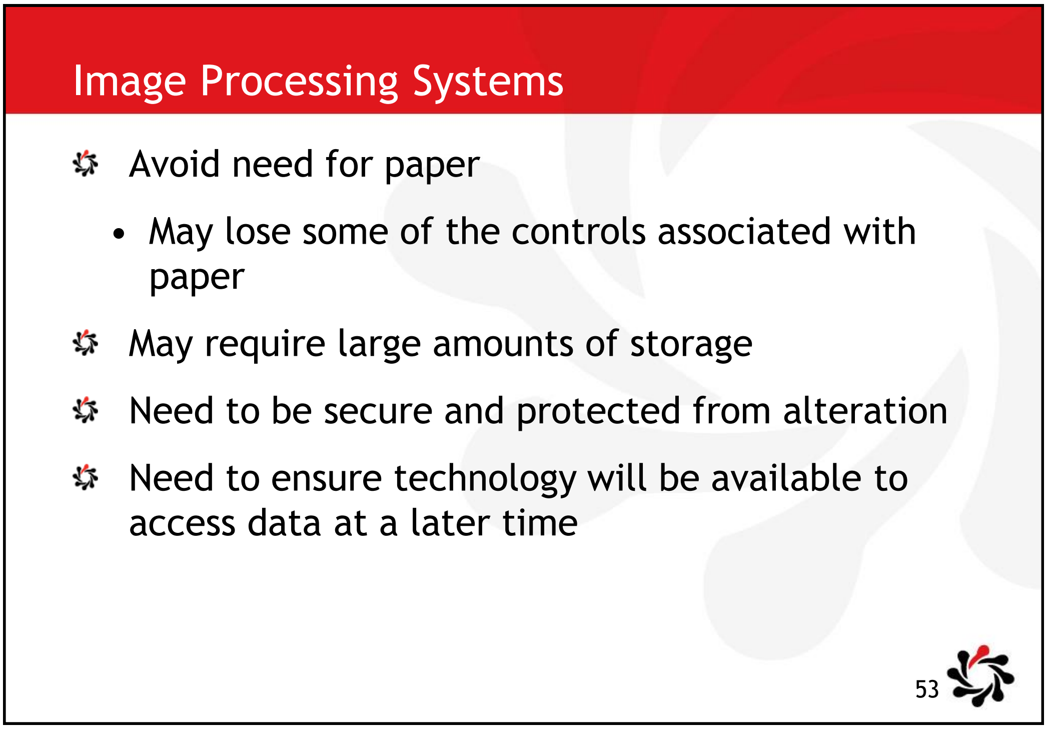
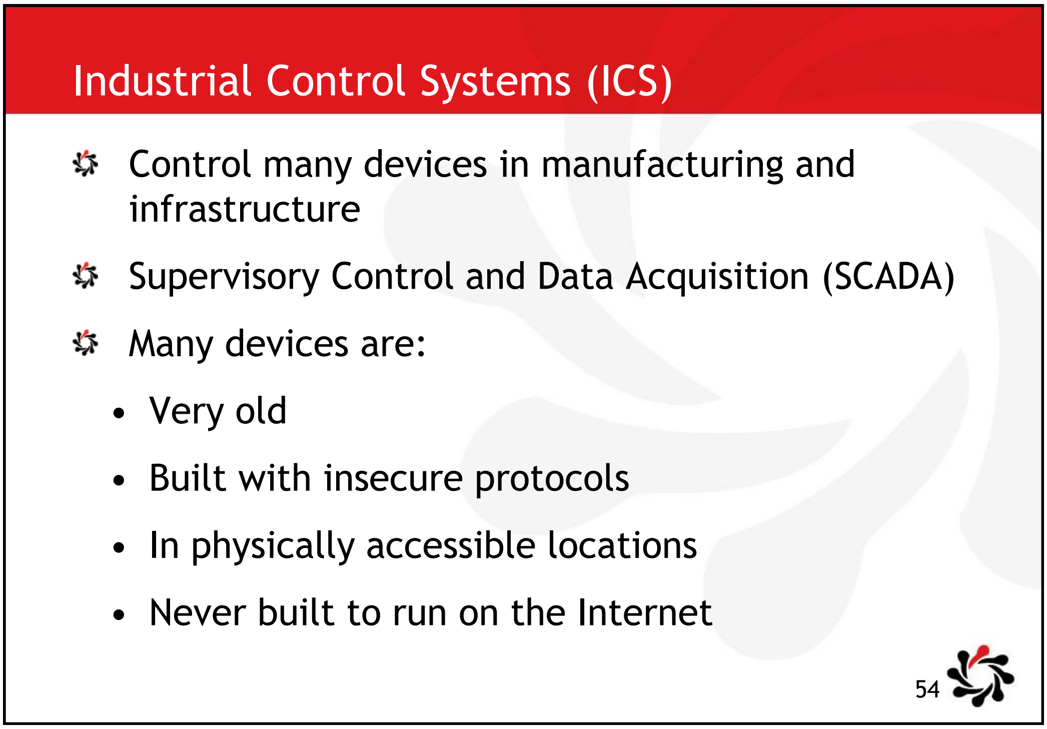


Image Processing Systems

- Avoid need for paper
  - May lose some of the controls associated with paper
- May require large amounts of storage
- Need to be secure and protected from alteration
- Need to ensure technology will be available to access data at a later time

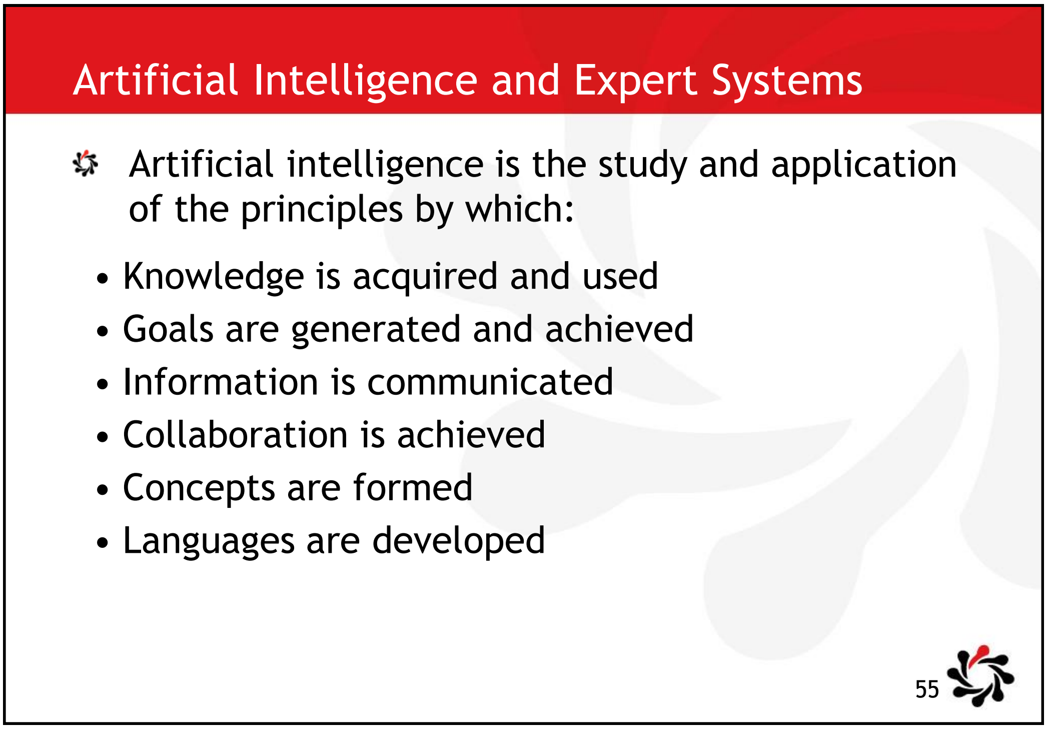
53



Industrial Control Systems (ICS)

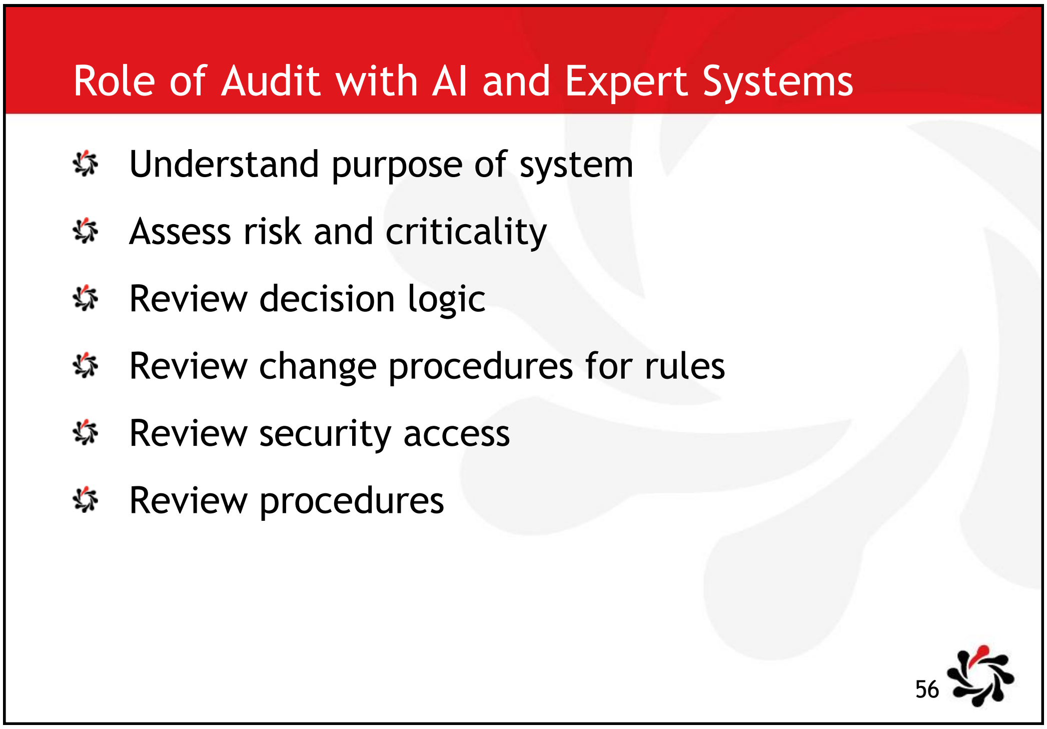
- Control many devices in manufacturing and infrastructure
- Supervisory Control and Data Acquisition (SCADA)
- Many devices are:
  - Very old
  - Built with insecure protocols
  - In physically accessible locations
  - Never built to run on the Internet

54



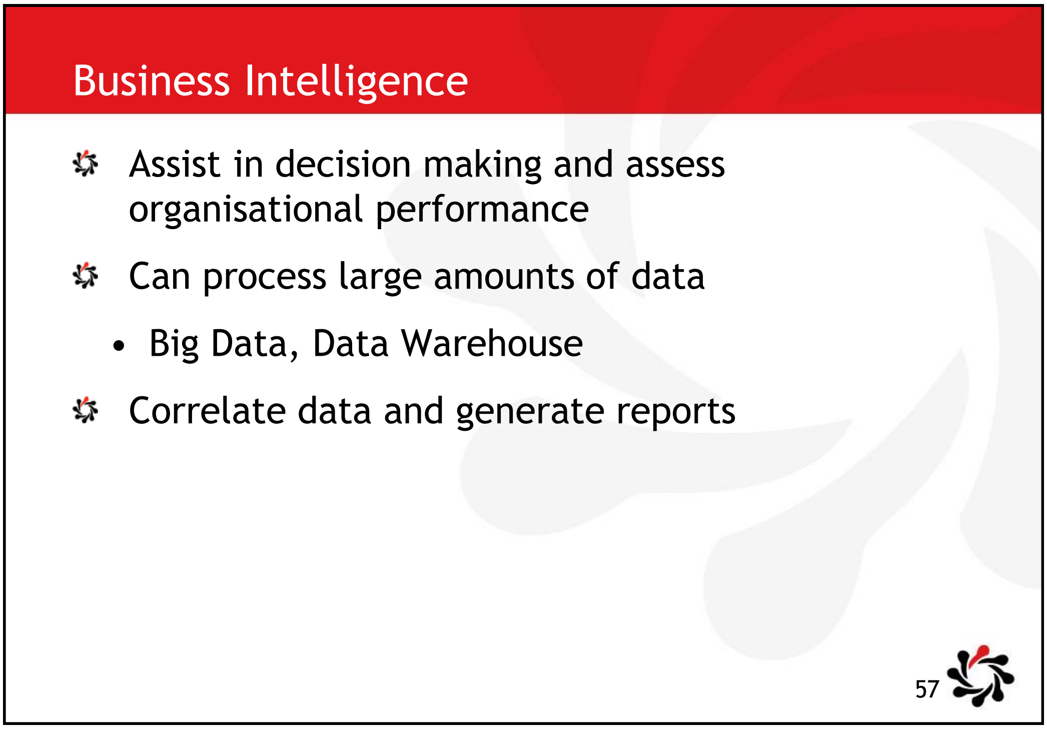
Artificial Intelligence and Expert Systems

- 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



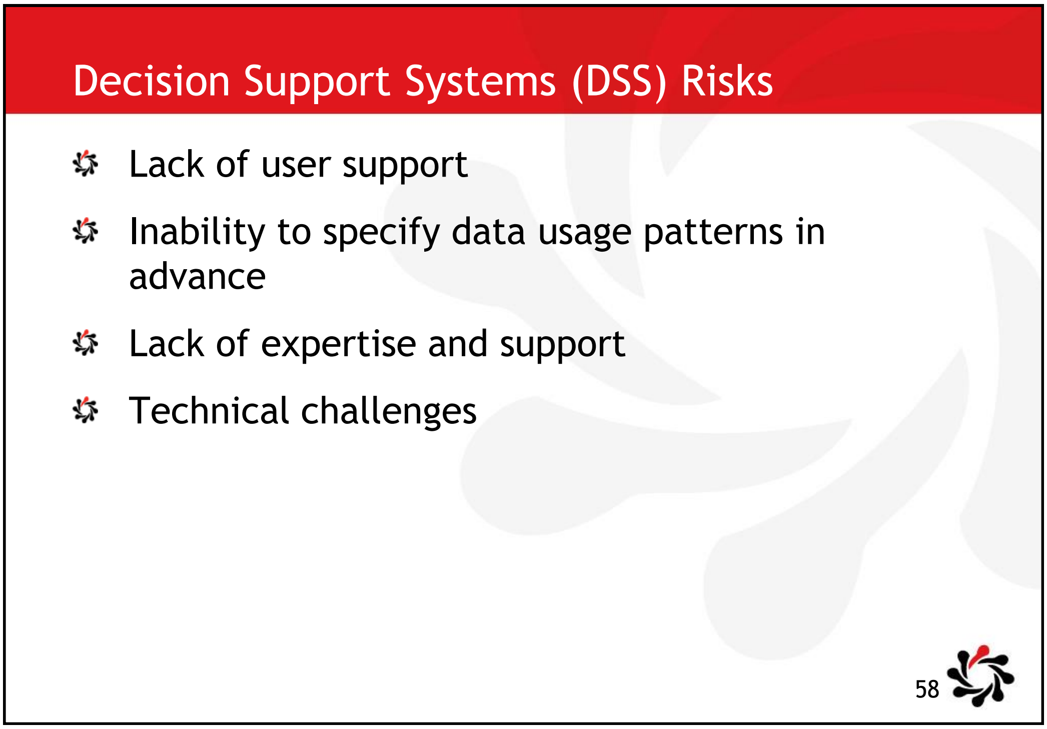
Role of Audit with AI and Expert Systems

- Understand purpose of system
- Assess risk and criticality
- Review decision logic
- Review change procedures for rules
- Review security access
- Review procedures



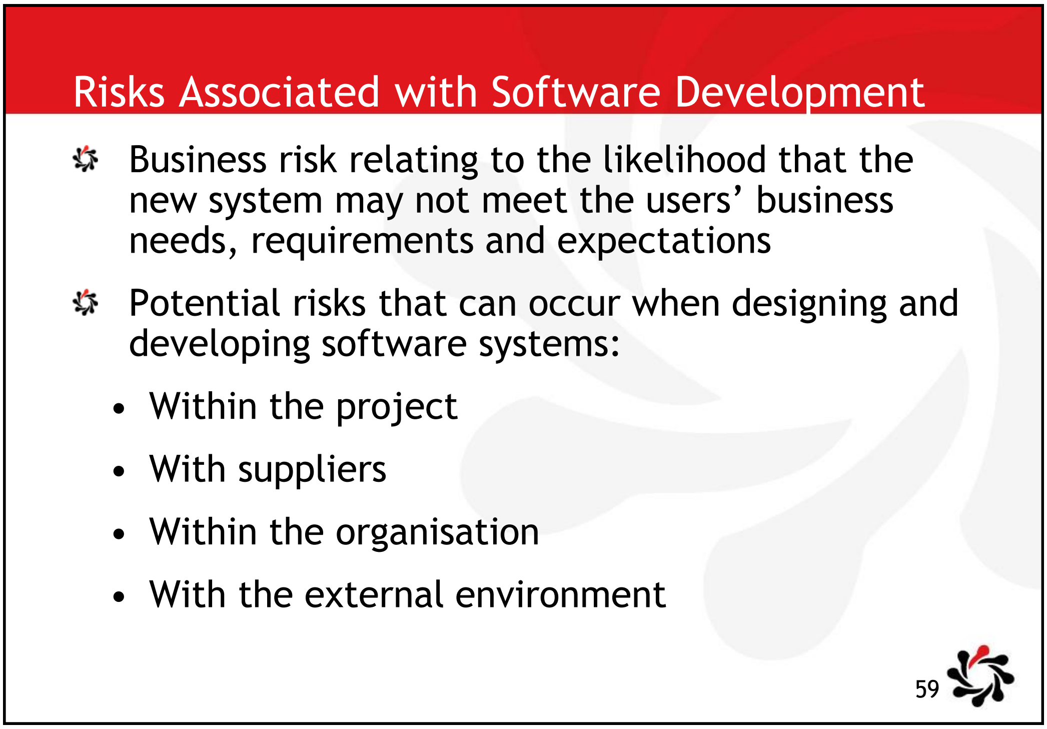
Business Intelligence

- Assist in decision making and assess organisational performance
- Can process large amounts of data
  - Big Data, Data Warehouse
- Correlate data and generate reports



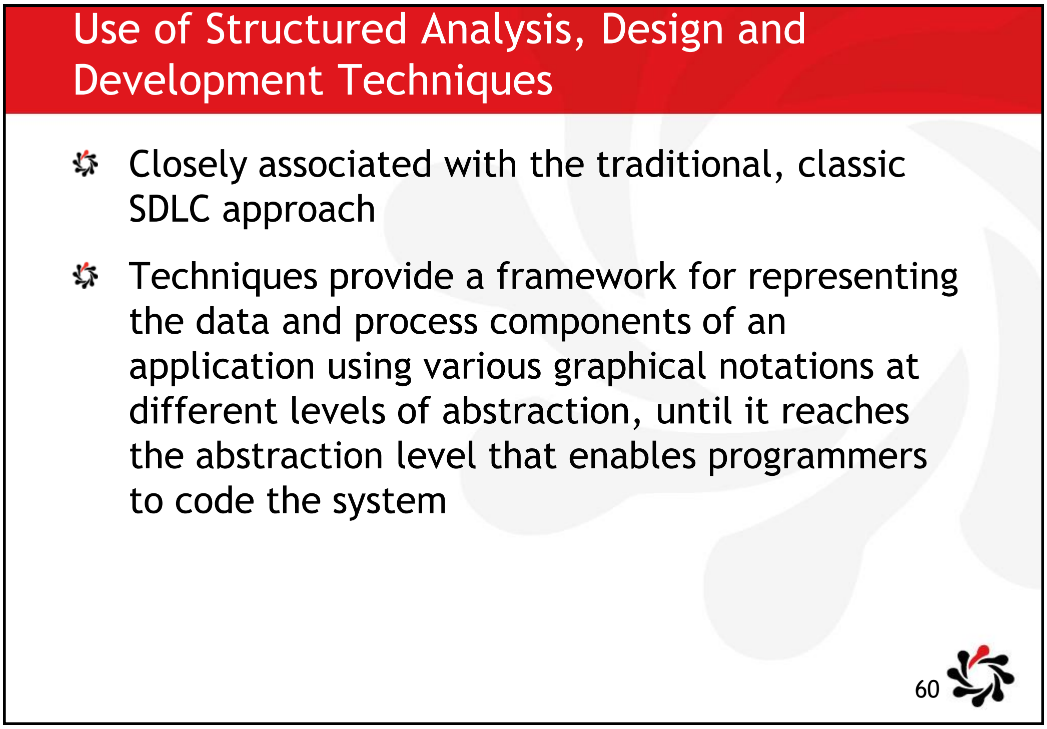
Decision Support Systems (DSS) Risks

- Lack of user support
- Inability to specify data usage patterns in advance
- Lack of expertise and support
- Technical challenges



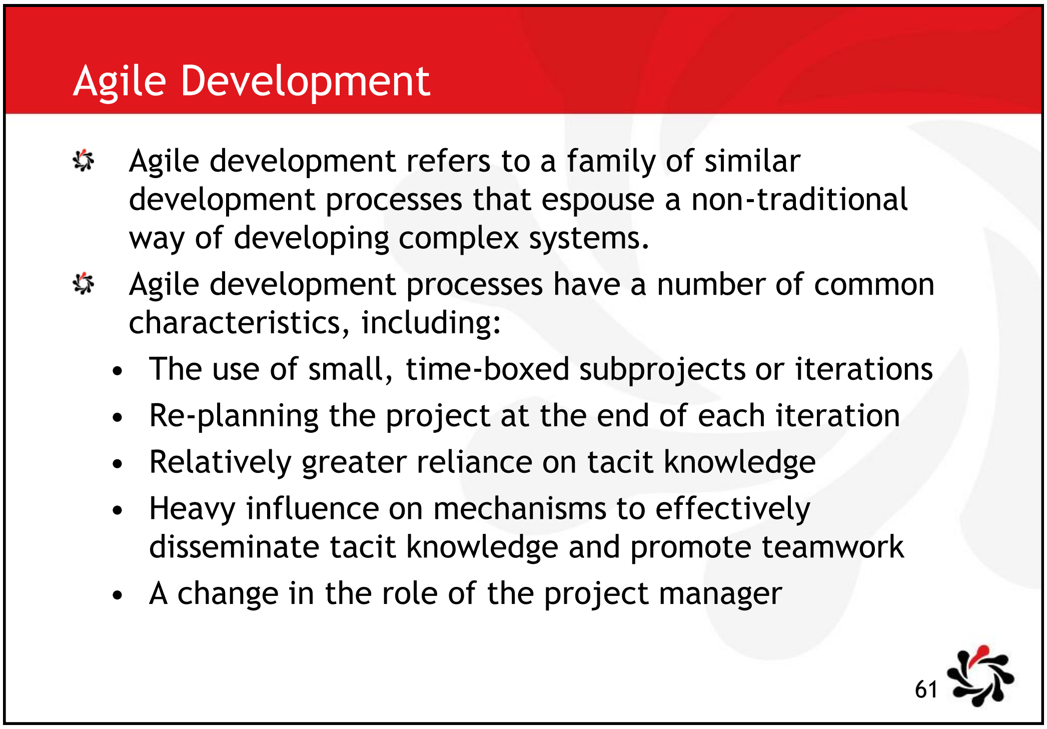
Risks Associated with Software Development

- 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



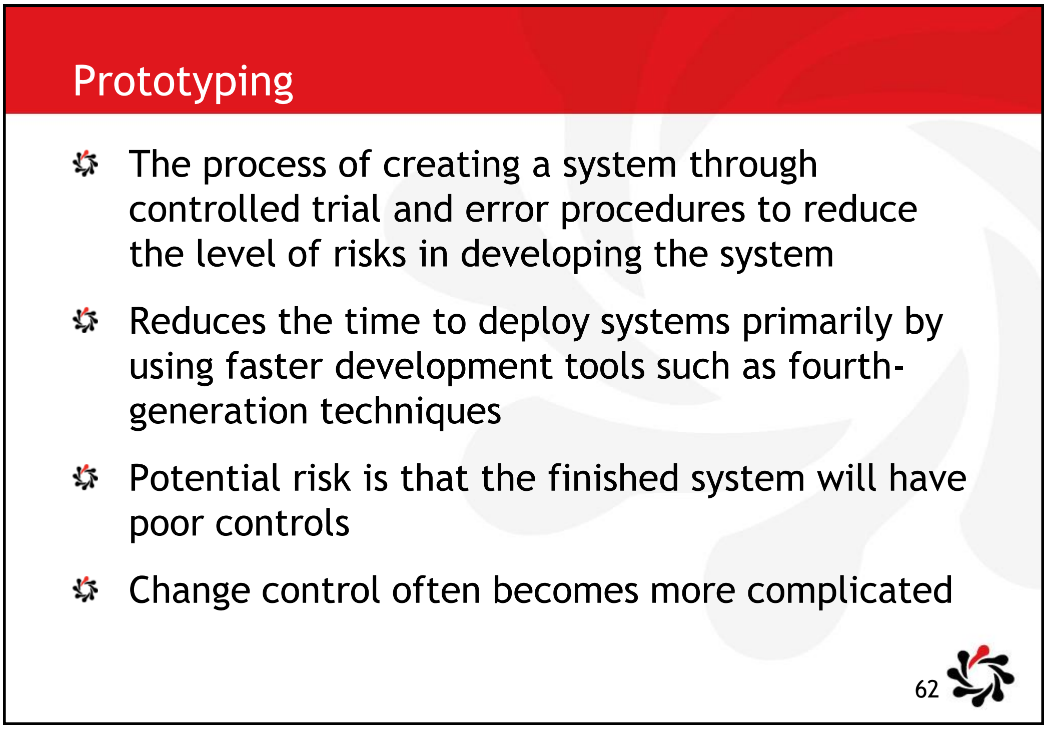
Use of Structured Analysis, Design and Development Techniques

- 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



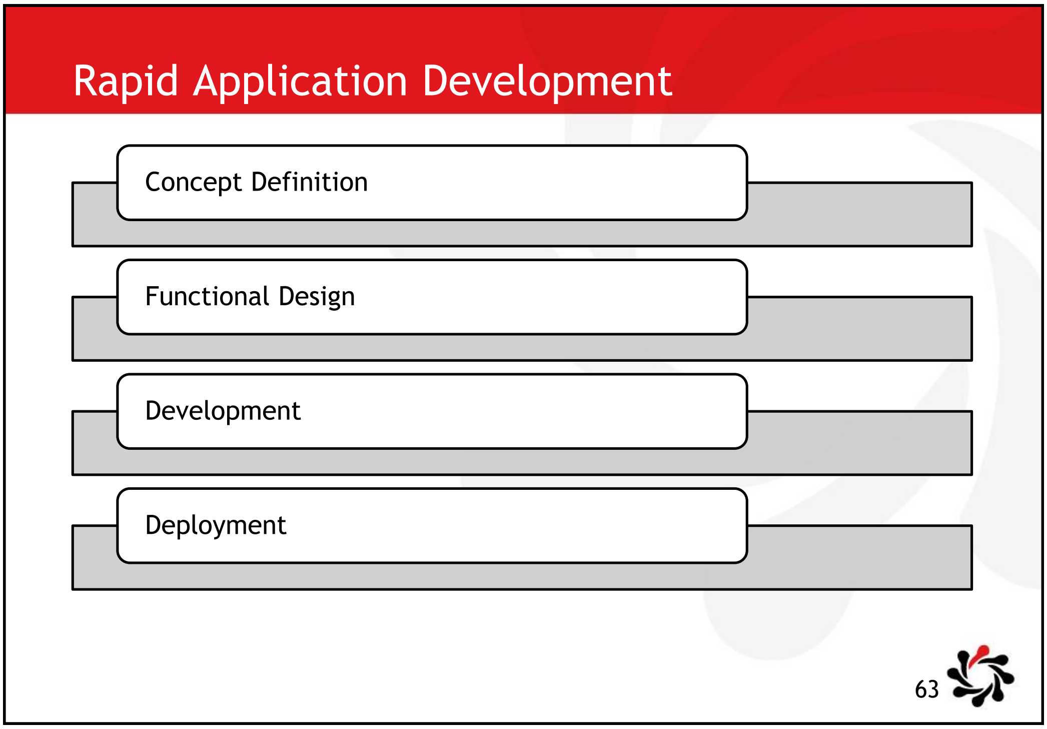
Agile Development

- 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



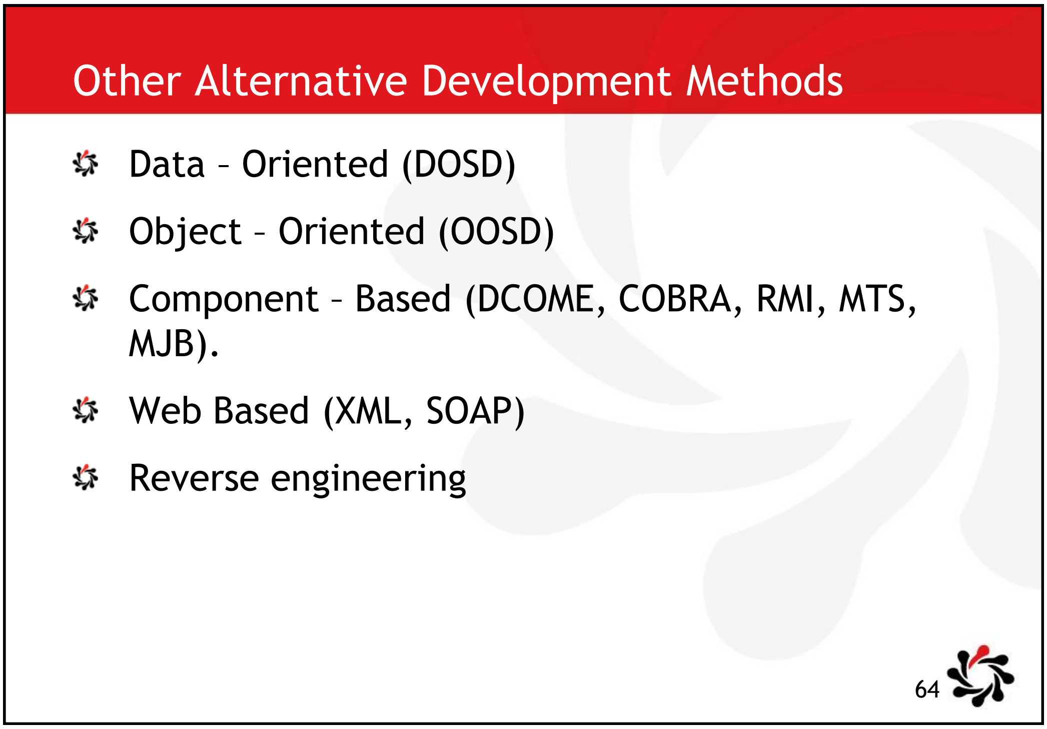
Prototyping

- 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

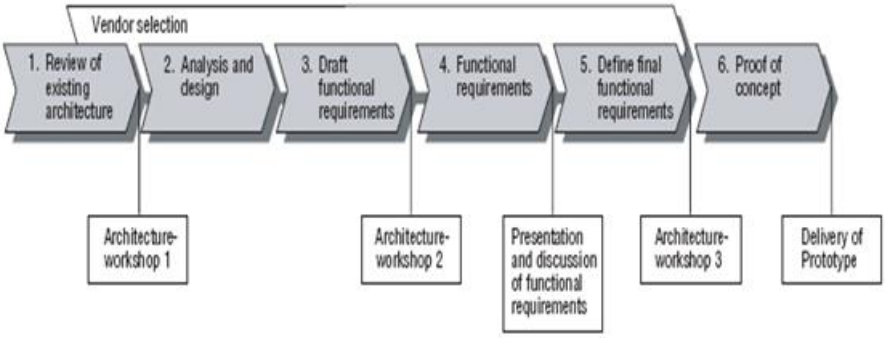
- Concept Definition
- Functional Design
- Development
- Deployment



Other Alternative Development Methods

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

Project Phases of Physical Architecture Analysis



Vendor selection

1. Review of existing architecture

2. Analysis and design

3. Draft functional requirements

4. Functional requirements

5. Define final functional requirements

6. Proof of concept

Architecture-workshop 1

Architecture-workshop 2

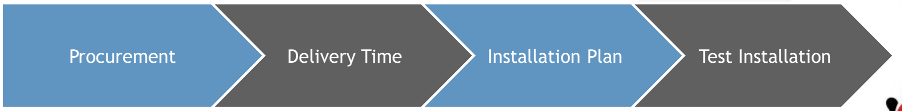
Presentation and discussion of functional requirements

Architecture-workshop 3

Delivery of Prototype

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

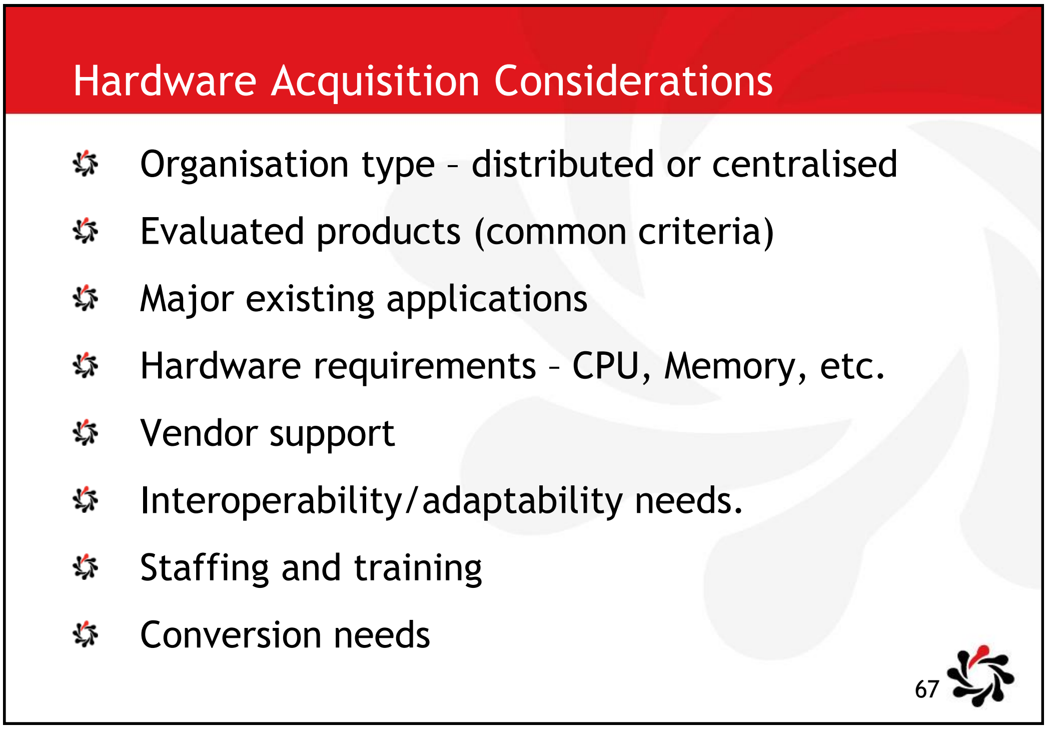


Procurement

Delivery Time

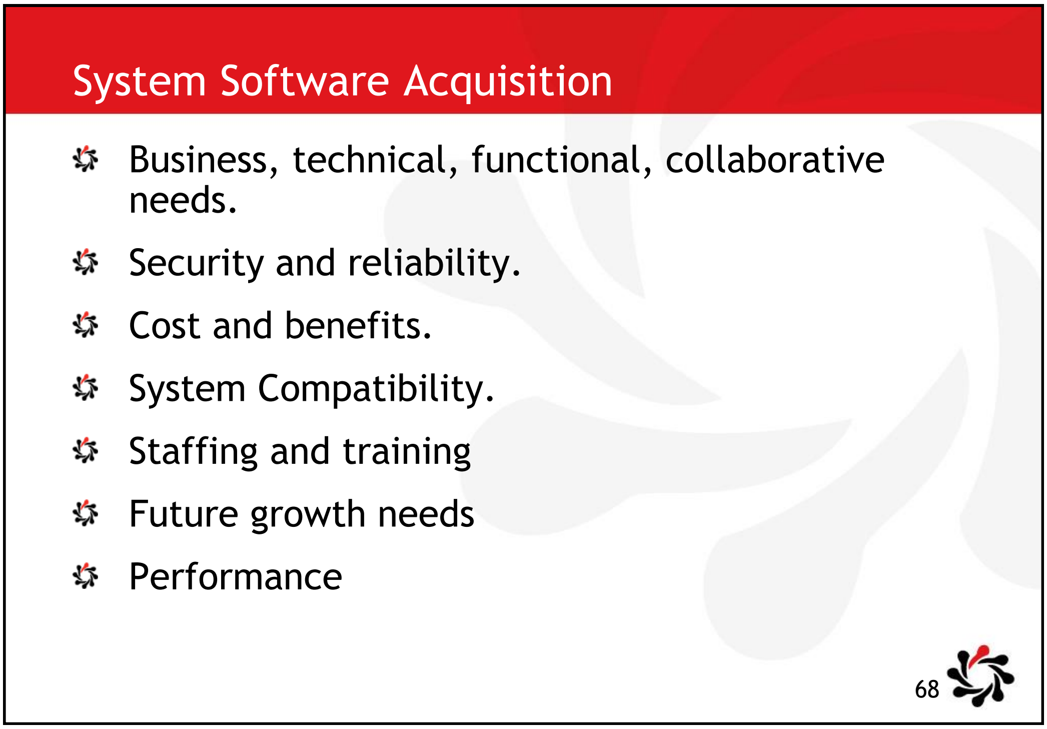
Installation Plan

Test Installation



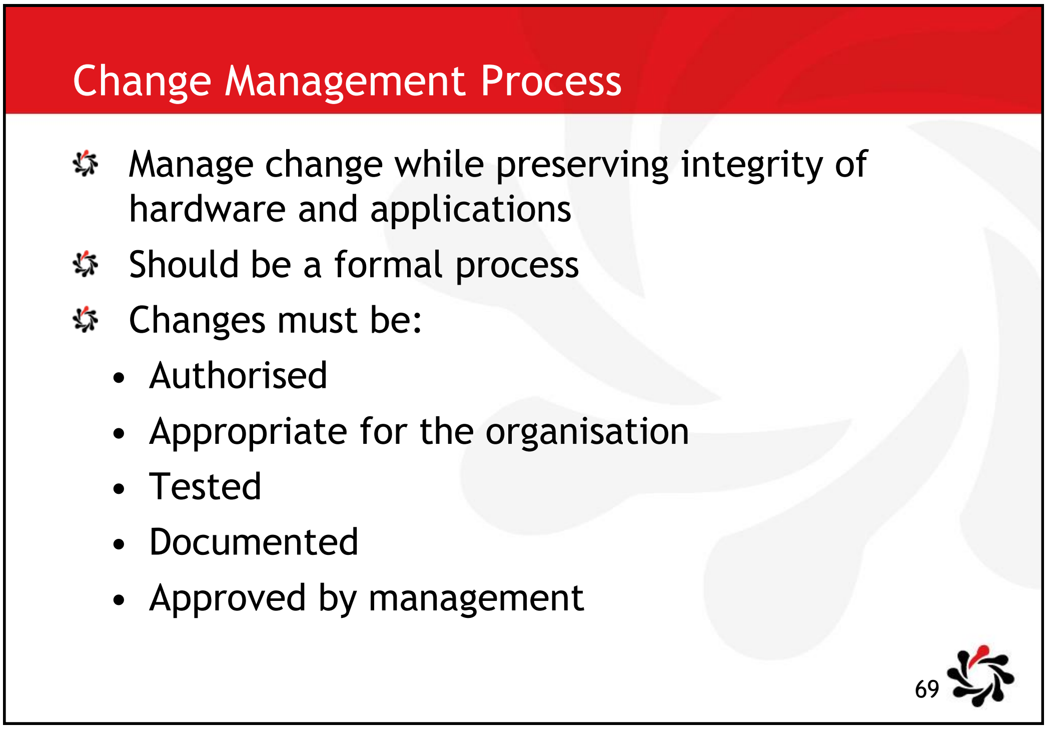
Hardware Acquisition Considerations

- Organisation type – distributed or centralised
- Evaluated products (common criteria)
- Major existing applications
- Hardware requirements – CPU, Memory, etc.
- Vendor support
- Interoperability/adaptability needs.
- Staffing and training
- Conversion needs



System Software Acquisition

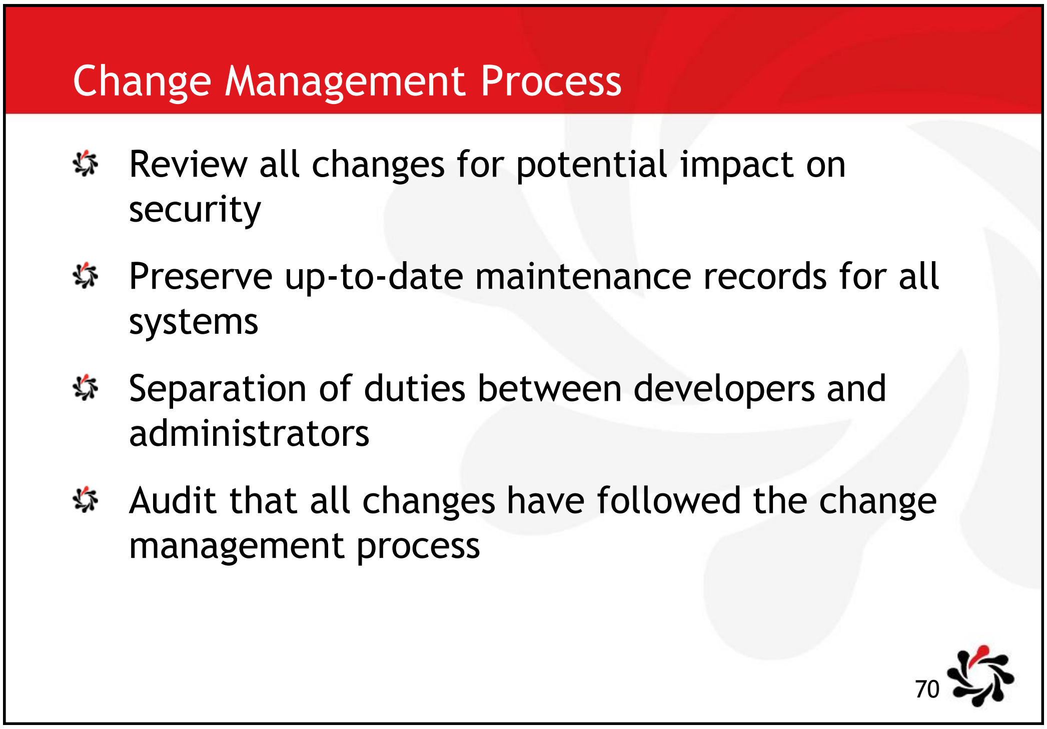
- Business, technical, functional, collaborative needs.
- Security and reliability.
- Cost and benefits.
- System Compatibility.
- Staffing and training
- Future growth needs
- Performance



Change Management Process

- Manage change while preserving integrity of hardware and applications
- Should be a formal process
- Changes must be:
  - Authorised
  - Appropriate for the organisation
  - Tested
  - Documented
  - Approved by management

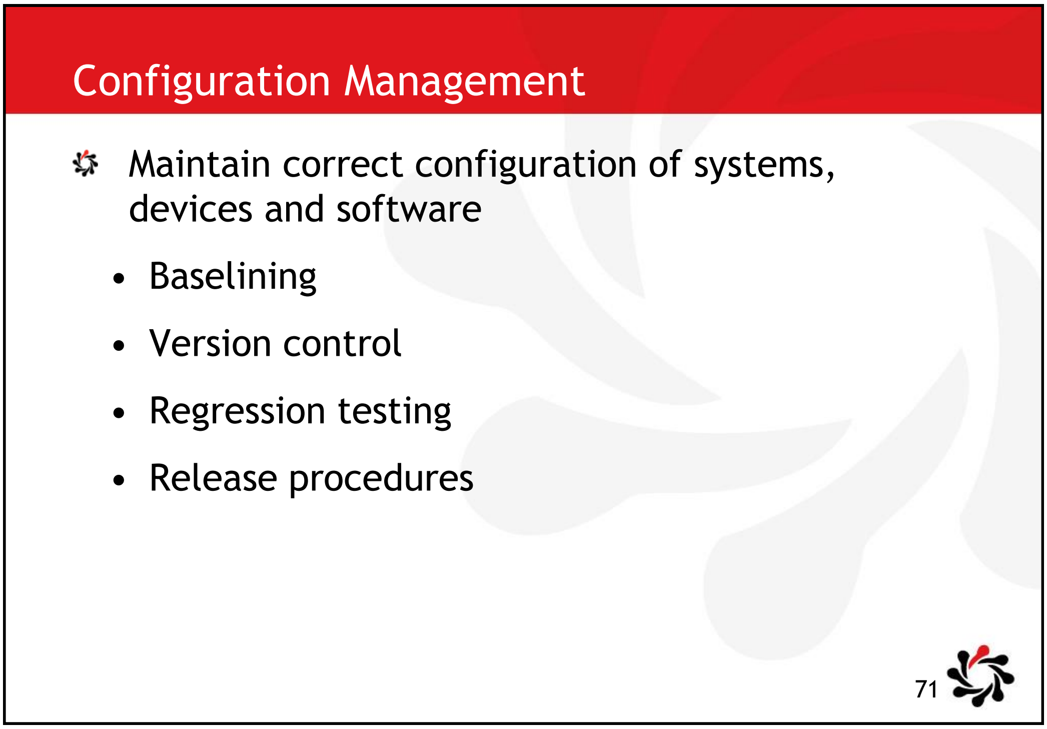
69



Change Management Process

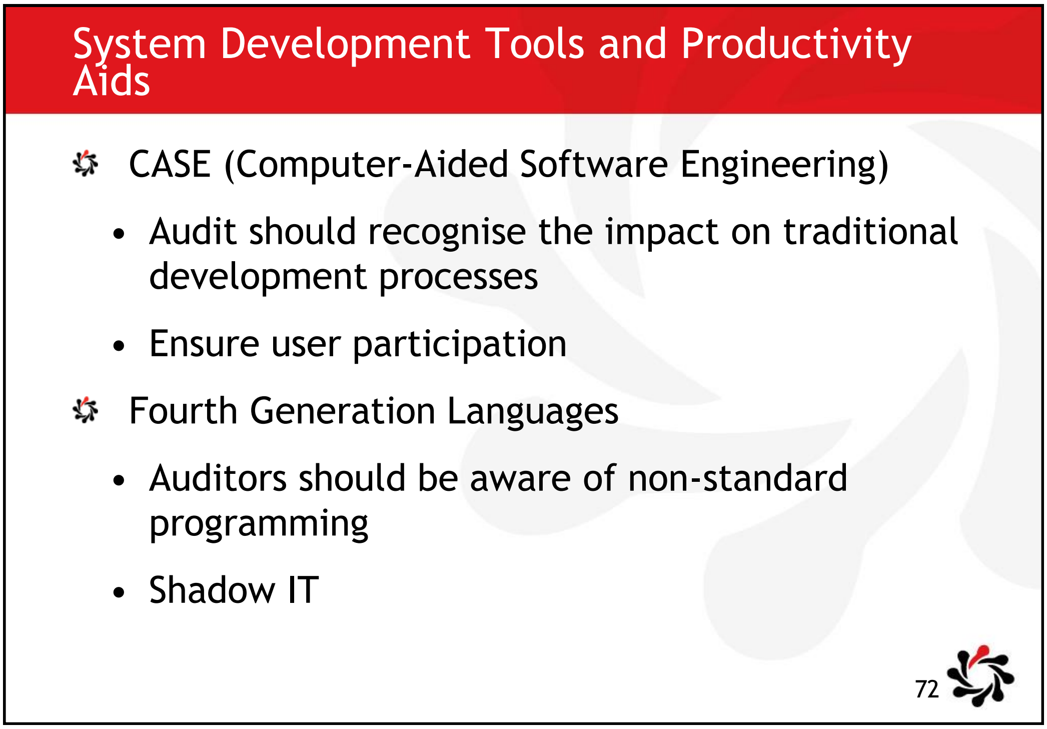
- Review all changes for potential impact on security
- Preserve up-to-date maintenance records for all systems
- Separation of duties between developers and administrators
- Audit that all changes have followed the change management process

70



Configuration Management

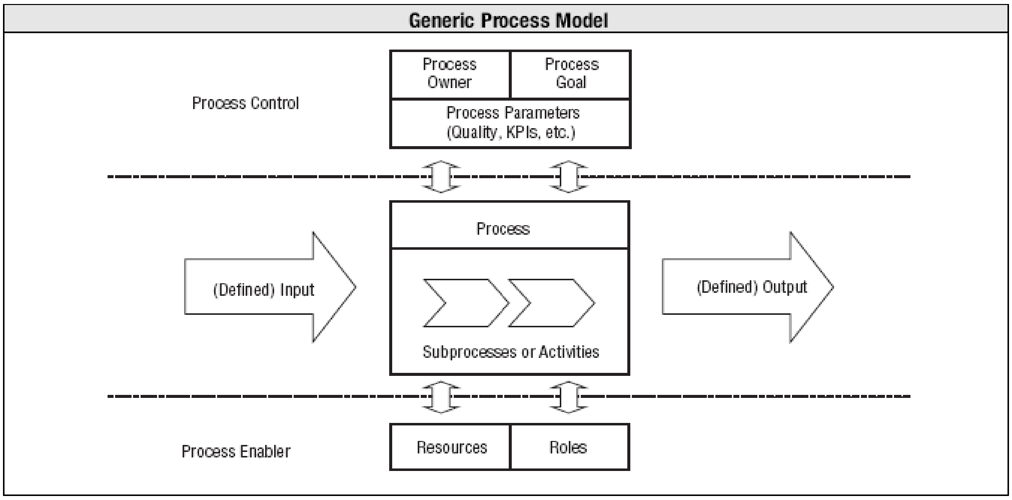
- Maintain correct configuration of systems, devices and software
  - Baselining
  - Version control
  - Regression testing
  - Release procedures



System Development Tools and Productivity Aids

- CASE (Computer-Aided Software Engineering)
  - Audit should recognise the impact on traditional development processes
  - Ensure user participation
- Fourth Generation Languages
  - Auditors should be aware of non-standard programming
  - Shadow IT

Business Process Reengineering and Process Change Projects


Generic Process Model

Process Control

Process Owner

Process Goal

Process Parameters (Quality, KPIs, etc.)

Process

(Defined) Input

Subprocesses or Activities

(Defined) Output

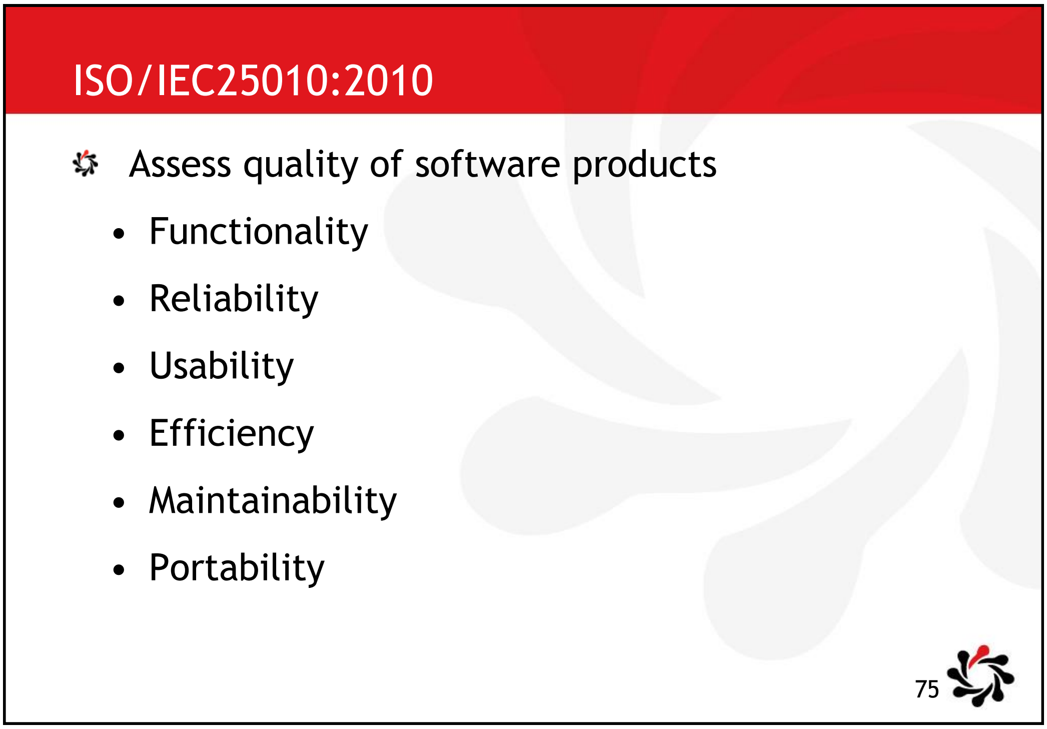
Process Enabler

Resources

Roles

Auditing BPR

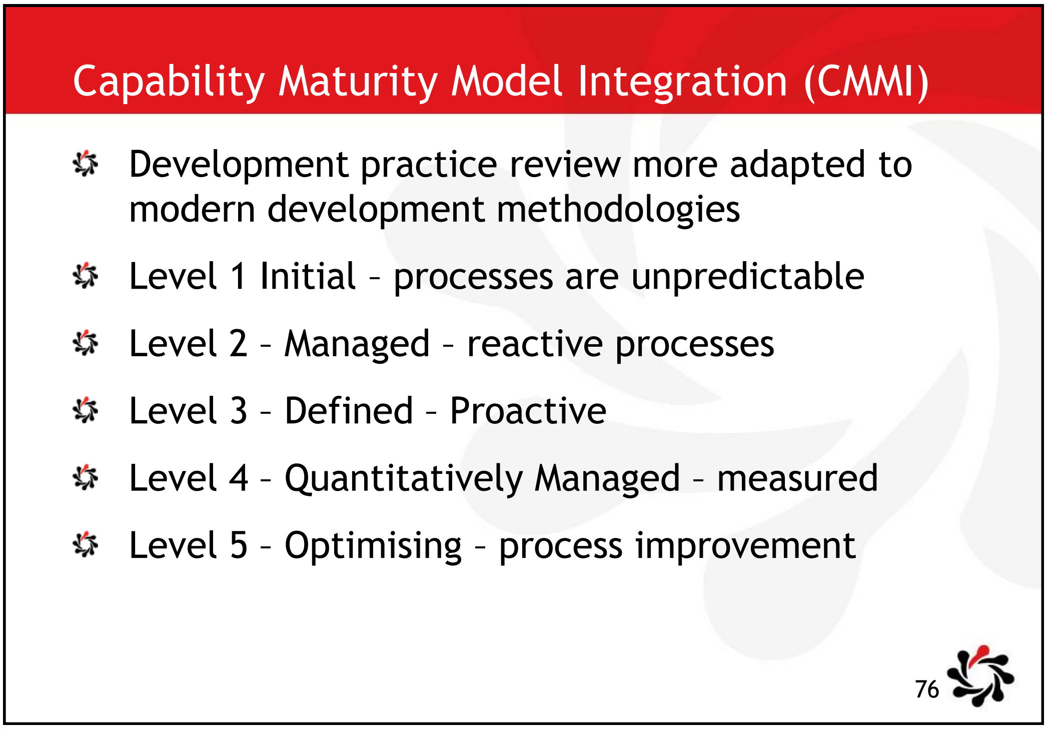
- Watch for:
  - Impact on culture
  - Minimise impact on business
  - Apply lessons learned



ISO/IEC25010:2010

- Assess quality of software products
  - Functionality
  - Reliability
  - Usability
  - Efficiency
  - Maintainability
  - Portability

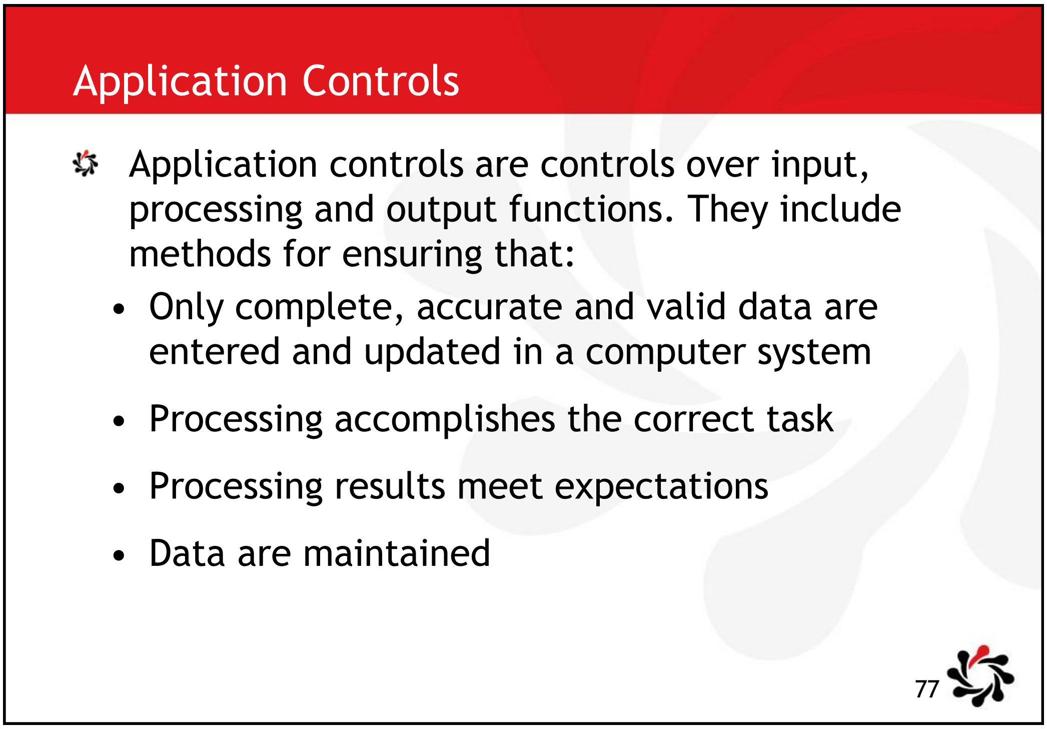
75



Capability Maturity Model Integration (CMMI)

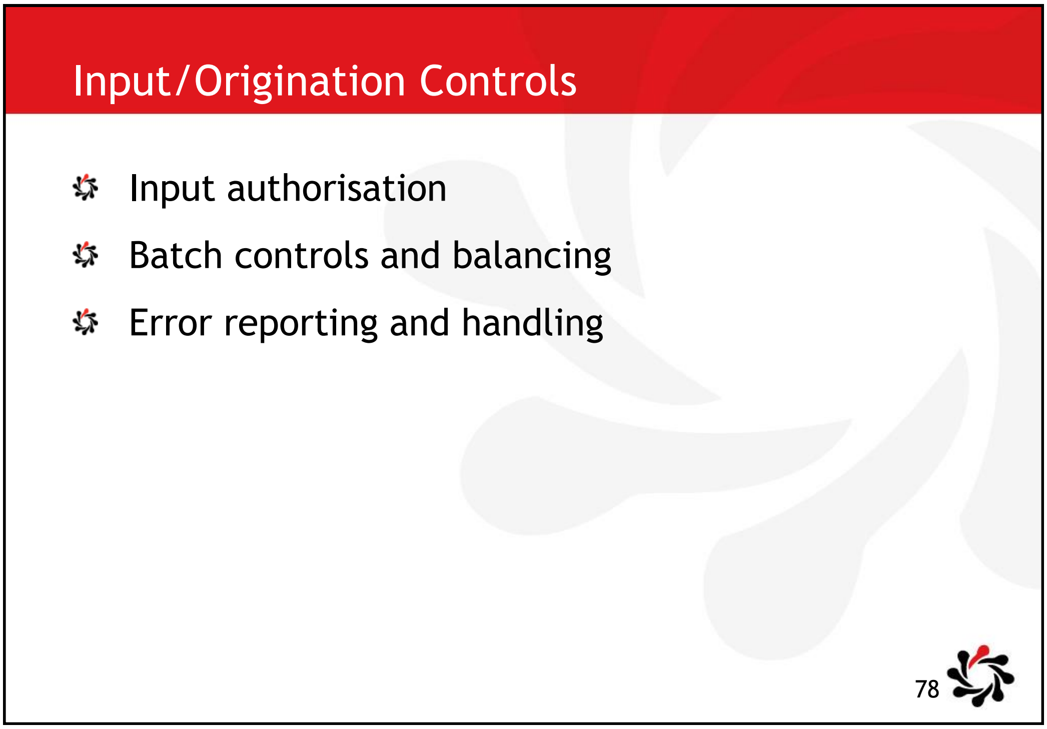
- Development practice review more adapted to modern development methodologies
- Level 1 Initial – processes are unpredictable
- Level 2 – Managed – reactive processes
- Level 3 – Defined – Proactive
- Level 4 – Quantitatively Managed – measured
- Level 5 – Optimising – process improvement

76



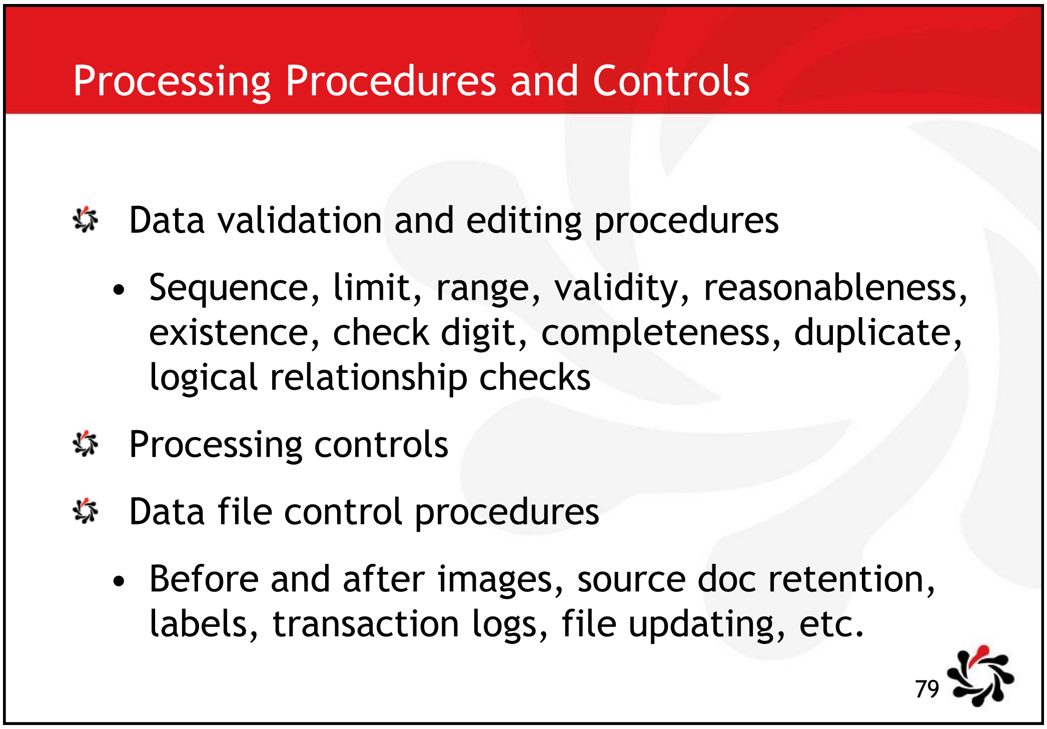
Application Controls

- 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



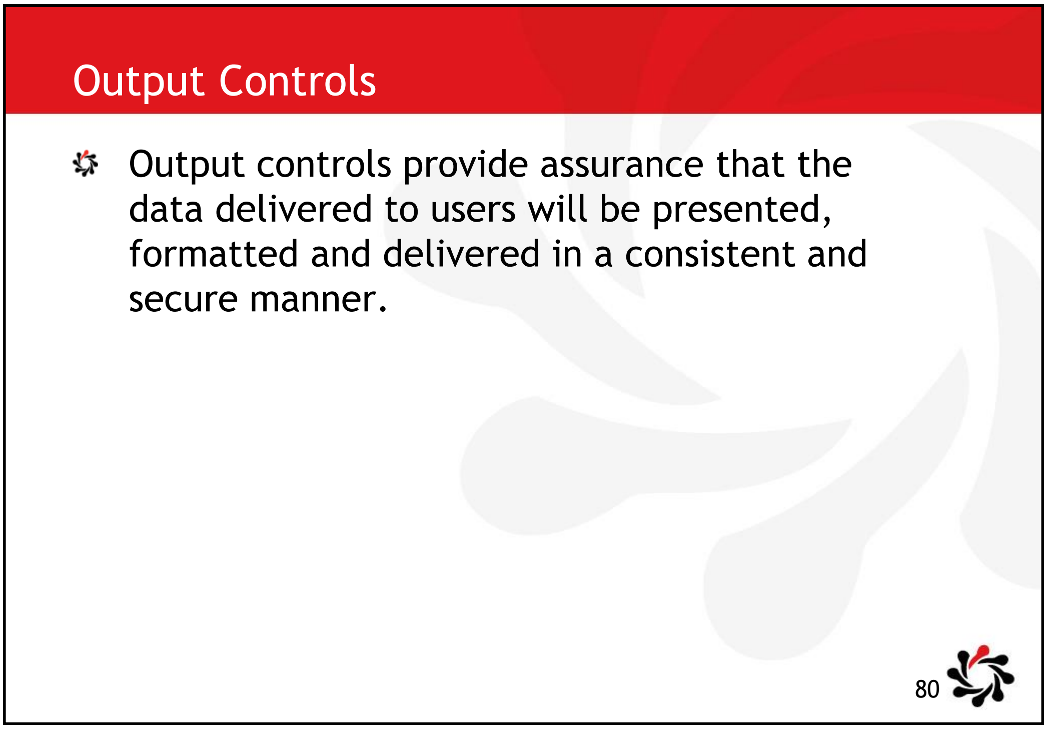
Input/Origination Controls

- Input authorisation
- Batch controls and balancing
- Error reporting and handling



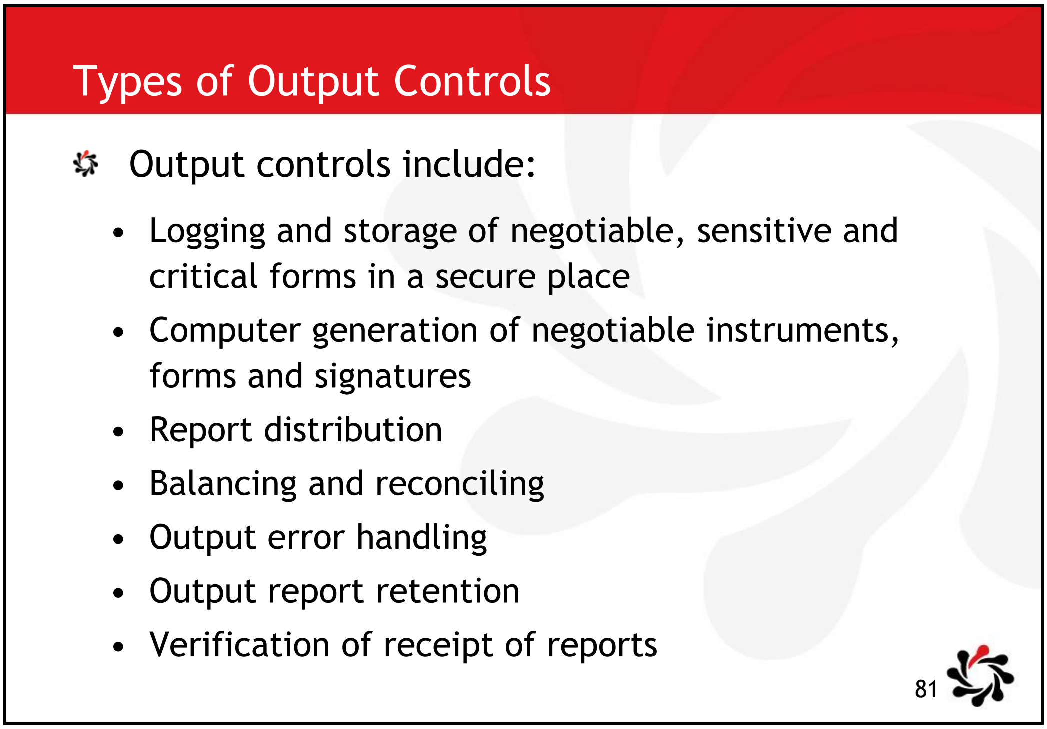
Processing Procedures and Controls

- Data validation and editing procedures
  - Sequence, limit, range, validity, reasonableness, existence, check digit, completeness, duplicate, logical relationship checks
- Processing controls
- Data file control procedures
  - Before and after images, source doc retention, labels, transaction logs, file updating, etc.



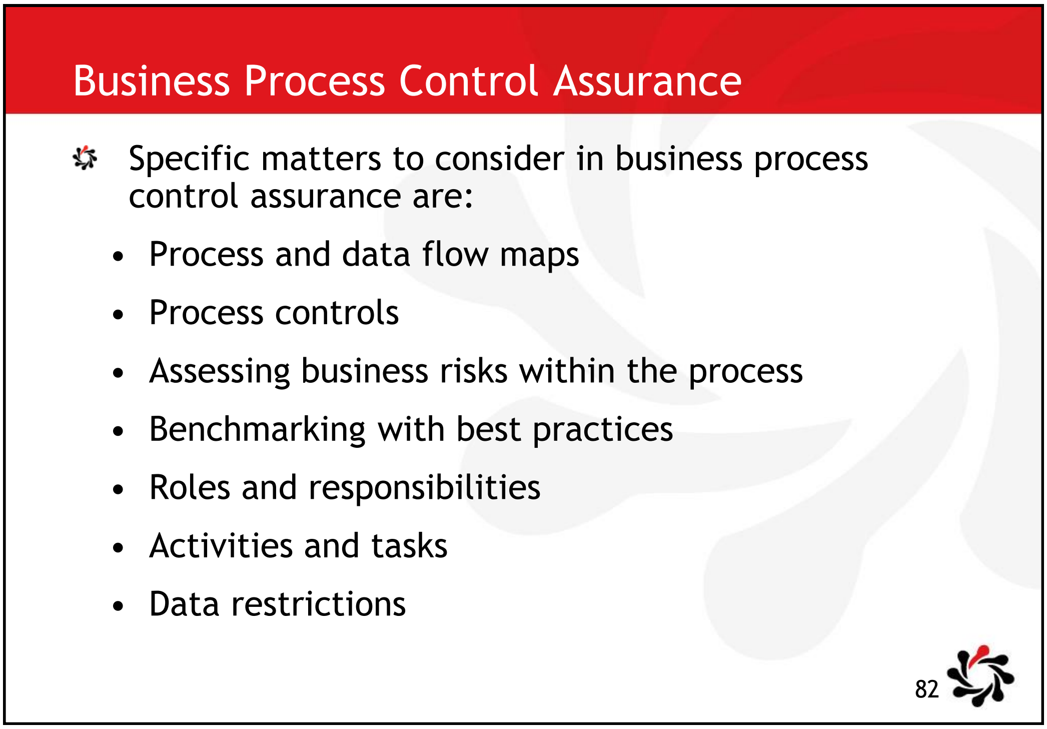
Output Controls

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



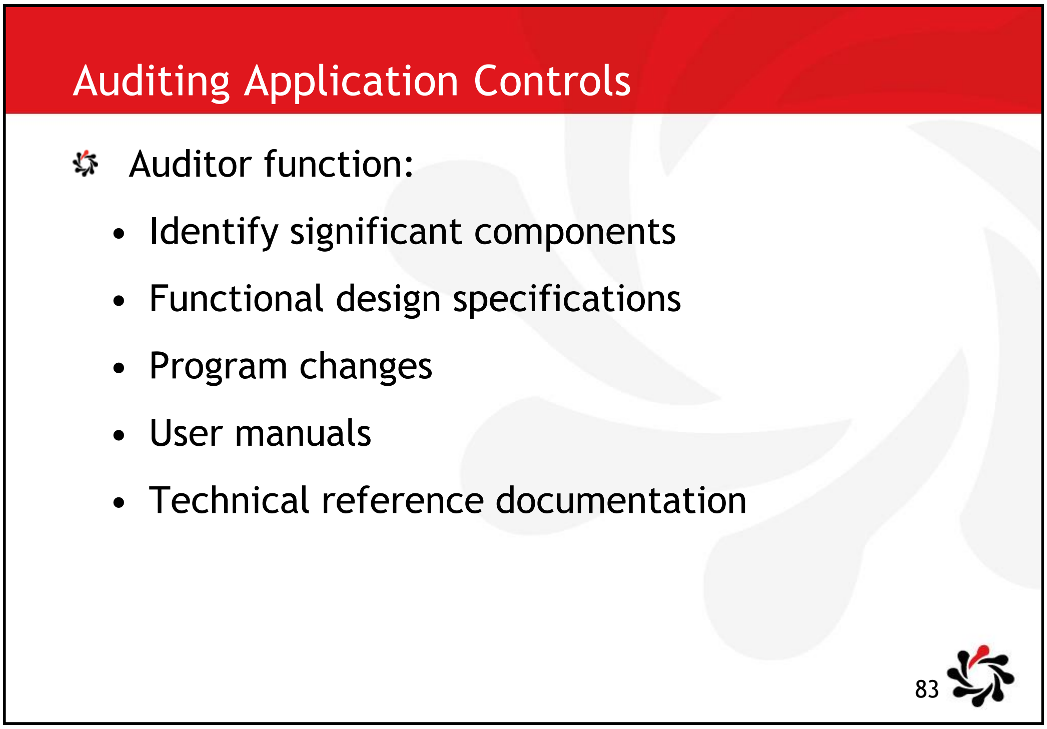
Types of Output Controls

- 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



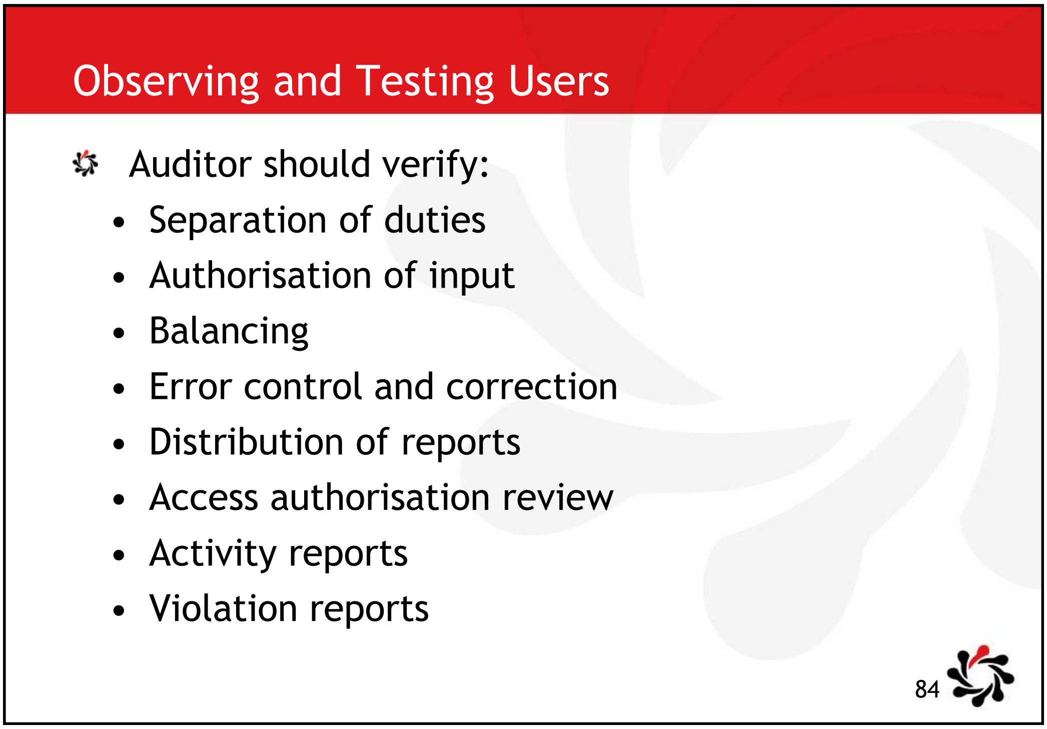
Business Process Control Assurance

- Specific matters to consider in business process control assurance are:
  - Process and data flow maps
  - Process controls
  - Assessing business risks within the process
  - Benchmarking with best practices
  - Roles and responsibilities
  - Activities and tasks
  - Data restrictions



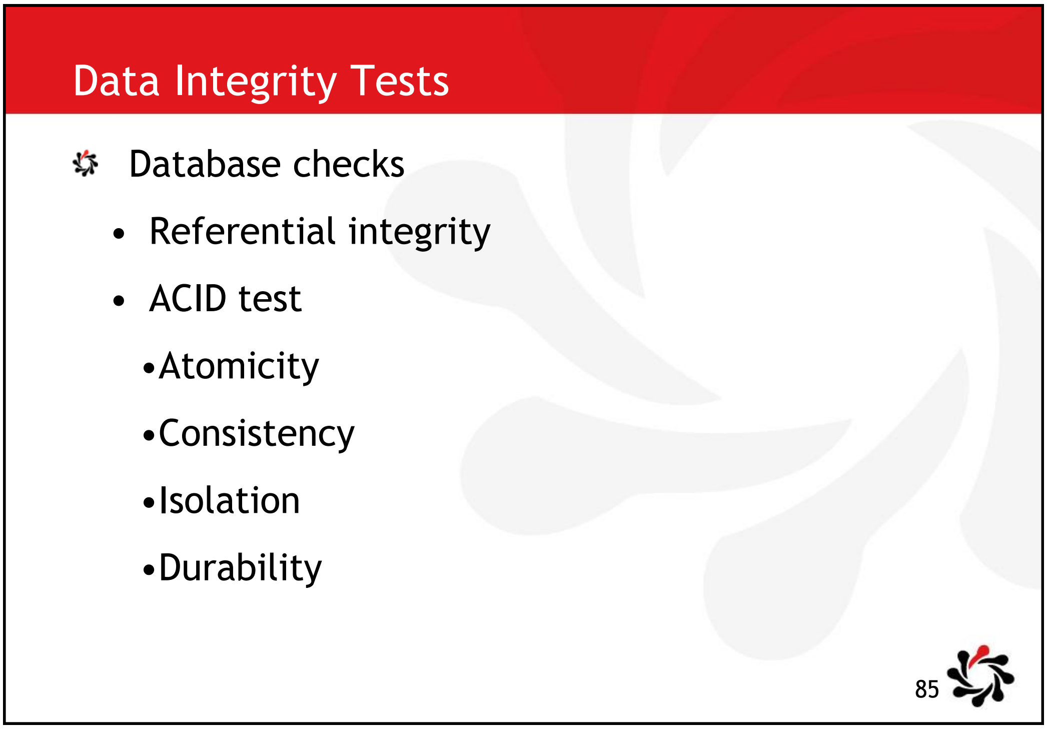
Auditing Application Controls

- Auditor function:
  - Identify significant components
  - Functional design specifications
  - Program changes
  - User manuals
  - Technical reference documentation



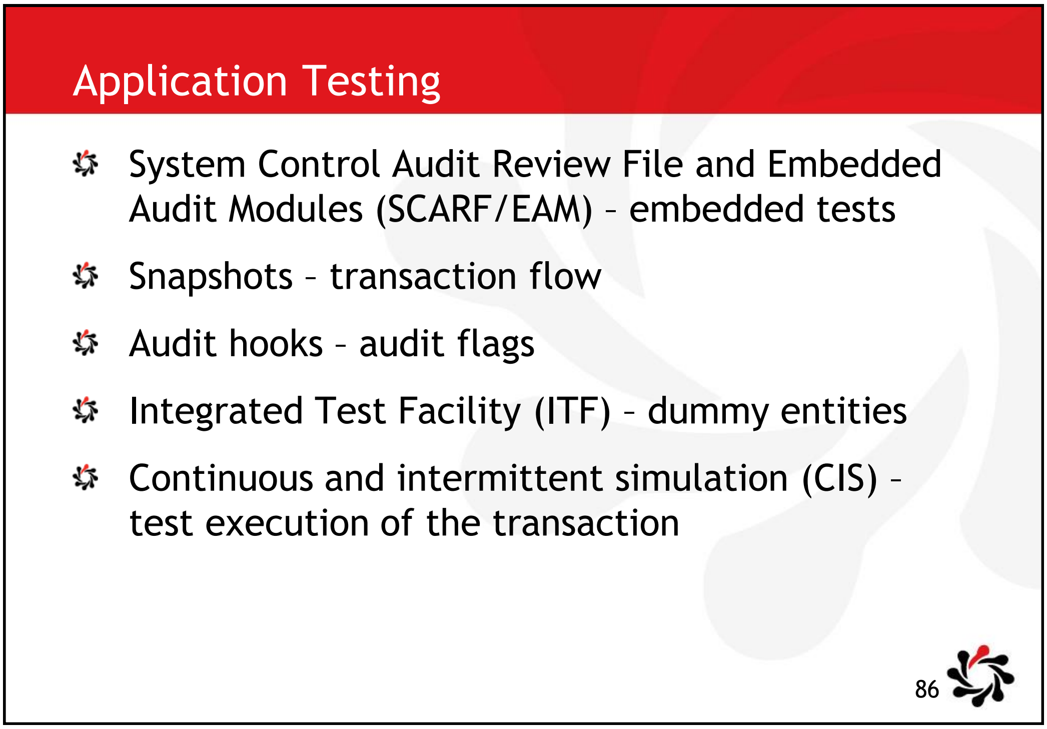
Observing and Testing Users

- Auditor should verify:
  - Separation of duties
  - Authorisation of input
  - Balancing
  - Error control and correction
  - Distribution of reports
  - Access authorisation review
  - Activity reports
  - Violation reports



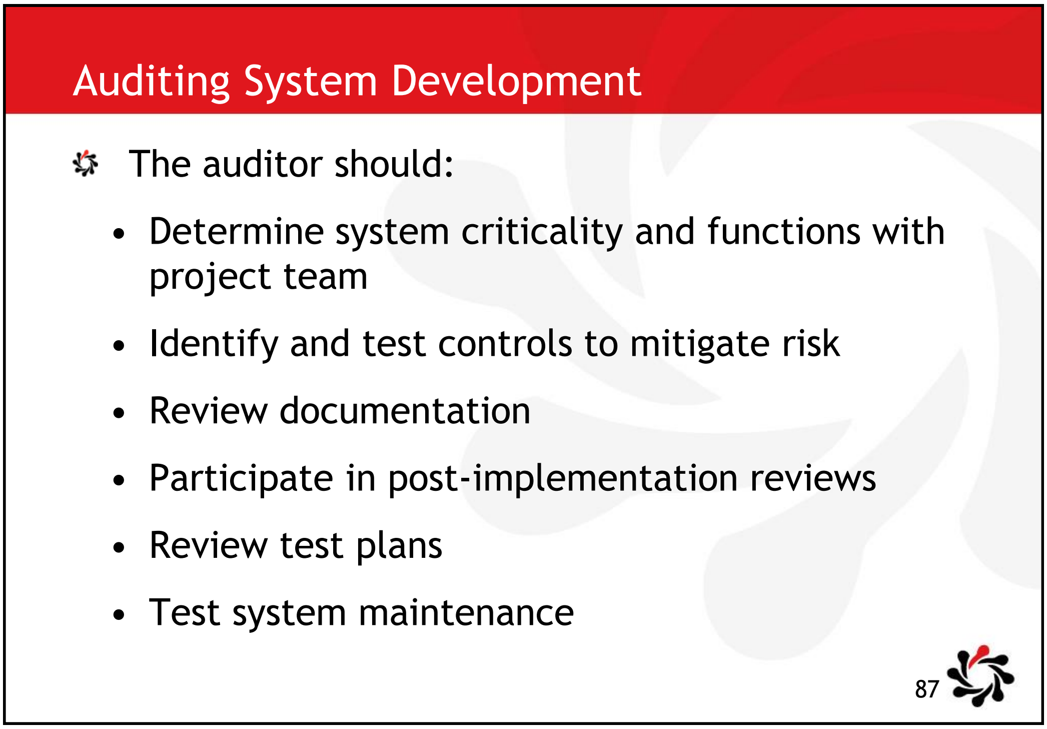
Data Integrity Tests

- Database checks
  - Referential integrity
  - ACID test
    - Atomicity
    - Consistency
    - Isolation
    - Durability



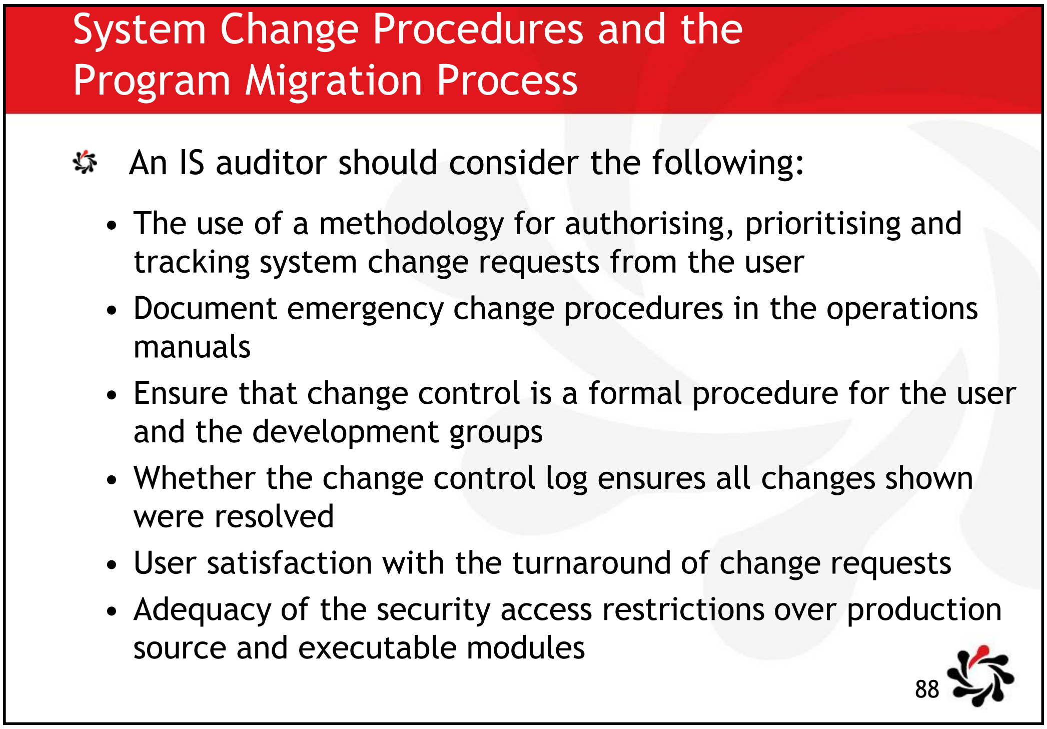
Application Testing

- System Control Audit Review File and Embedded Audit Modules (SCARF/EAM) – embedded tests
- Snapshots – transaction flow
- Audit hooks – audit flags
- Integrated Test Facility (ITF) – dummy entities
- Continuous and intermittent simulation (CIS) – test execution of the transaction



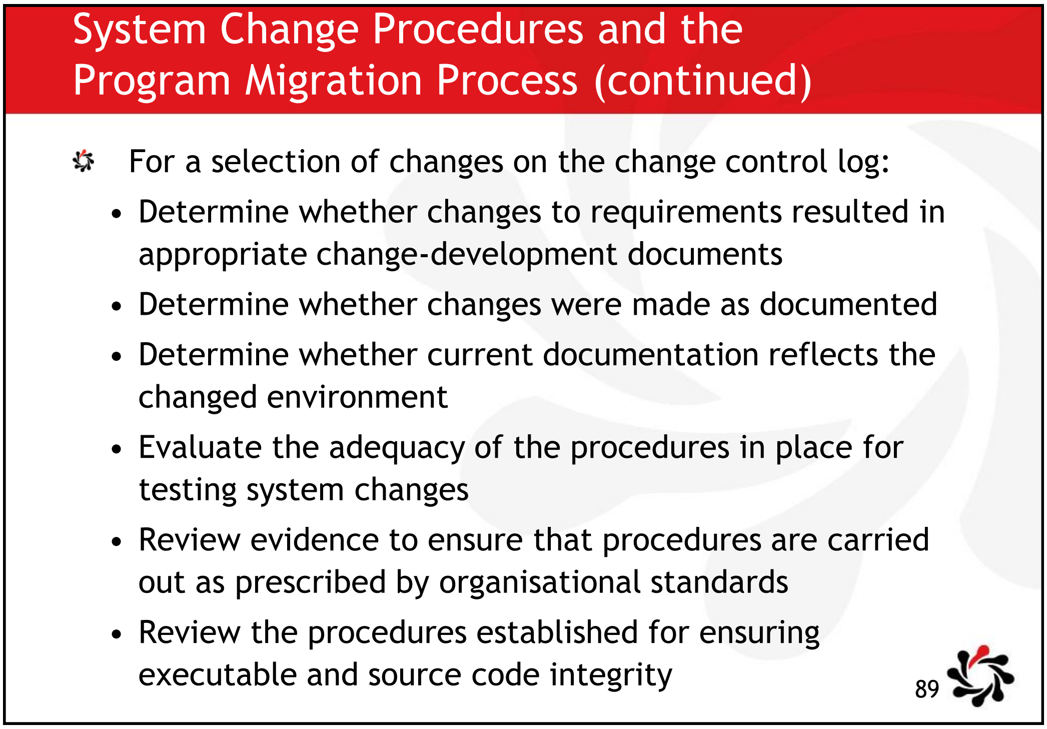
Auditing System Development

- The auditor should:
  - Determine system criticality and functions with project team
  - Identify and test controls to mitigate risk
  - Review documentation
  - Participate in post-implementation reviews
  - Review test plans
  - Test system maintenance



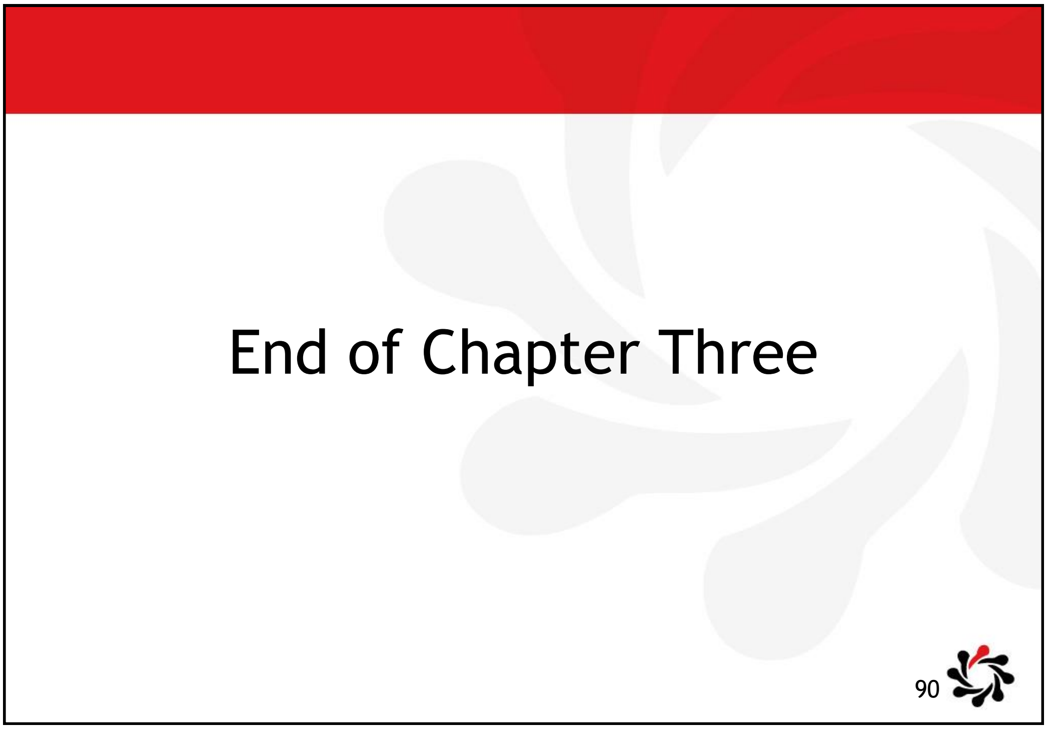
System Change Procedures and the Program Migration Process

- 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

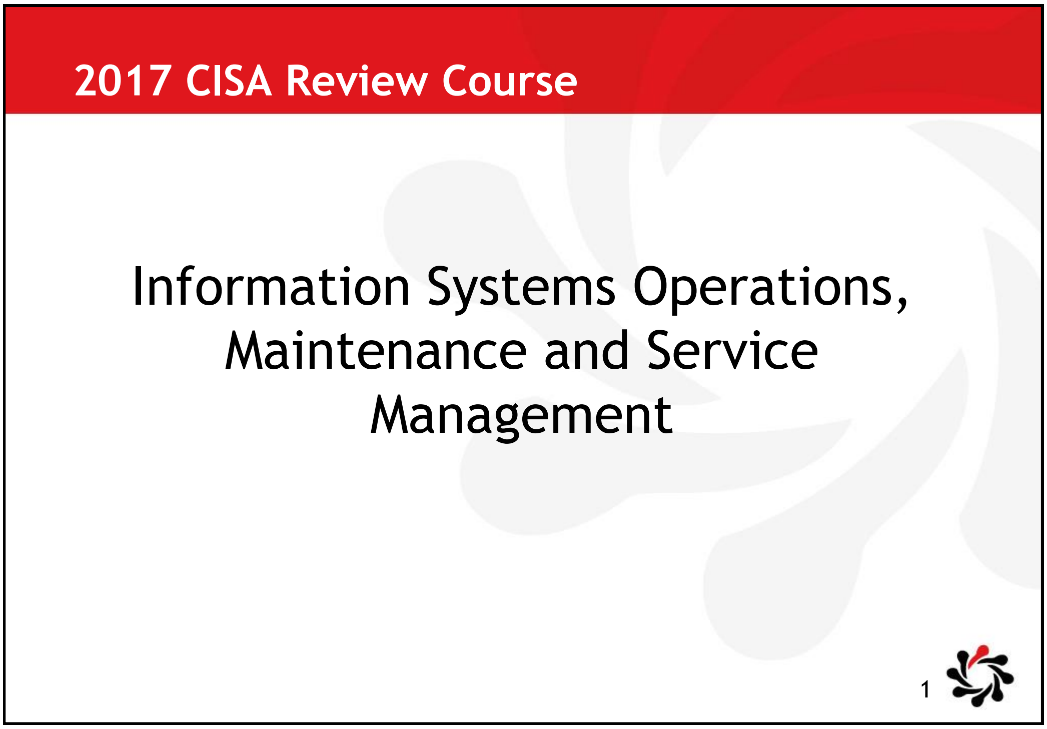


System Change Procedures and the Program Migration Process (continued)

- 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



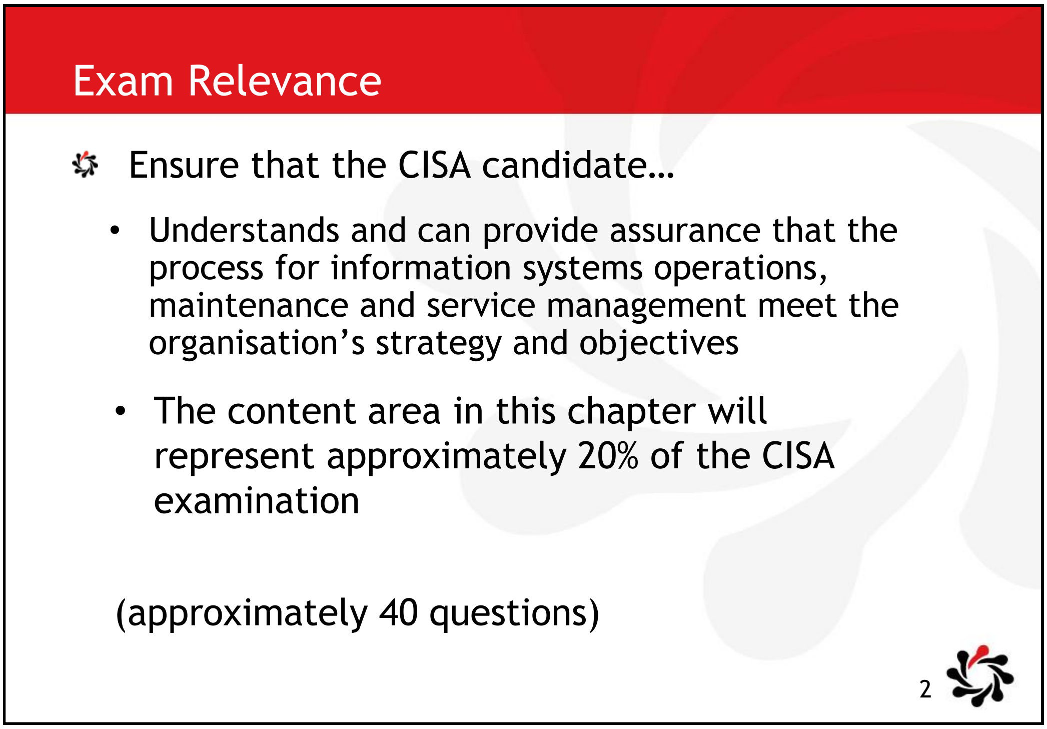
End of Chapter Three



2017 CISA Review Course

Information Systems Operations, Maintenance and Service Management

1

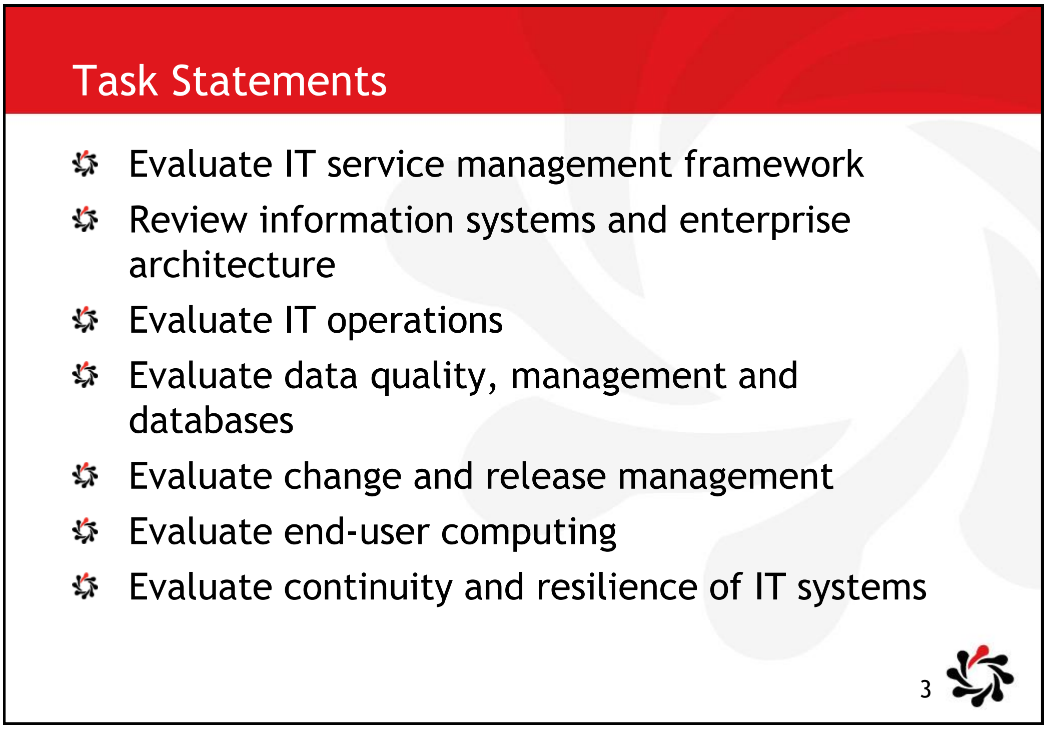


Exam Relevance

- Ensure that the CISA candidate…
  - Understands and can provide assurance that the process for information systems operations, maintenance and service management meet the organisation’s strategy and objectives
  - The content area in this chapter will represent approximately 20% of the CISA examination

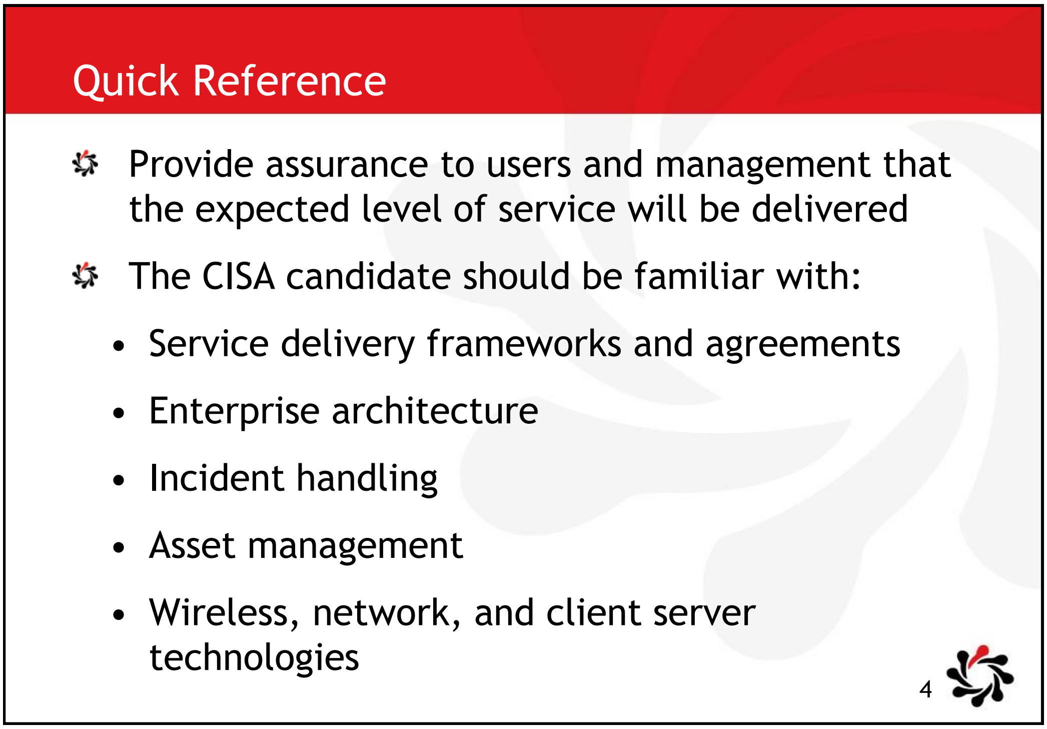
(approximately 40 questions)

2



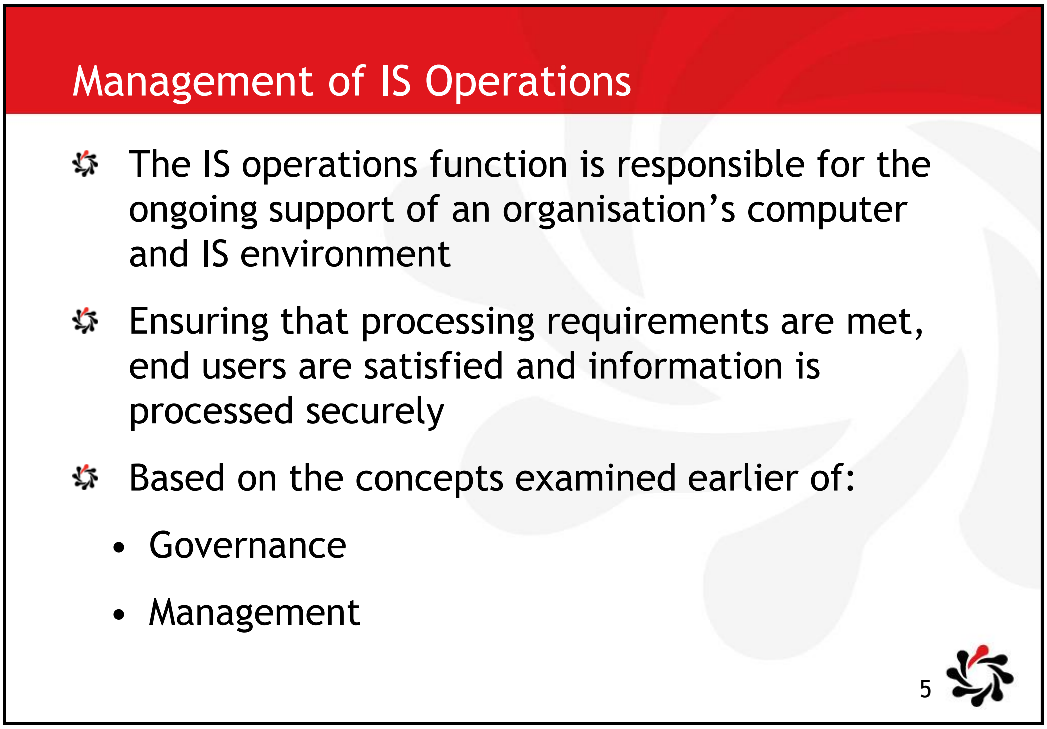
Task Statements

- Evaluate IT service management framework
- Review information systems and enterprise architecture
- Evaluate IT operations
- Evaluate data quality, management and databases
- Evaluate change and release management
- Evaluate end-user computing
- Evaluate continuity and resilience of IT systems



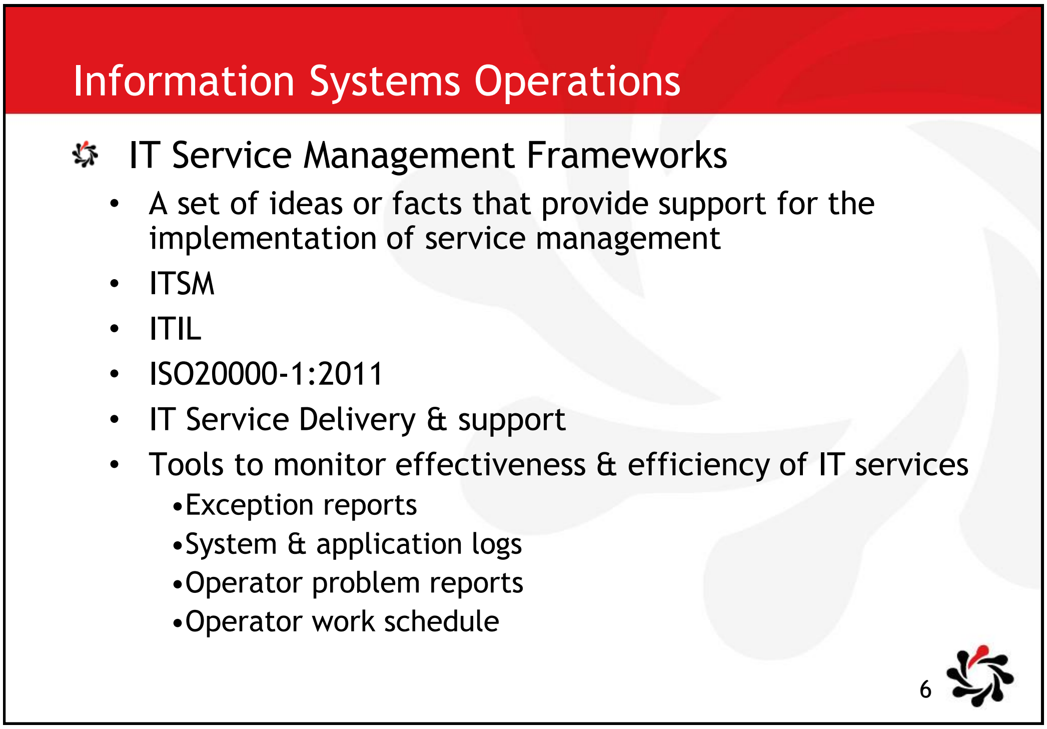
Quick Reference

- Provide assurance to users and management that the expected level of service will be delivered
- The CISA candidate should be familiar with:
  - Service delivery frameworks and agreements
  - Enterprise architecture
  - Incident handling
  - Asset management
  - Wireless, network, and client server technologies



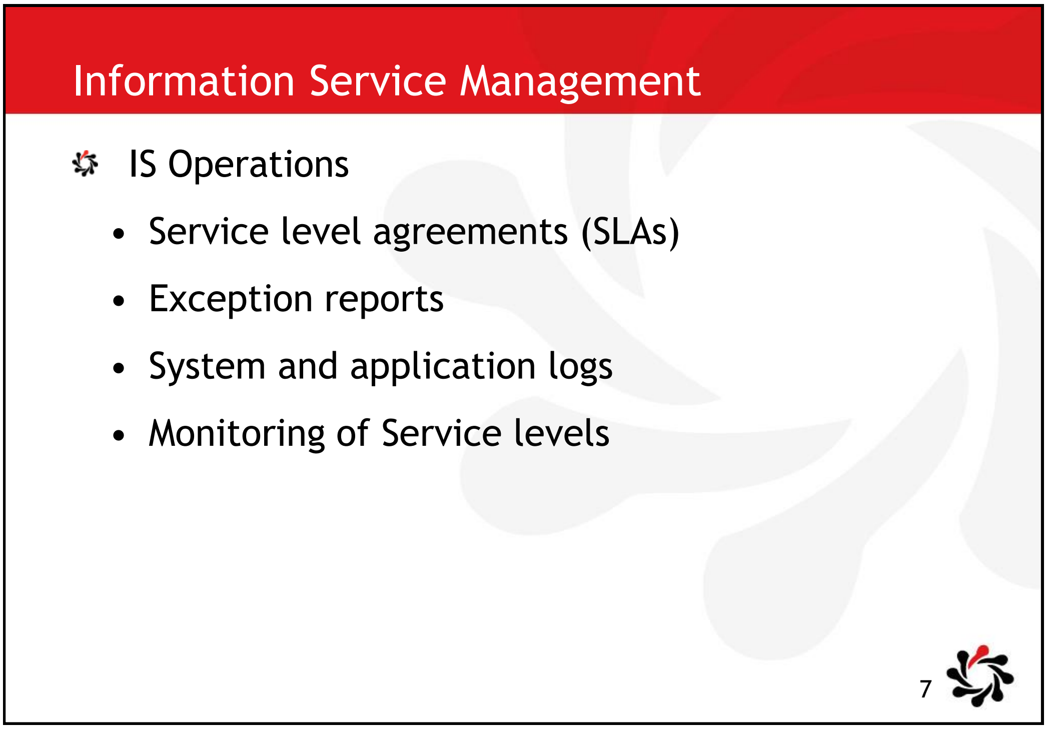
Management of IS Operations

- The IS operations function is responsible for the ongoing support of an organisation's computer and IS environment
- Ensuring that processing requirements are met, end users are satisfied and information is processed securely
- Based on the concepts examined earlier of:
  - Governance
  - Management



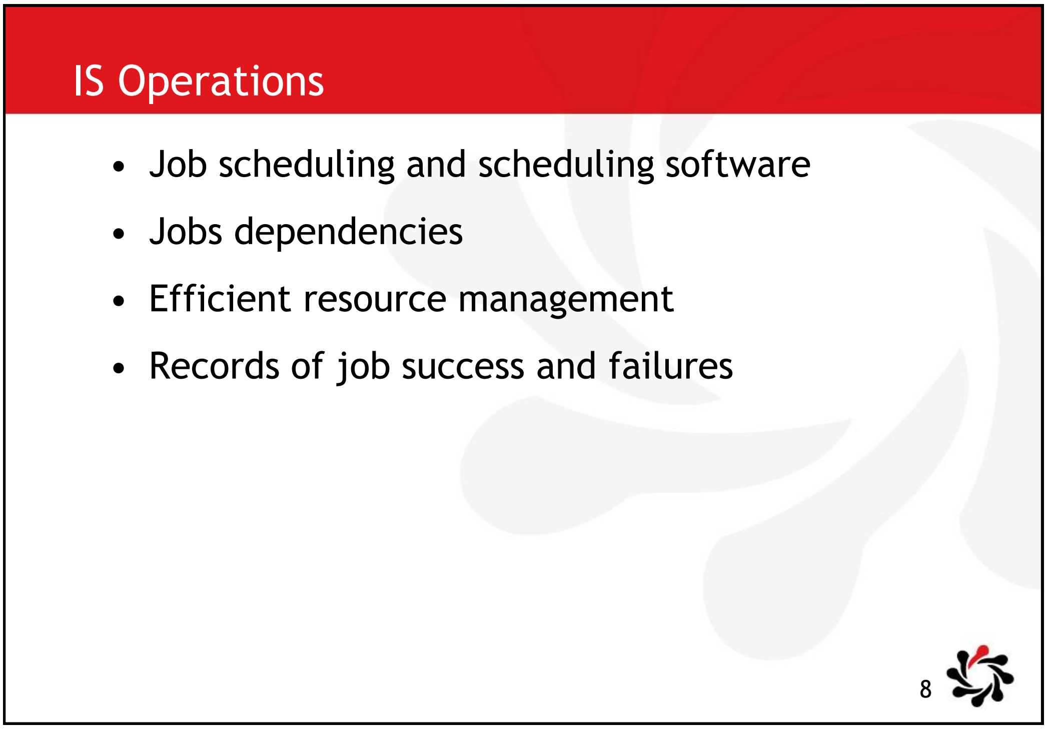
Information Systems Operations

- 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



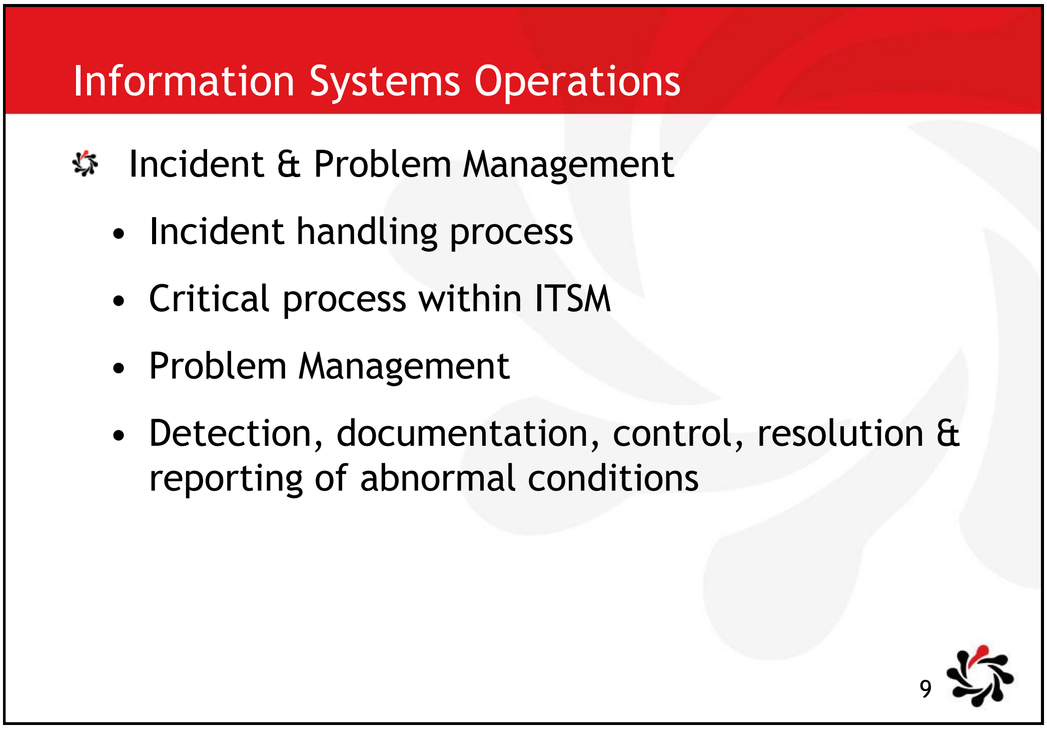
Information Service Management

- IS Operations
  - Service level agreements (SLAs)
  - Exception reports
  - System and application logs
  - Monitoring of Service levels



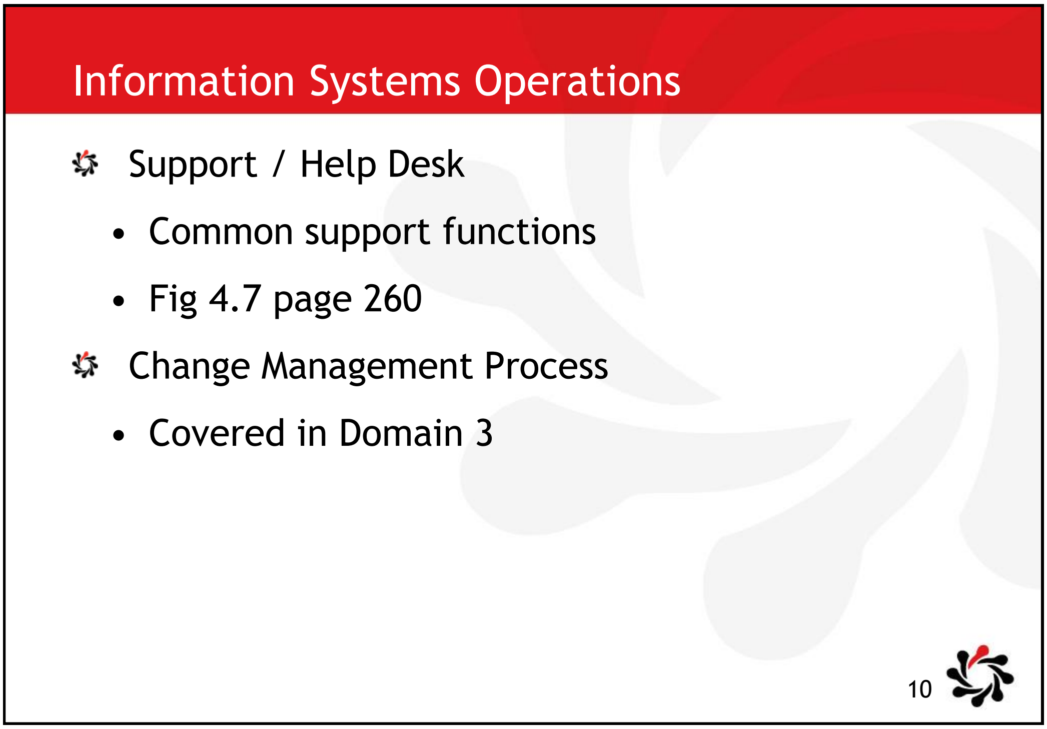
IS Operations

- Job scheduling and scheduling software
- Jobs dependencies
- Efficient resource management
- Records of job success and failures



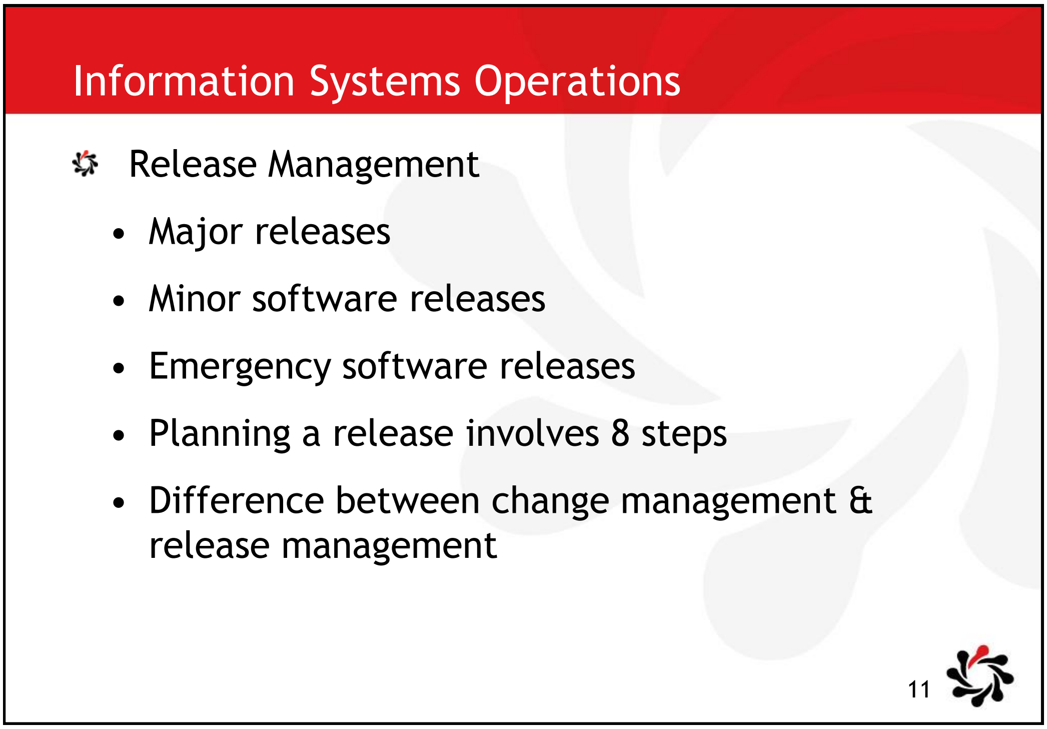
Information Systems Operations

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



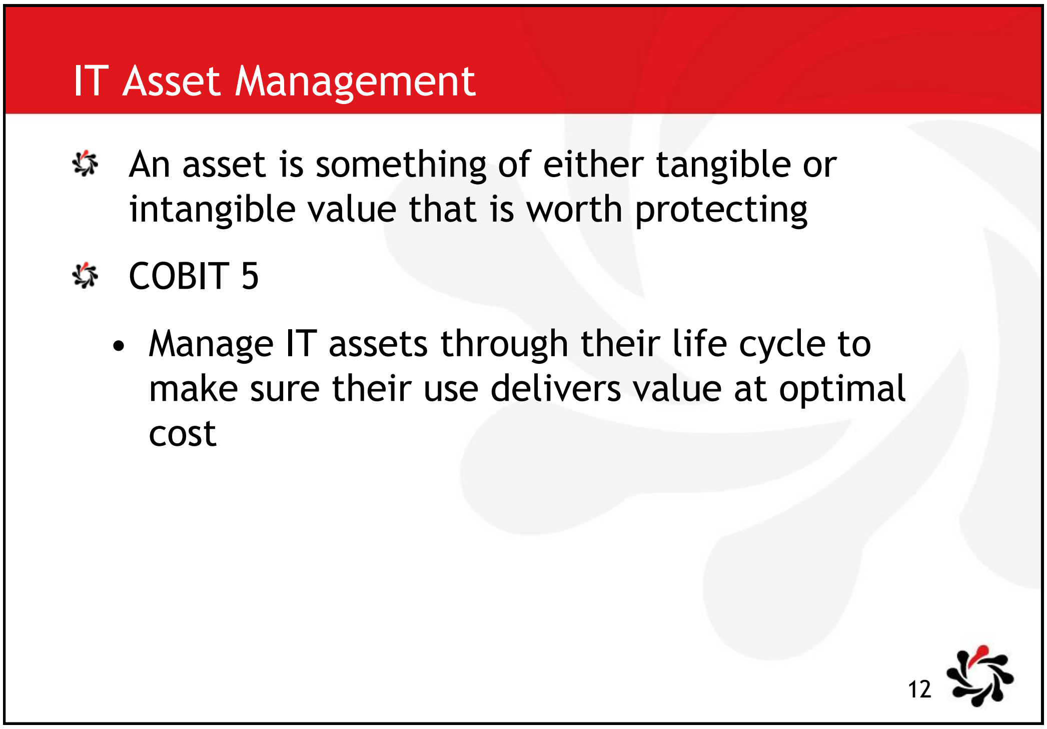
Information Systems Operations

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



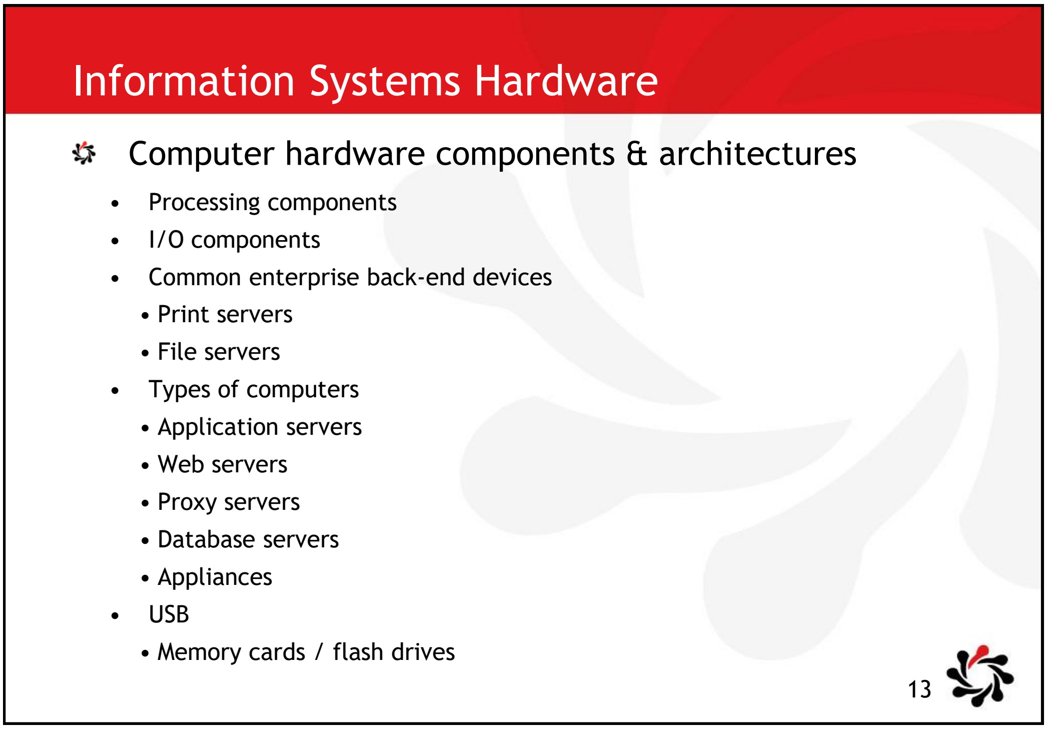
Information Systems Operations

- Release Management
  - Major releases
  - Minor software releases
  - Emergency software releases
  - Planning a release involves 8 steps
  - Difference between change management & release management



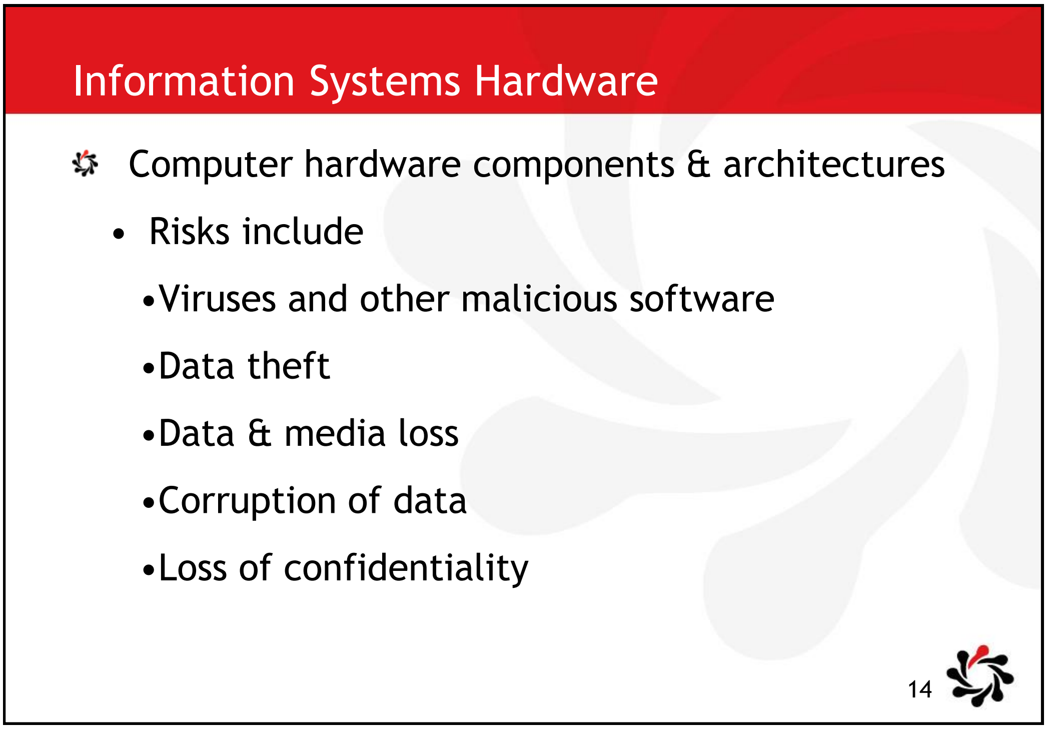
IT Asset Management

- 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



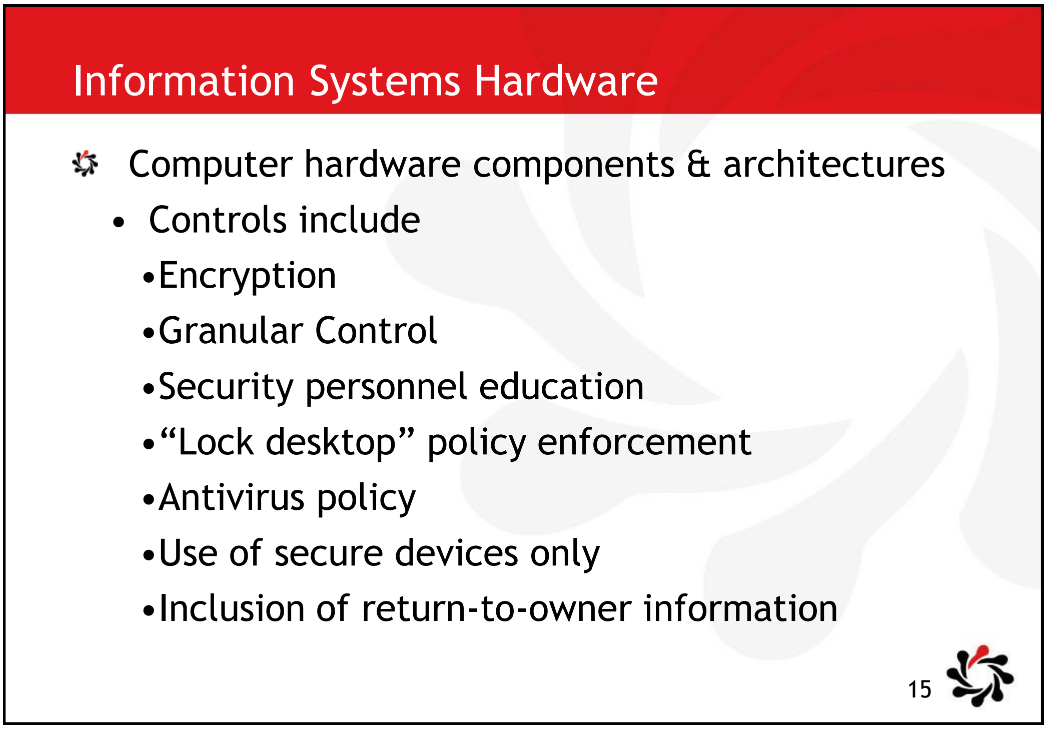
Information Systems Hardware

- 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

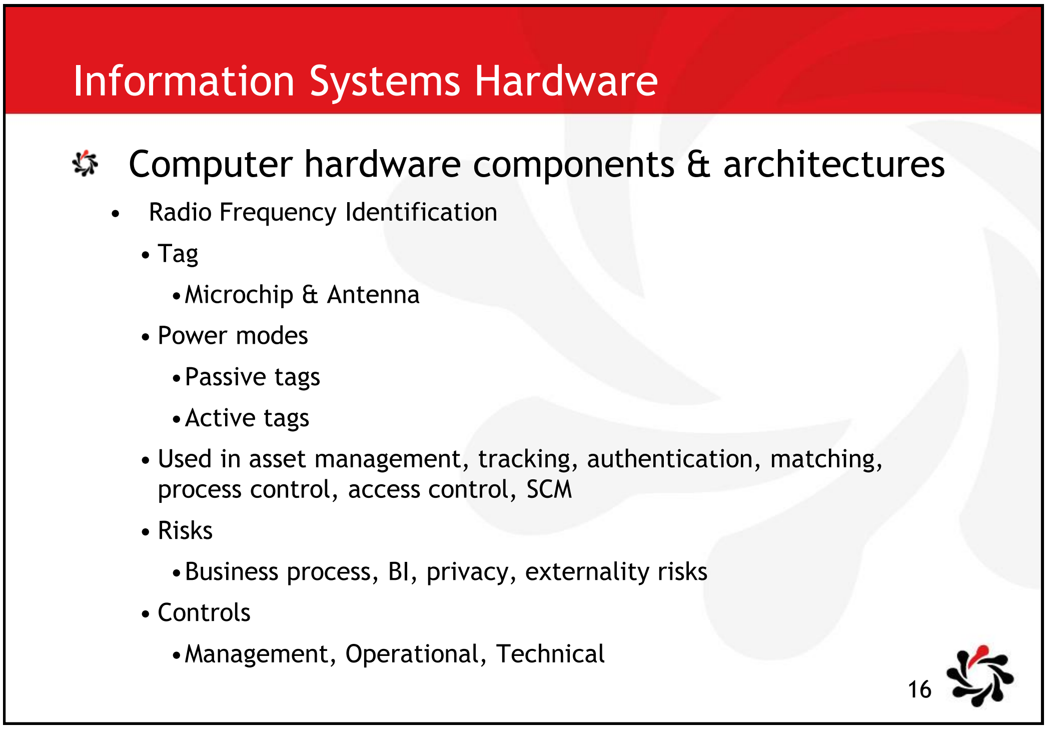
- Computer hardware components & architectures
  - Risks include
    - Viruses and other malicious software
    - Data theft
    - Data & media loss
    - Corruption of data
    - Loss of confidentiality



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

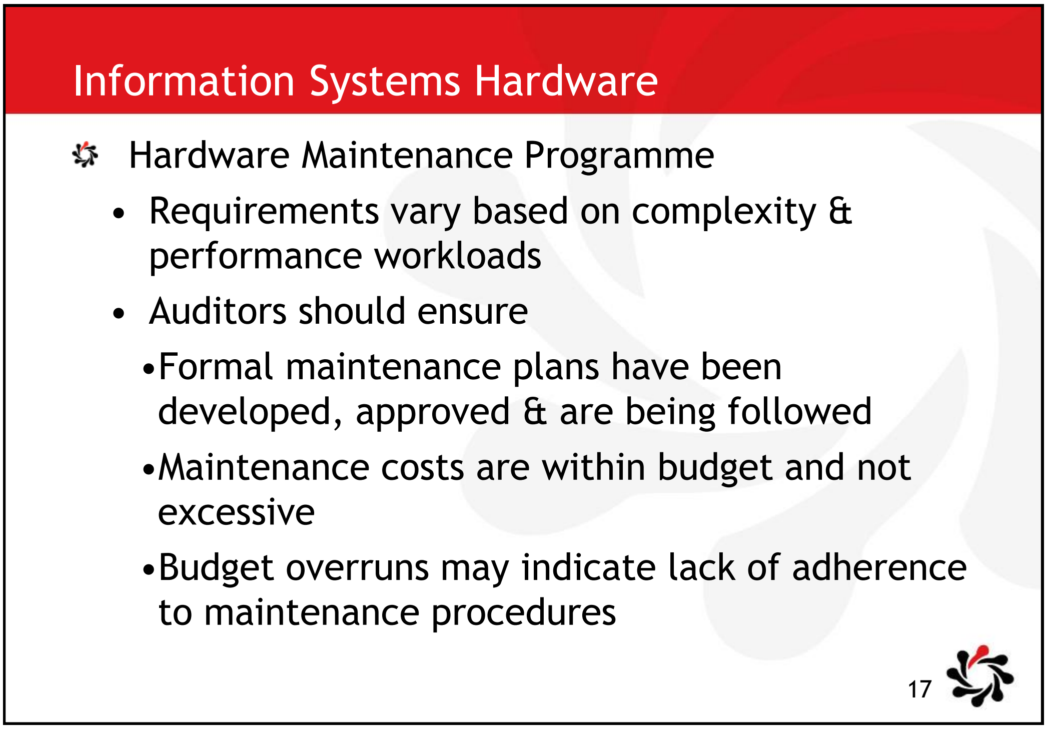
15



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

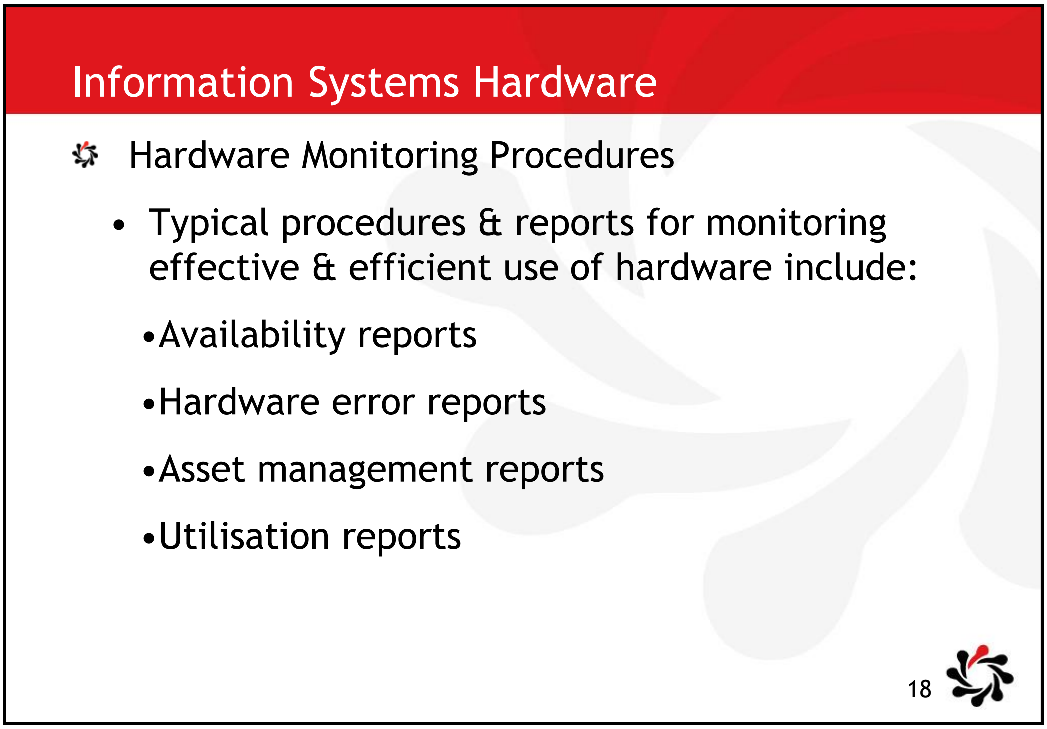
16



Information Systems Hardware

- 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

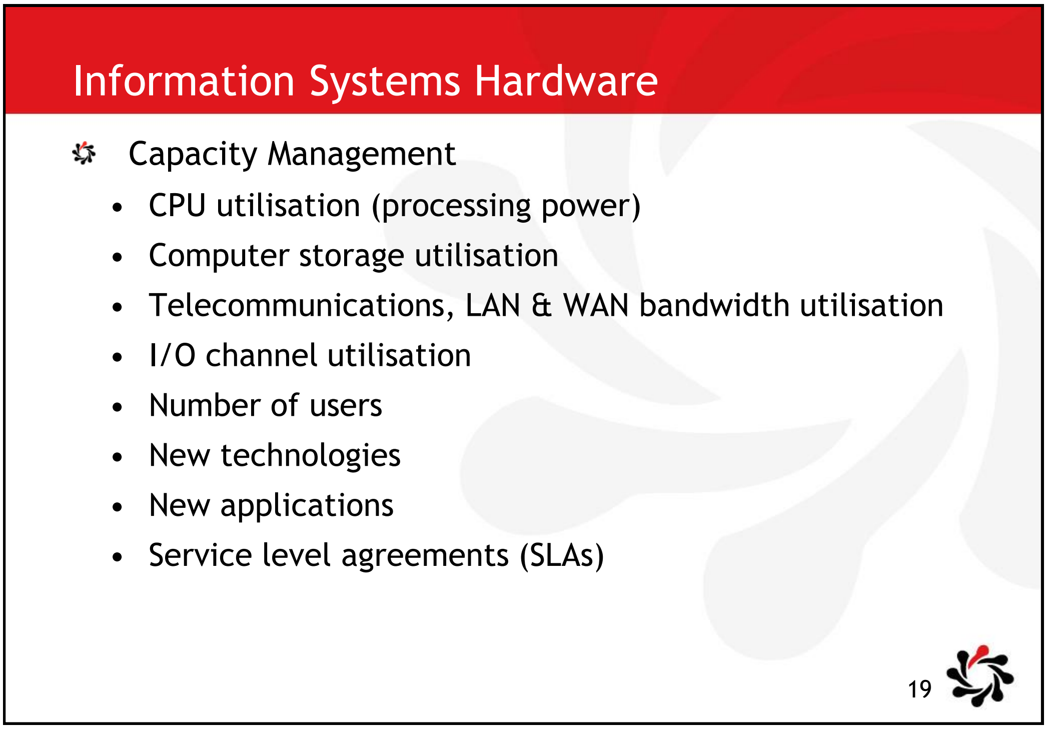
17



Information Systems Hardware

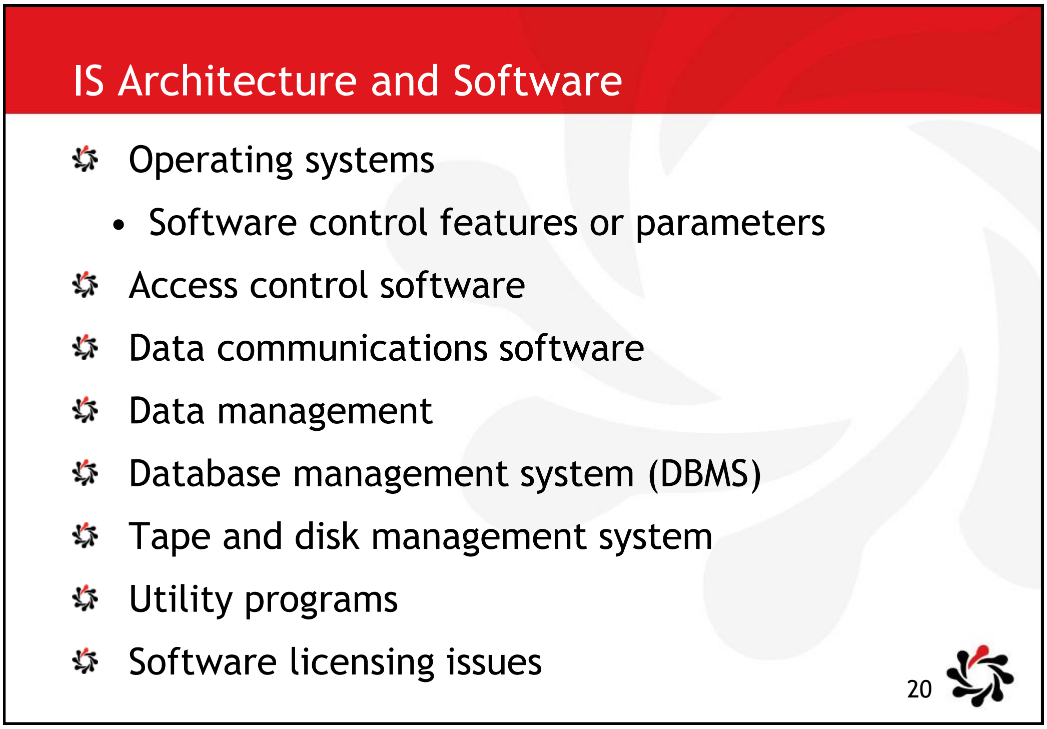
- Hardware Monitoring Procedures
  - Typical procedures & reports for monitoring effective & efficient use of hardware include:
    - Availability reports
    - Hardware error reports
    - Asset management reports
    - Utilisation reports

18



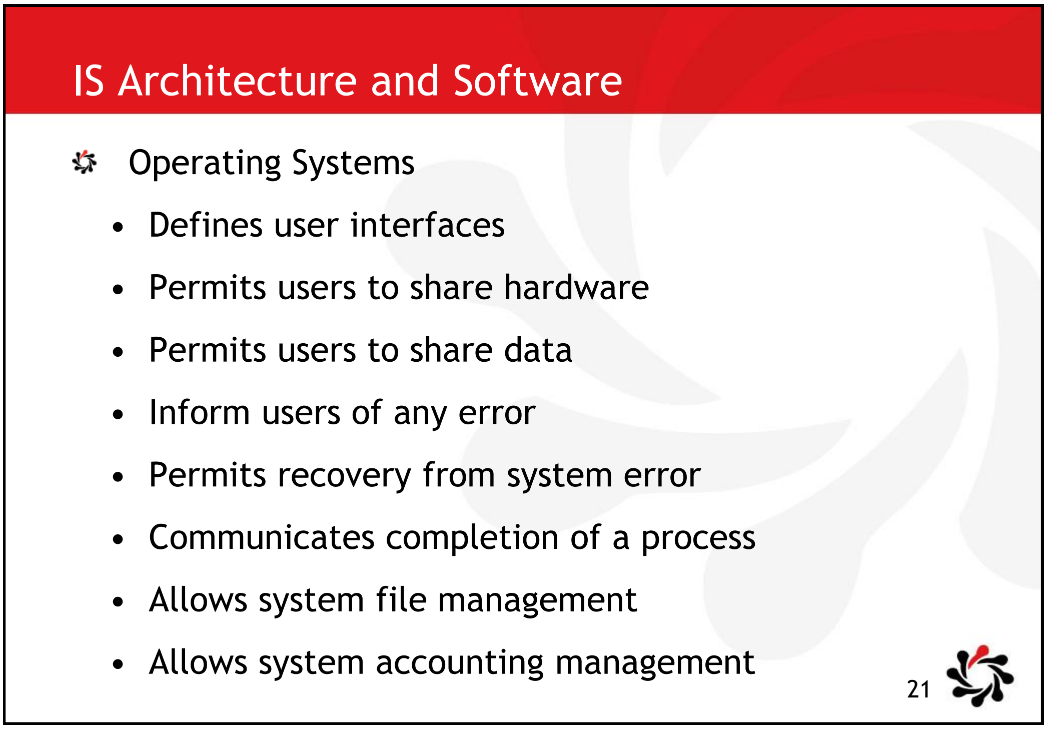
Information Systems Hardware

- Capacity Management
  - CPU utilisation (processing power)
  - Computer storage utilisation
  - Telecommunications, LAN & WAN bandwidth utilisation
  - I/O channel utilisation
  - Number of users
  - New technologies
  - New applications
  - Service level agreements (SLAs)



IS Architecture and Software

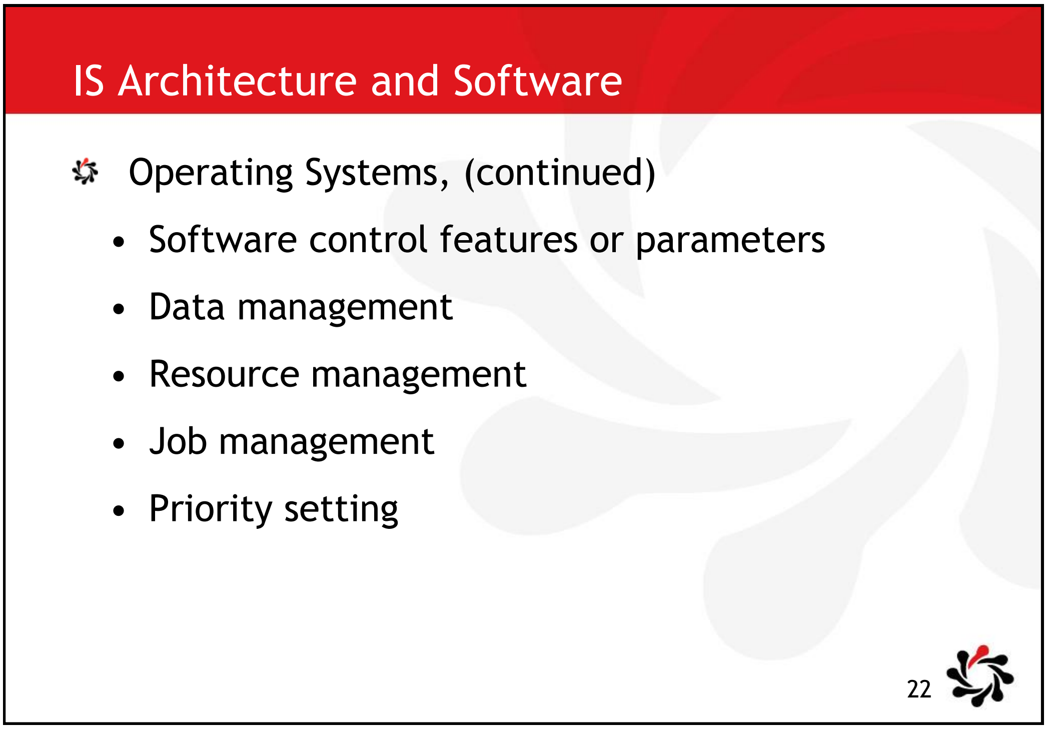
- Operating systems
  - Software control features or parameters
- Access control software
- Data communications software
- Data management
- Database management system (DBMS)
- Tape and disk management system
- Utility programs
- Software licensing issues



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

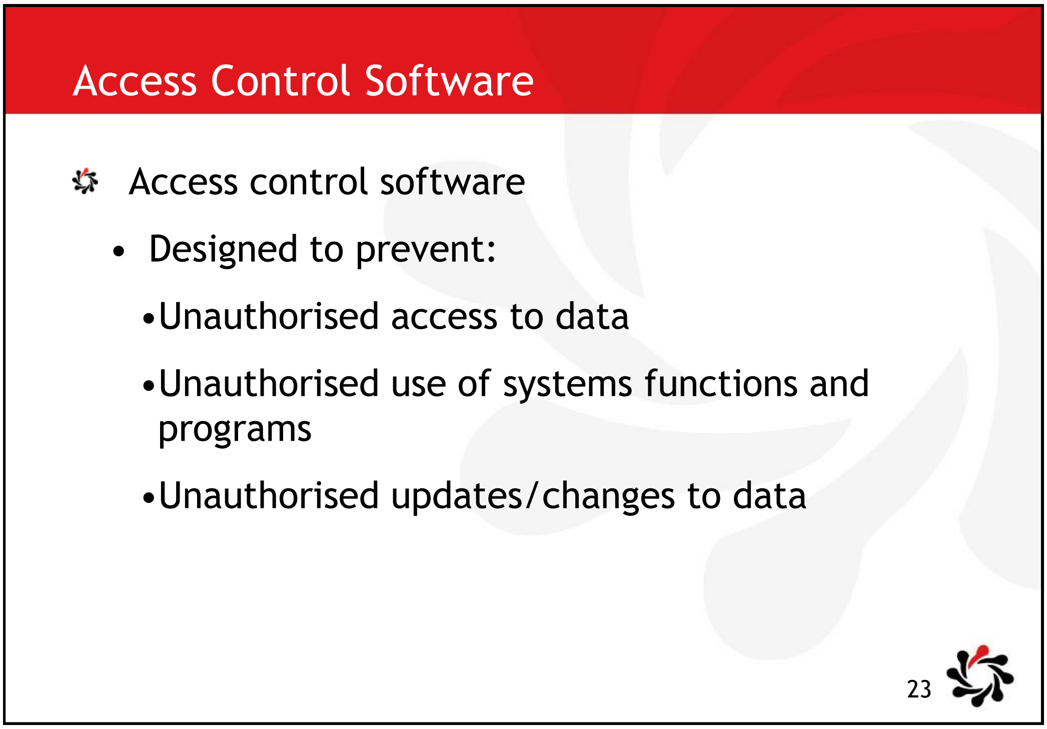
21



IS Architecture and Software

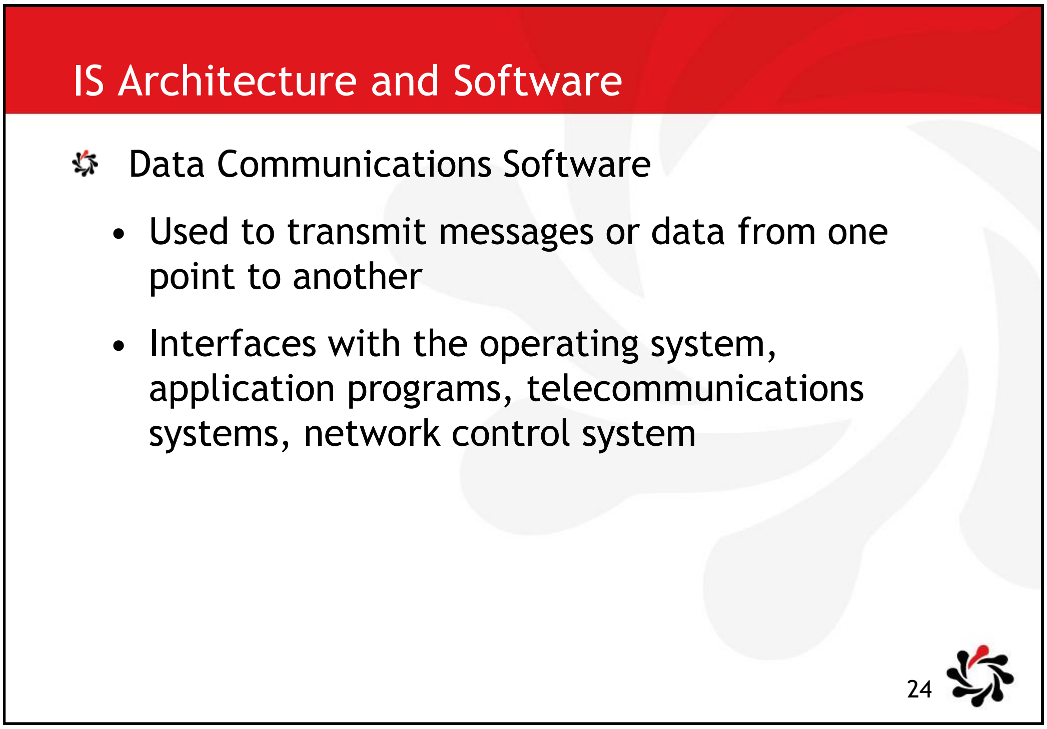
- Operating Systems, (continued)
  - Software control features or parameters
  - Data management
  - Resource management
  - Job management
  - Priority setting

22



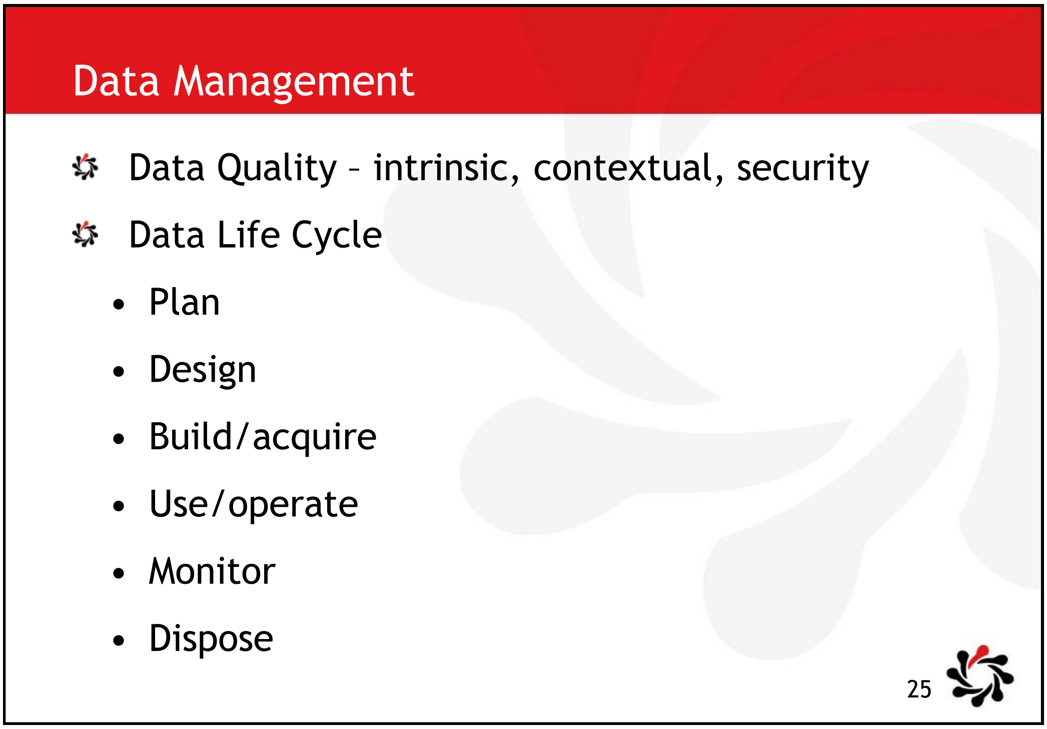
Access Control Software

- Access control software
  - Designed to prevent:
    - Unauthorised access to data
    - Unauthorised use of systems functions and programs
    - Unauthorised updates/changes to data



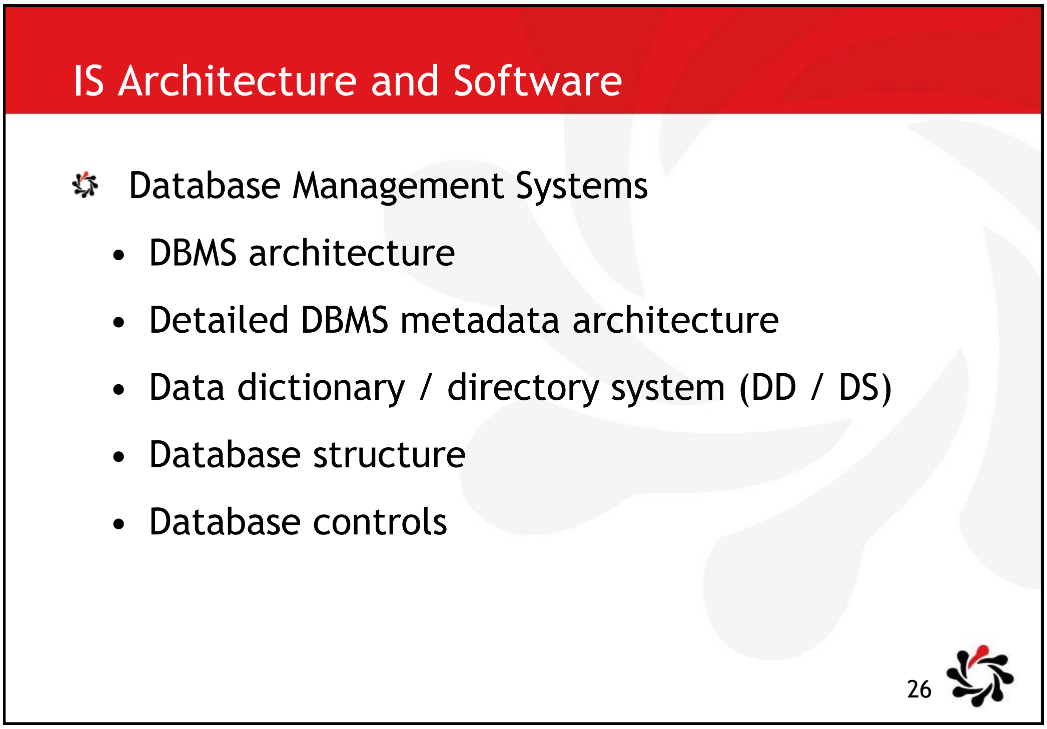
IS Architecture and Software

- 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



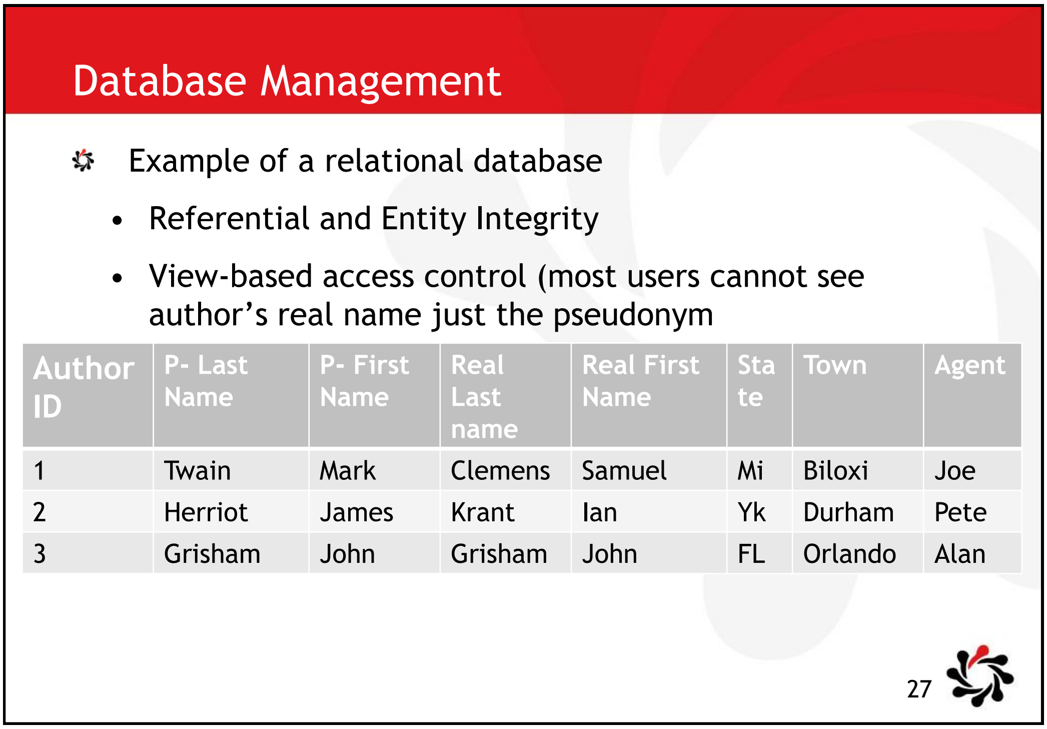
Data Management

- Data Quality – intrinsic, contextual, security
- Data Life Cycle
  - Plan
  - Design
  - Build/acquire
  - Use/operate
  - Monitor
  - Dispose



IS Architecture and Software

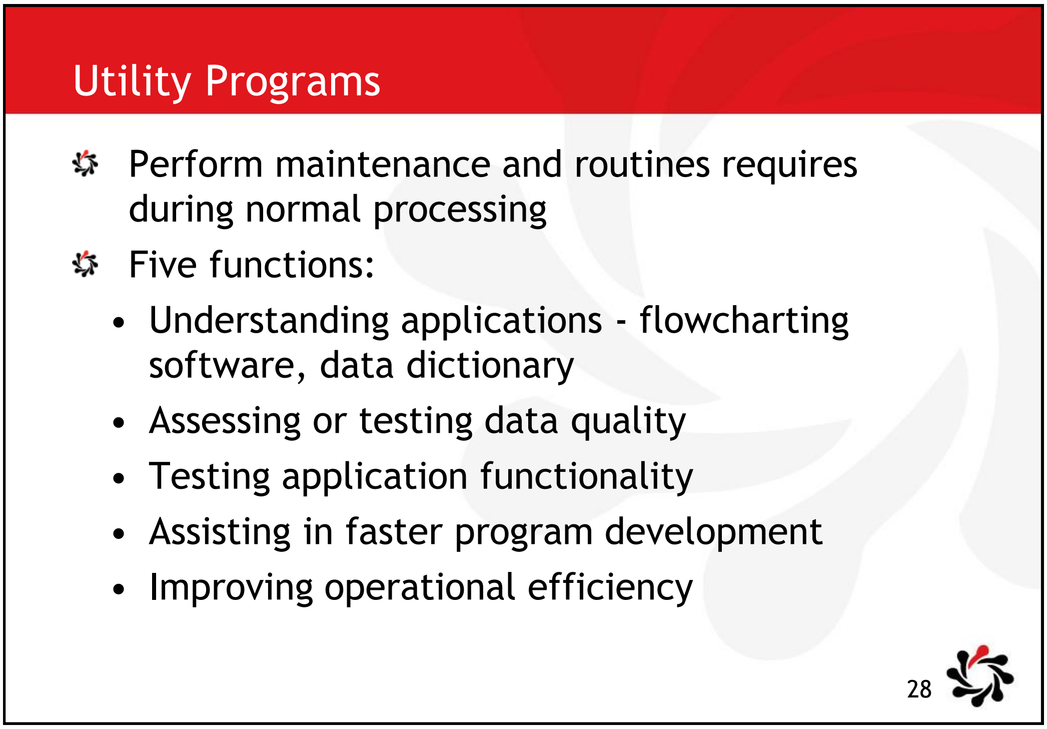
- Database Management Systems
  - DBMS architecture
  - Detailed DBMS metadata architecture
  - Data dictionary / directory system (DD / DS)
  - Database structure
  - Database controls



Database Management

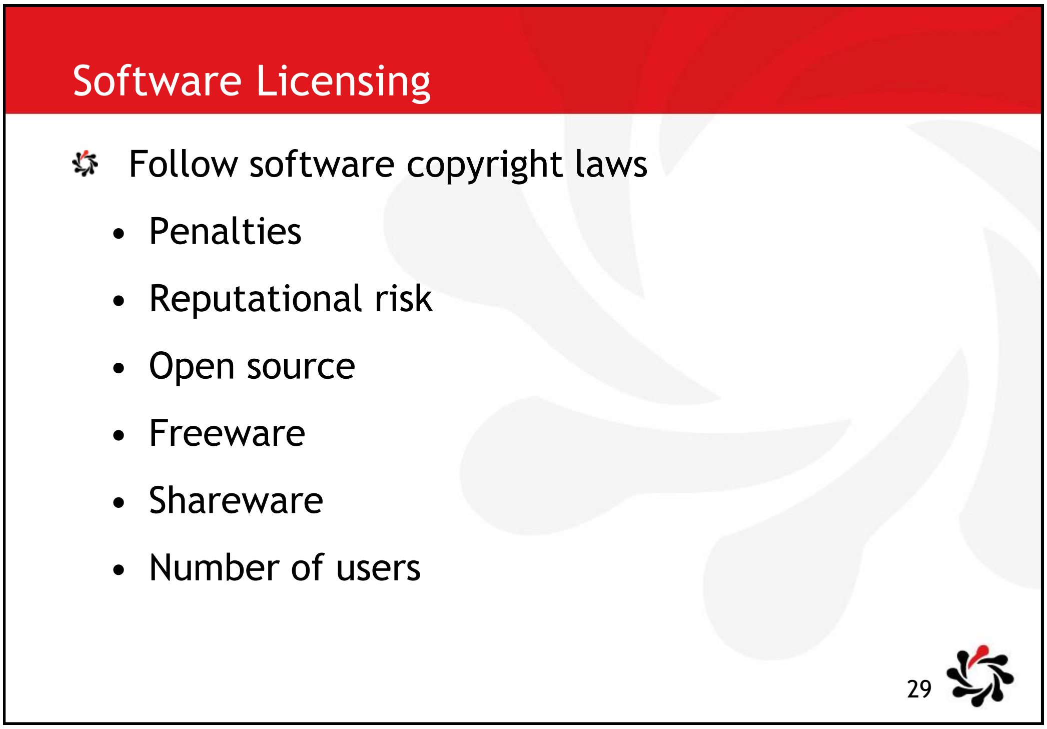
- Example of a relational database
  - Referential and Entity Integrity
  - View-based access control (most users cannot see author’s real name just the pseudonym

Author ID	P- Last Name	P- First Name	Real Last name	Real First Name	Sta te	Town	Agent
1	Twain	Mark	Clemens	Samuel	Mi	Biloxi	Joe
2	Herriot	James	Krant	Ian	Yk	Durham	Pete
3	Grisham	John	Grisham	John	FL	Orlando	Alan



Utility Programs

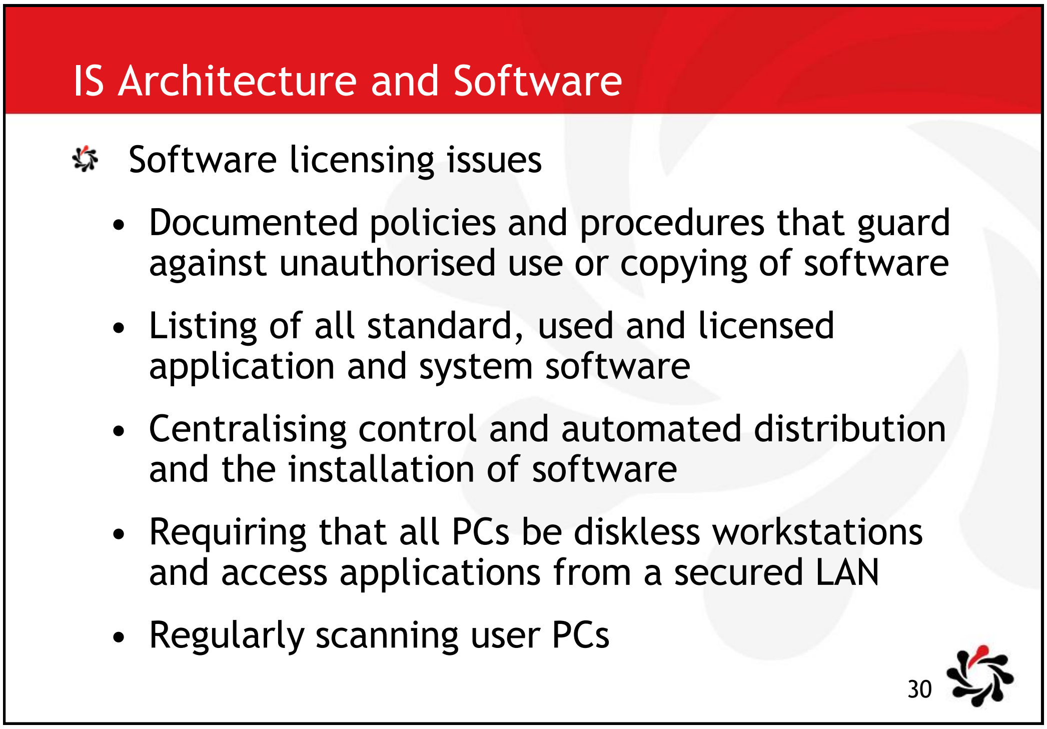
- Perform maintenance and routines requires during normal processing
- Five functions:
  - Understanding applications - flowcharting software, data dictionary
  - Assessing or testing data quality
  - Testing application functionality
  - Assisting in faster program development
  - Improving operational efficiency



Software Licensing

- Follow software copyright laws
  - Penalties
  - Reputational risk
  - Open source
  - Freeware
  - Shareware
  - Number of users

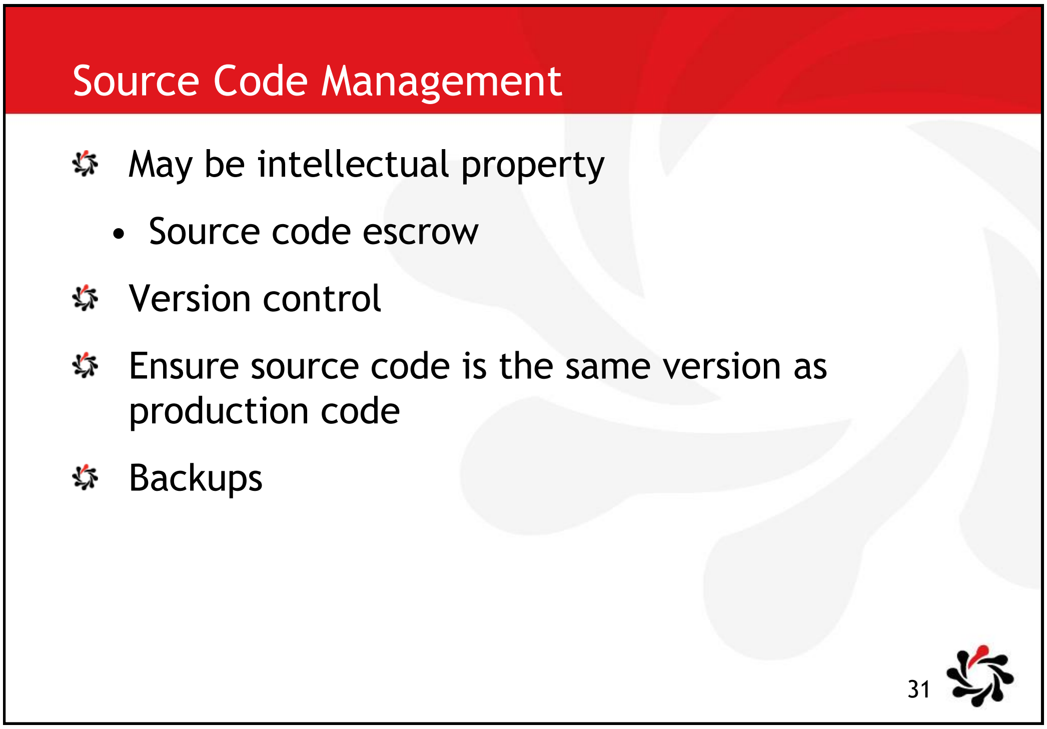
29



IS Architecture and Software

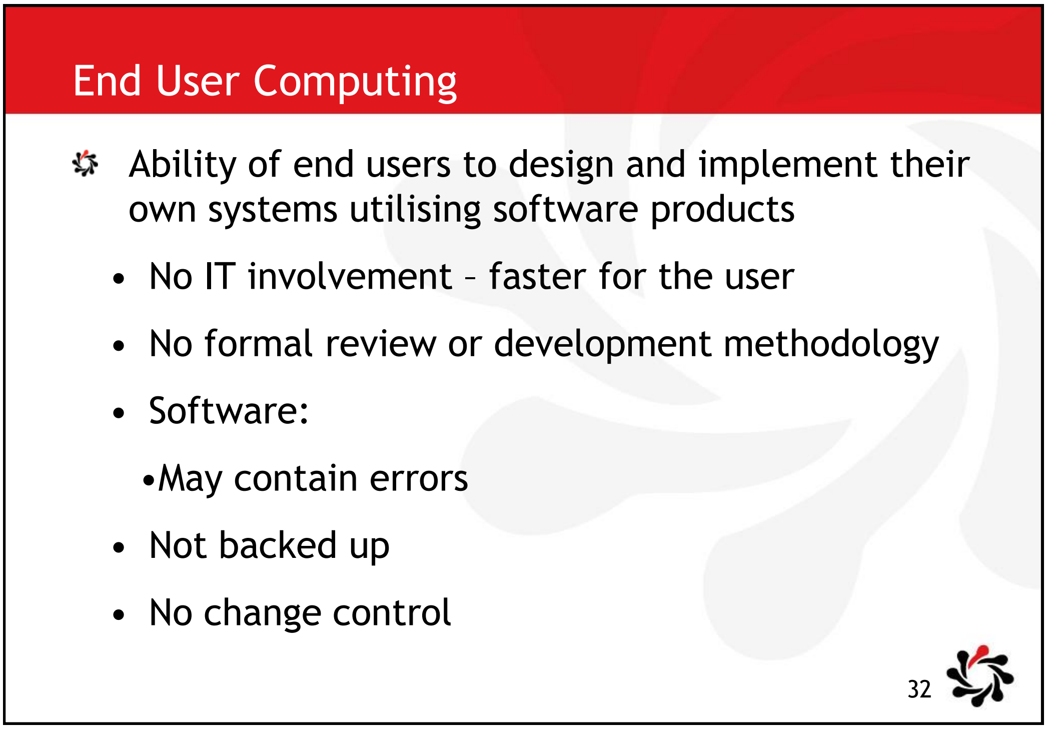
- Software licensing issues
  - Documented policies and procedures that guard against unauthorised use or copying of software
  - Listing of all standard, used and licensed application and system software
  - Centralising control and automated distribution and the installation of software
  - Requiring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

30



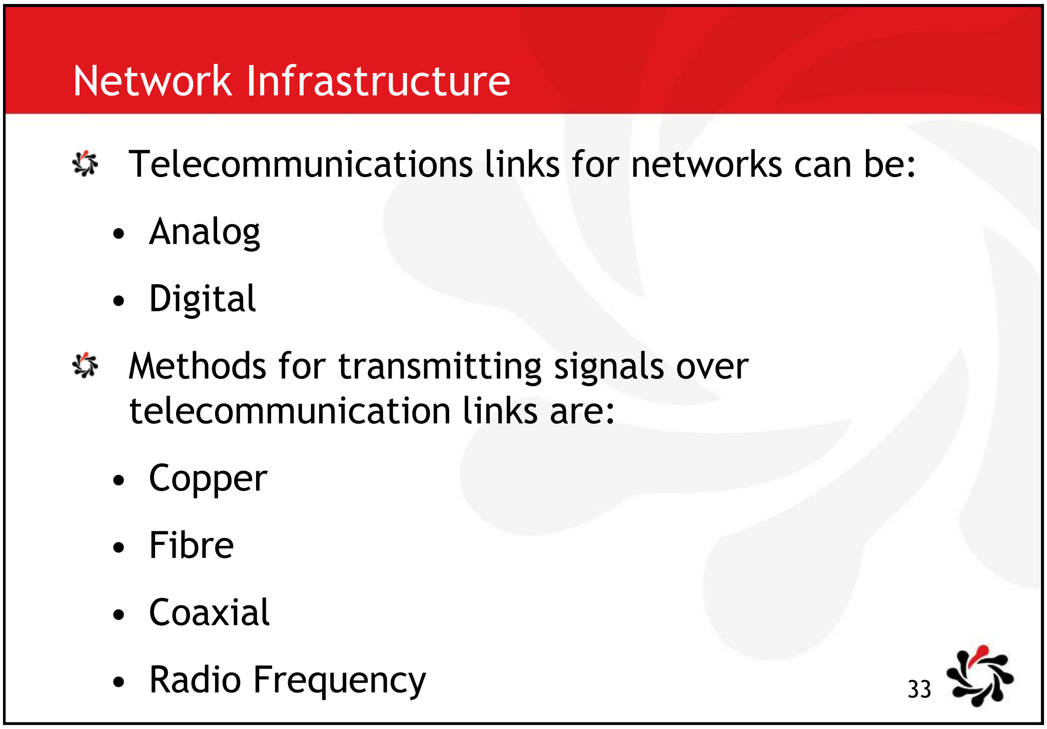
Source Code Management

- May be intellectual property
  - Source code escrow
- Version control
- Ensure source code is the same version as production code
- Backups



End User Computing

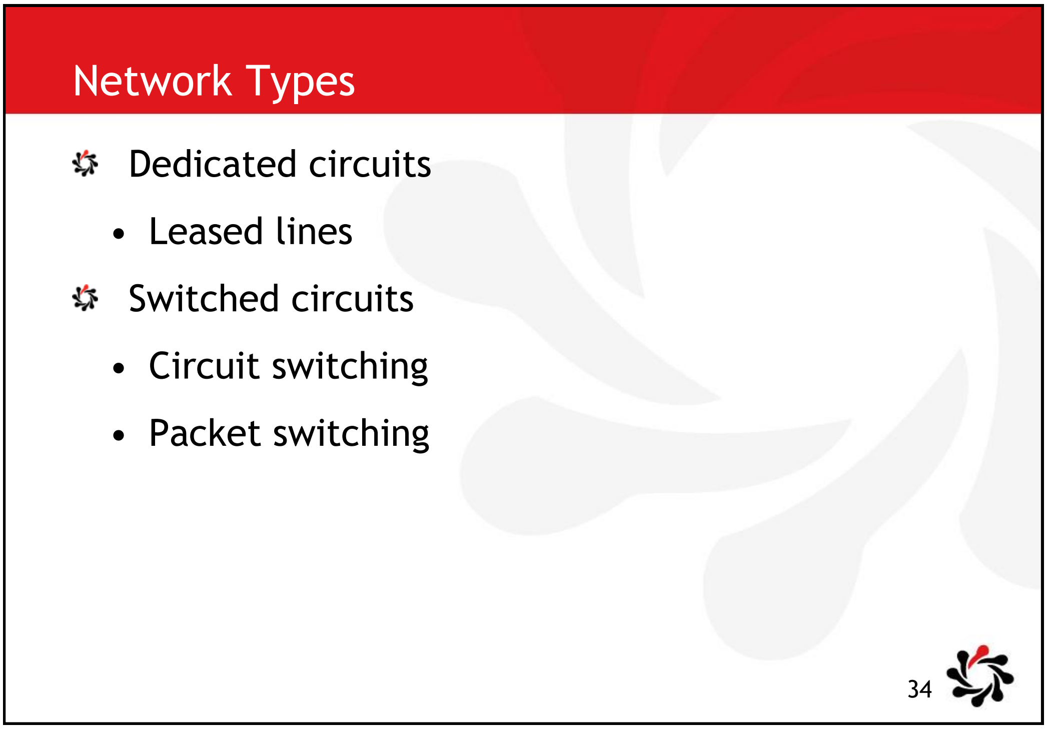
- Ability of end users to design and implement their own systems utilising software products
  - No IT involvement – faster for the user
  - No formal review or development methodology
  - Software:
    - May contain errors
  - Not backed up
  - No change control



Network Infrastructure

- Telecommunications links for networks can be:
  - Analog
  - Digital
- Methods for transmitting signals over telecommunication links are:
  - Copper
  - Fibre
  - Coaxial
  - Radio Frequency

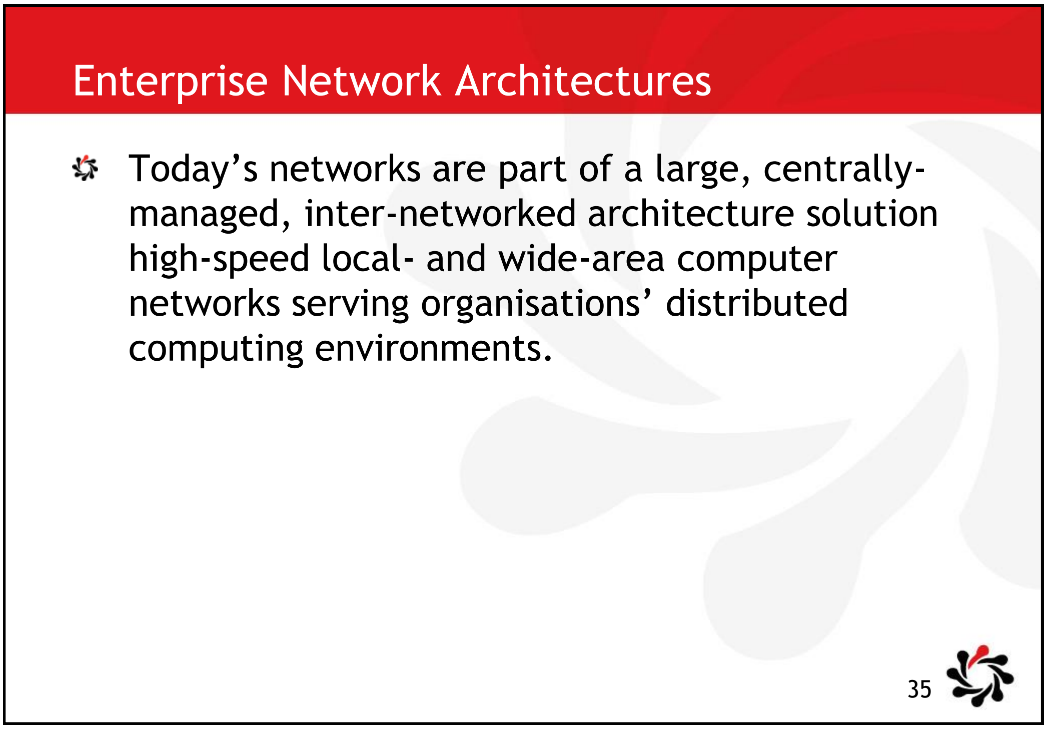
33



Network Types

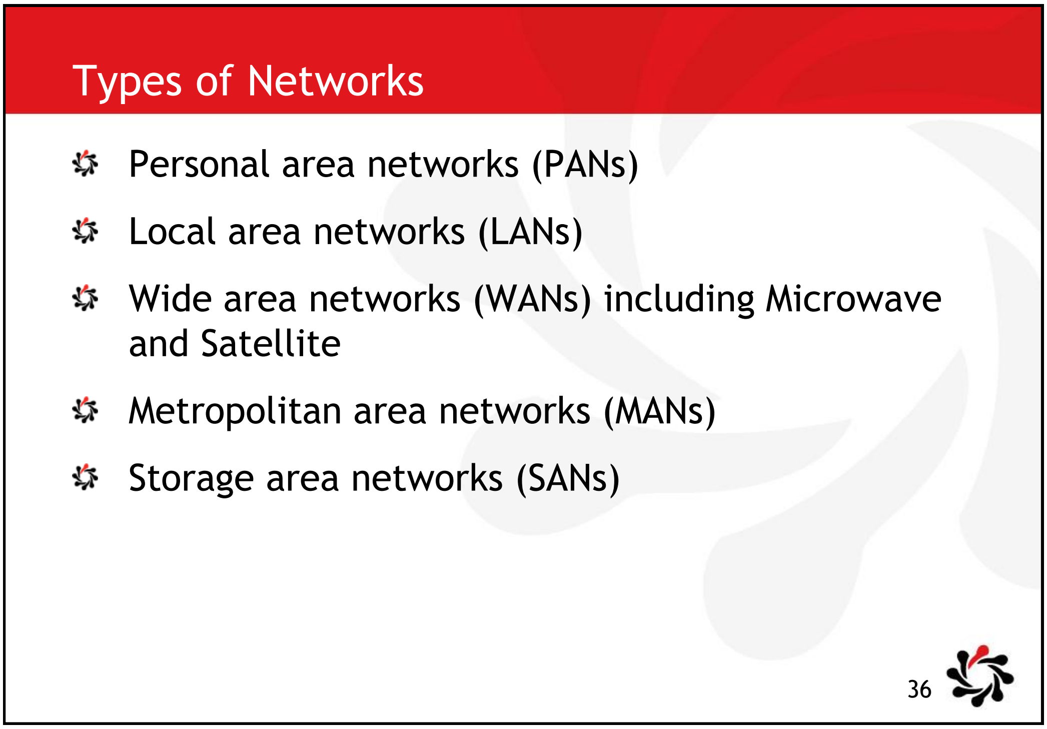
- Dedicated circuits
  - Leased lines
- Switched circuits
  - Circuit switching
  - Packet switching

34



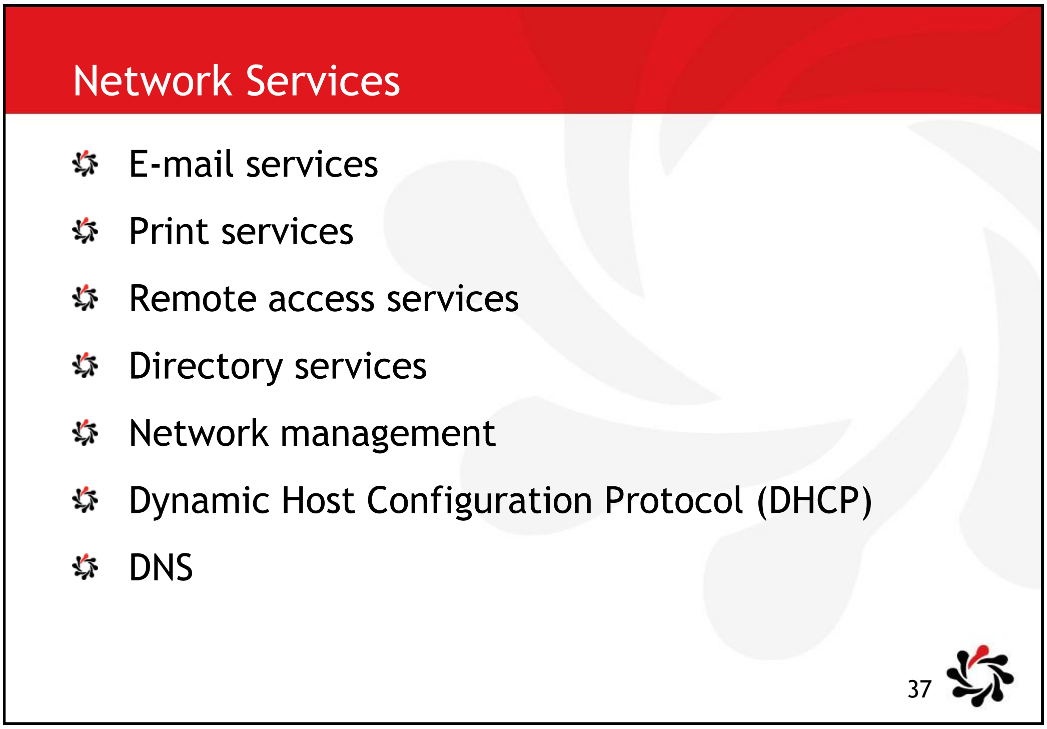
Enterprise Network Architectures

- 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.



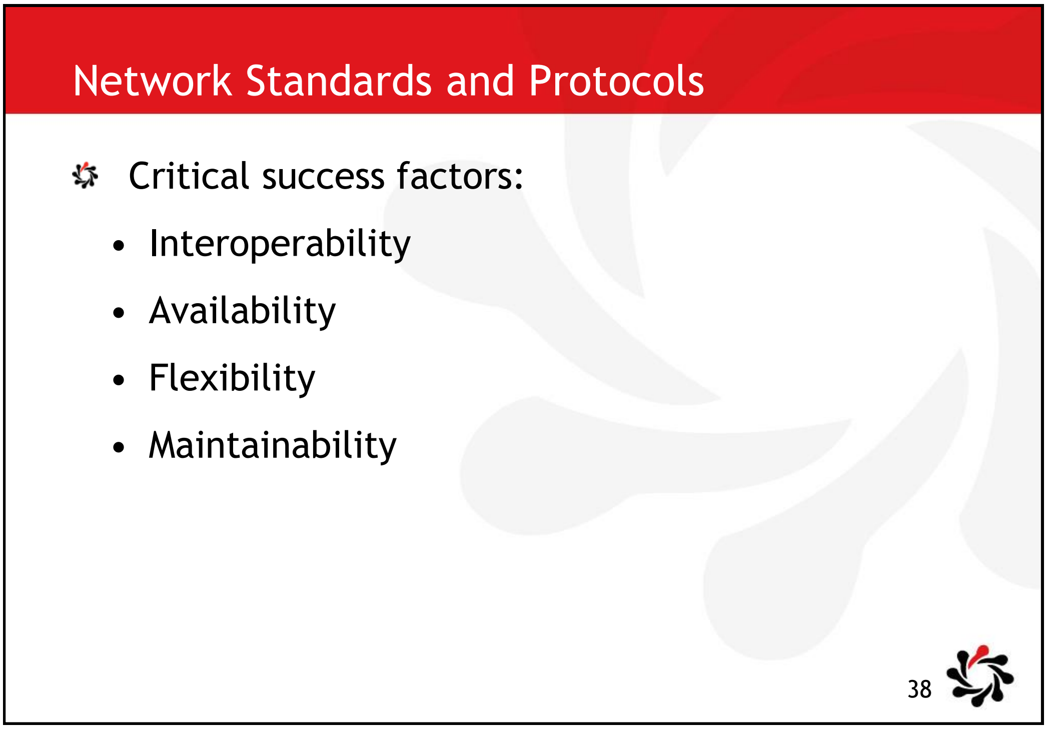
Types of Networks

- Personal area networks (PANs)
- Local area networks (LANs)
- Wide area networks (WANs) including Microwave and Satellite
- Metropolitan area networks (MANs)
- Storage area networks (SANs)



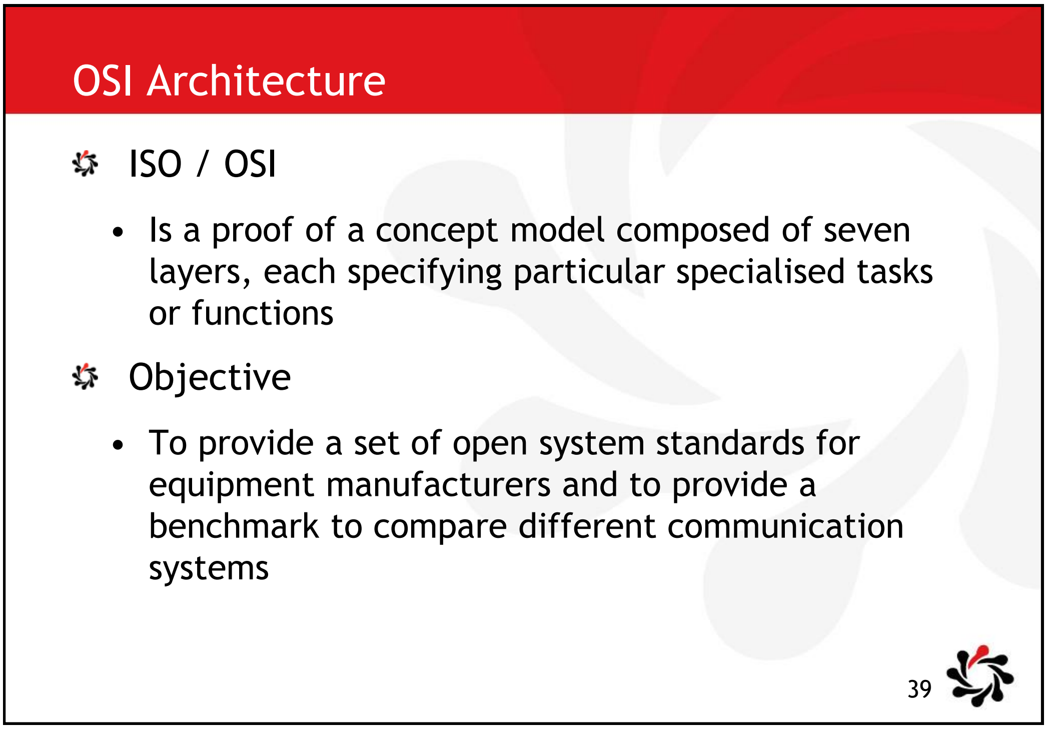
Network Services

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



Network Standards and Protocols

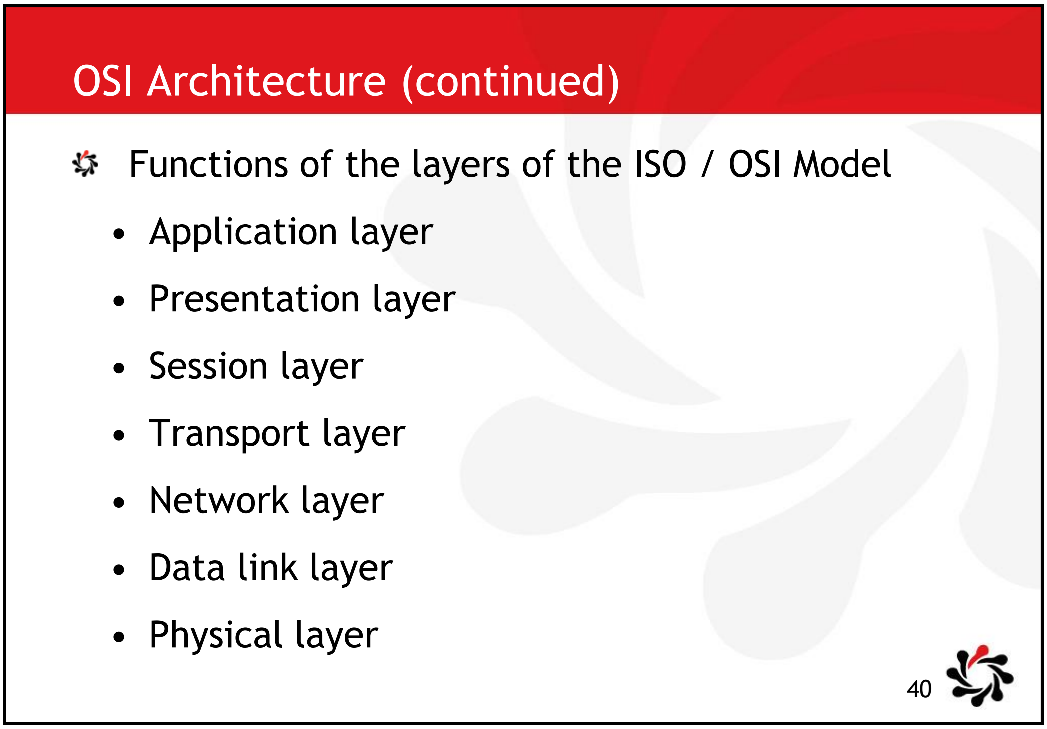
- Critical success factors:
  - Interoperability
  - Availability
  - Flexibility
  - Maintainability



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

39

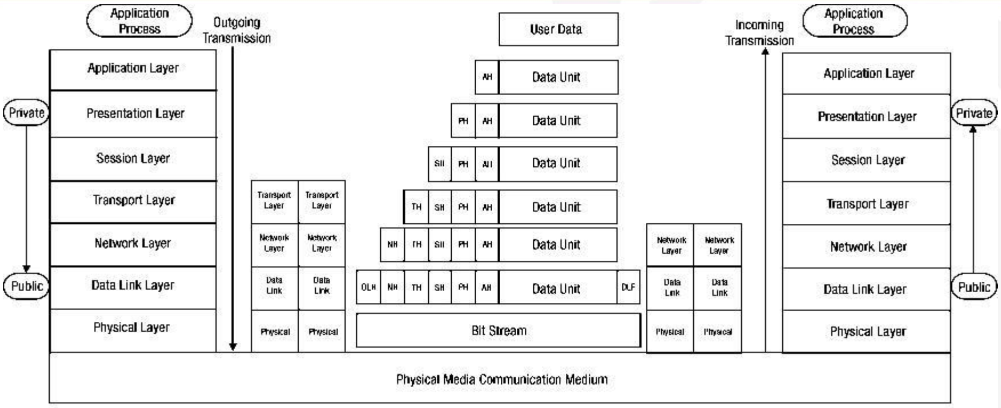


OSI Architecture (continued)

- Functions of the layers of the ISO / OSI Model
  - Application layer
  - Presentation layer
  - Session layer
  - Transport layer
  - Network layer
  - Data link layer
  - Physical layer

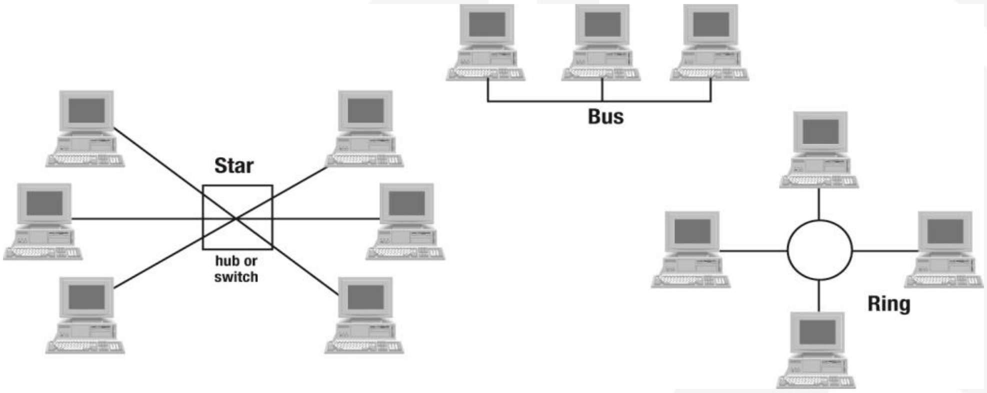
40

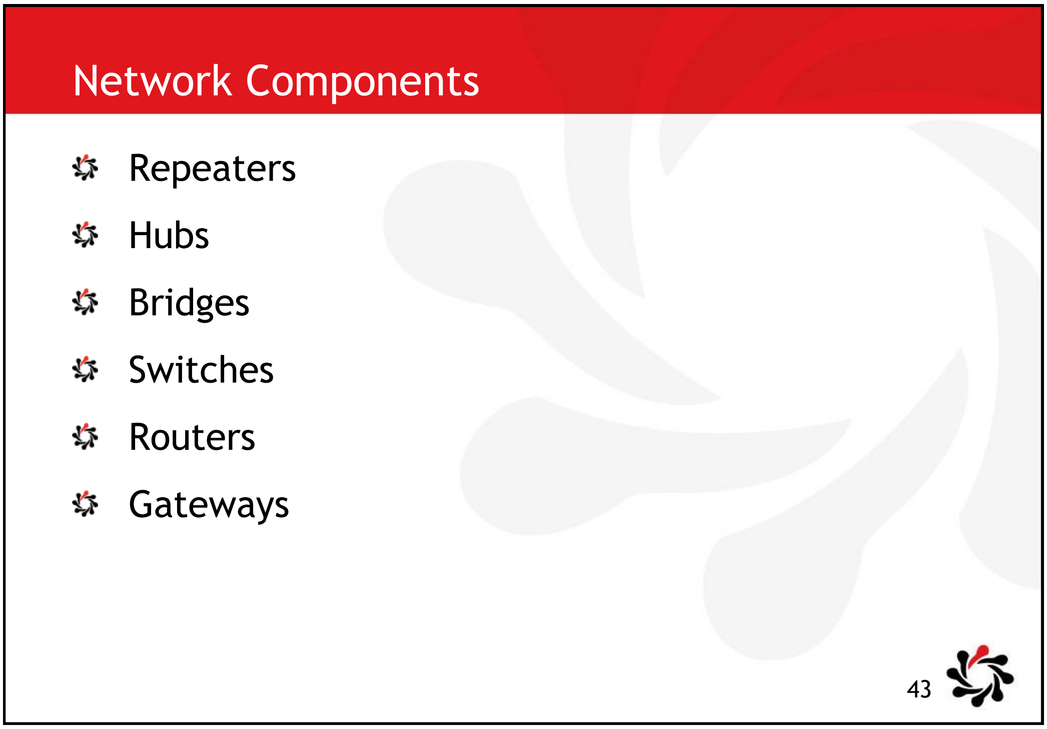
Application of the OSI Model in Network Architectures (continued)



AH = Application Header
PH = Presentation Header
SH = Session Header
TH = Transport Header
NH = Network Header
DLH = Data Link Header
DLF = Data Link Footer

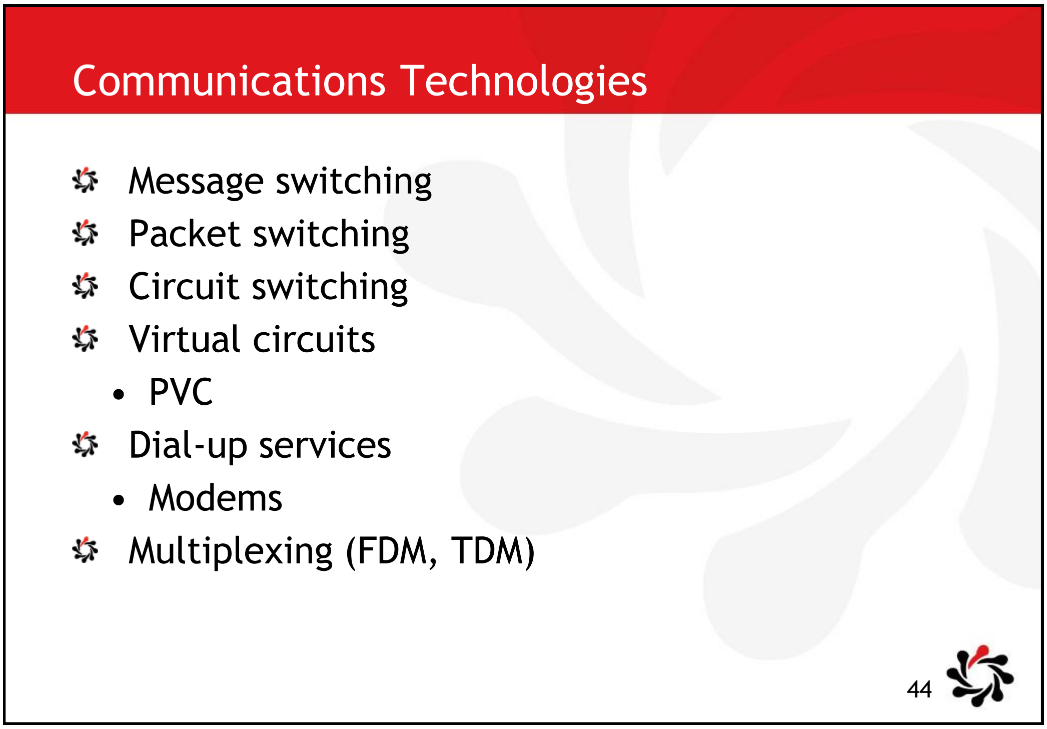
Network Architectures





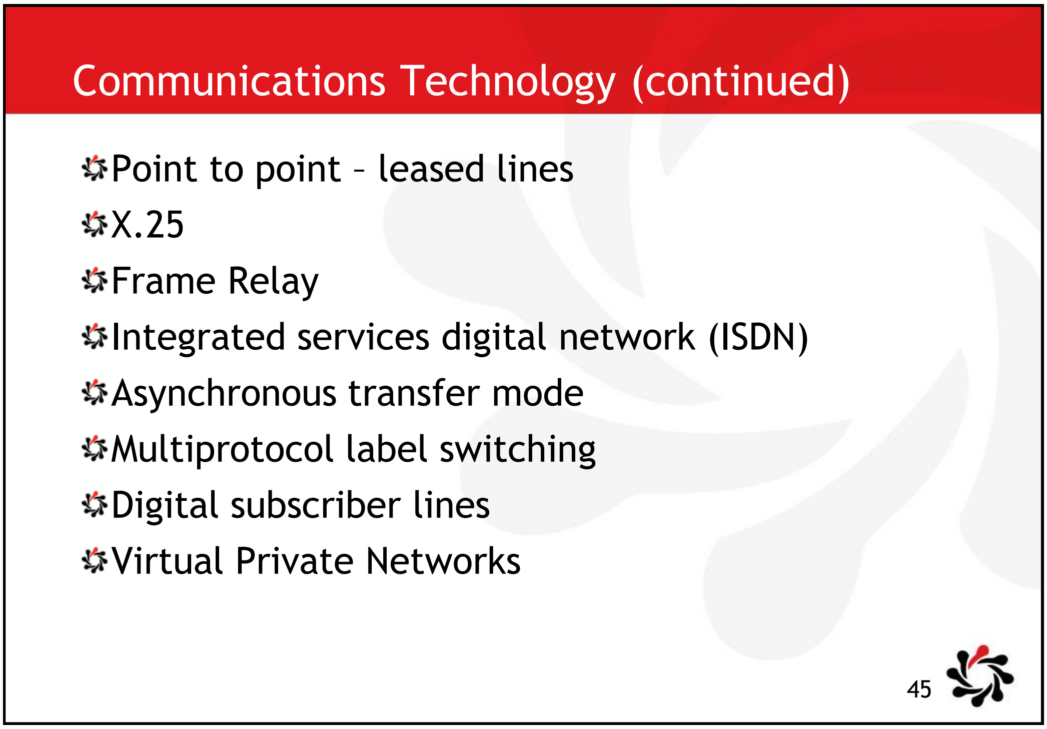
Network Components

- Repeaters
- Hubs
- Bridges
- Switches
- Routers
- Gateways



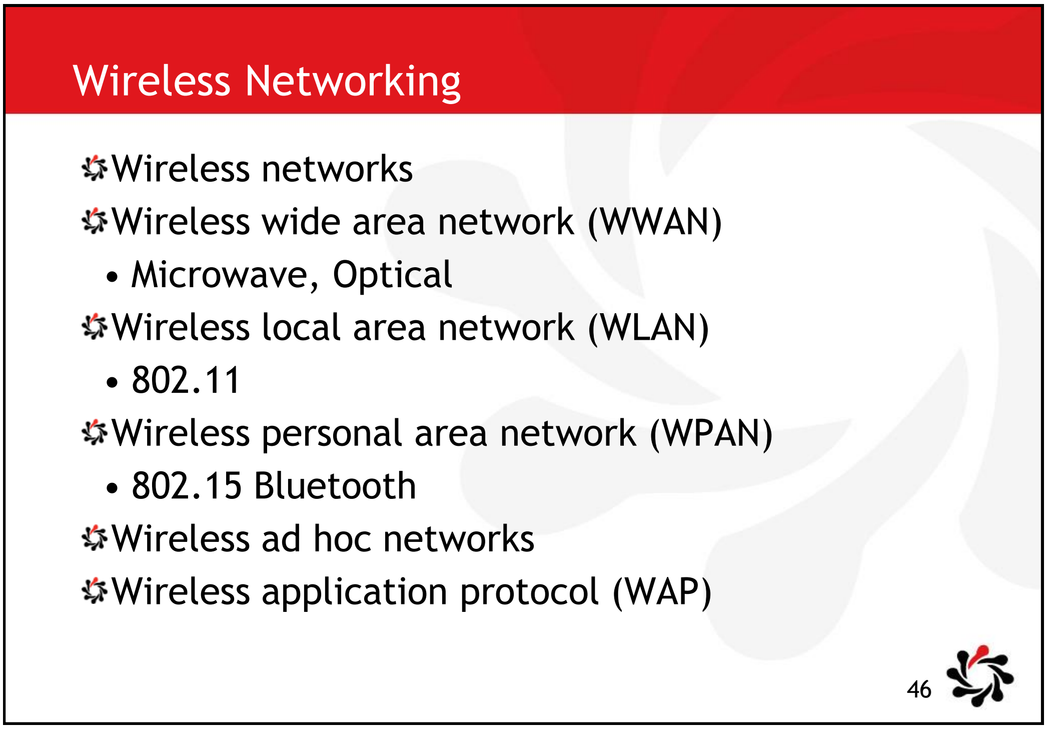
Communications Technologies

- Message switching
- Packet switching
- Circuit switching
- Virtual circuits
  - PVC
- Dial-up services
  - Modems
- Multiplexing (FDM, TDM)



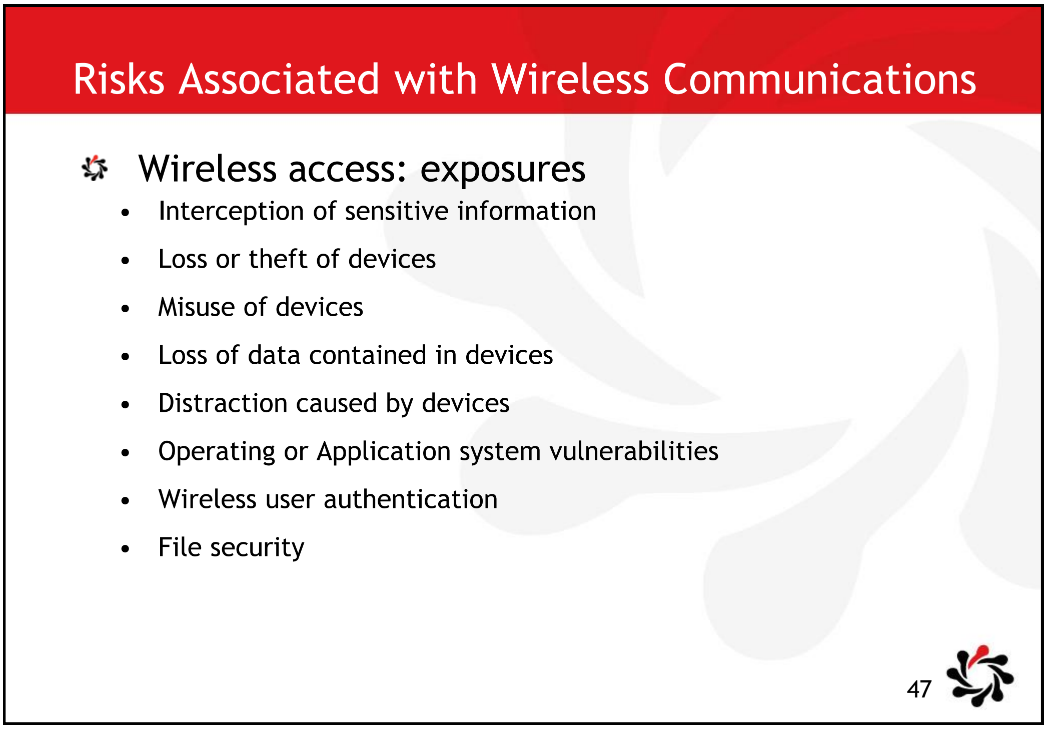
Communications Technology (continued)

- 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



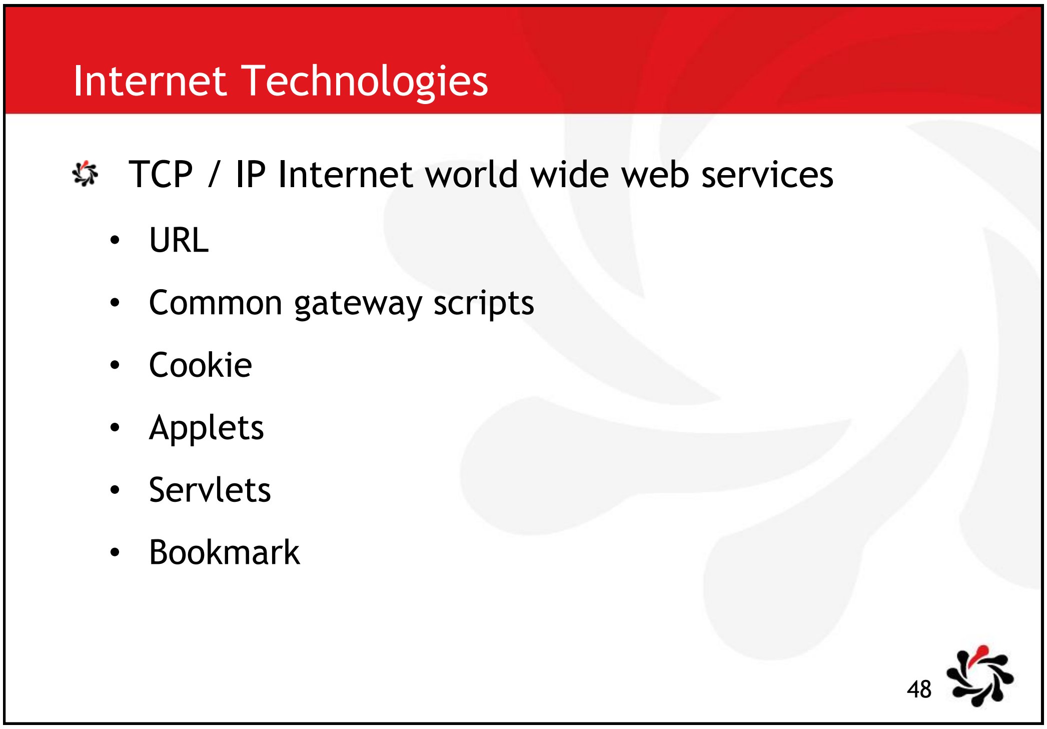
Wireless Networking

- 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)



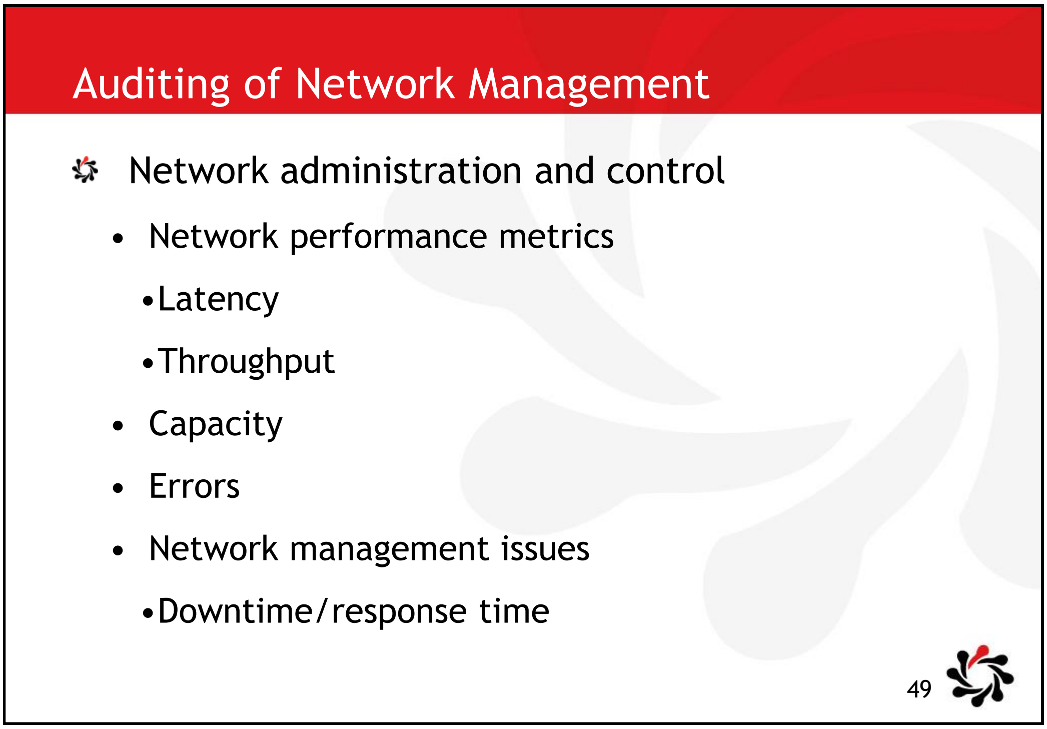
Risks Associated with Wireless Communications

- 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
  - Operating or Application system vulnerabilities
  - Wireless user authentication
  - File security



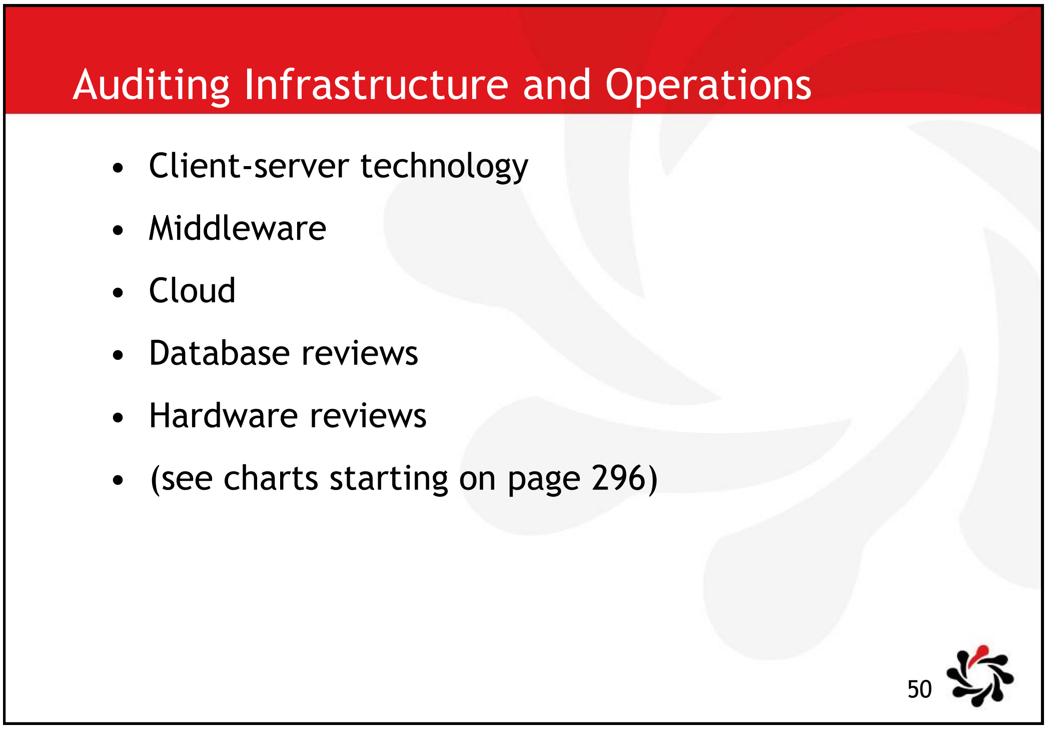
Internet Technologies

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



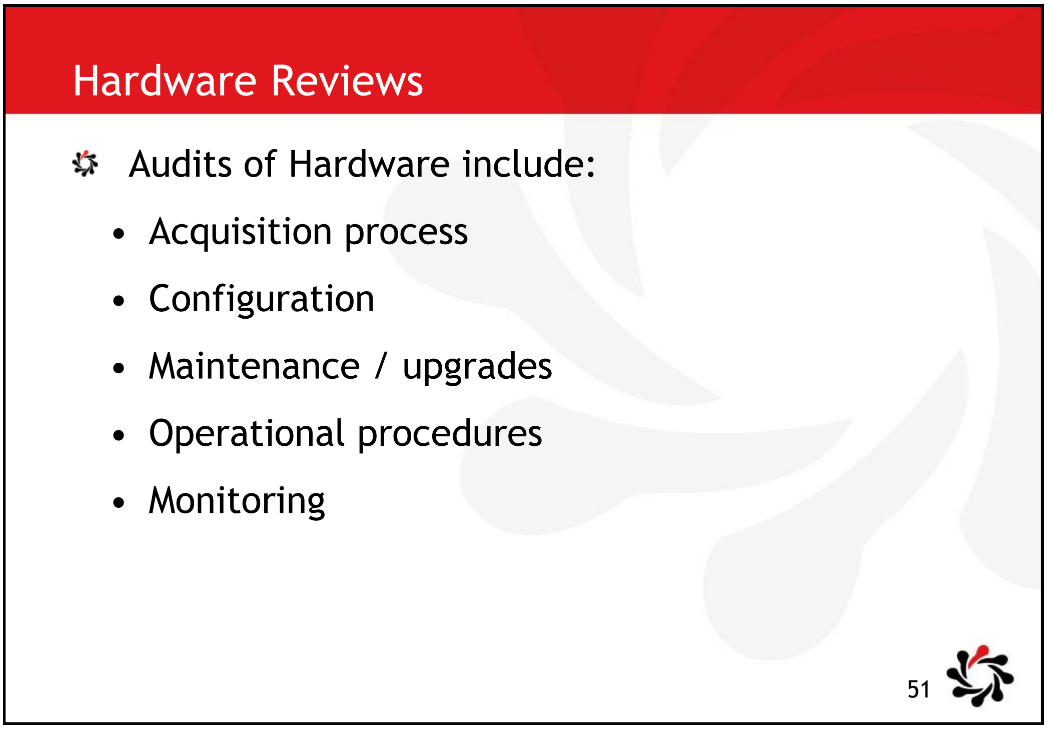
Auditing of Network Management

- Network administration and control
  - Network performance metrics
    - Latency
    - Throughput
  - Capacity
  - Errors
  - Network management issues
    - Downtime/response time



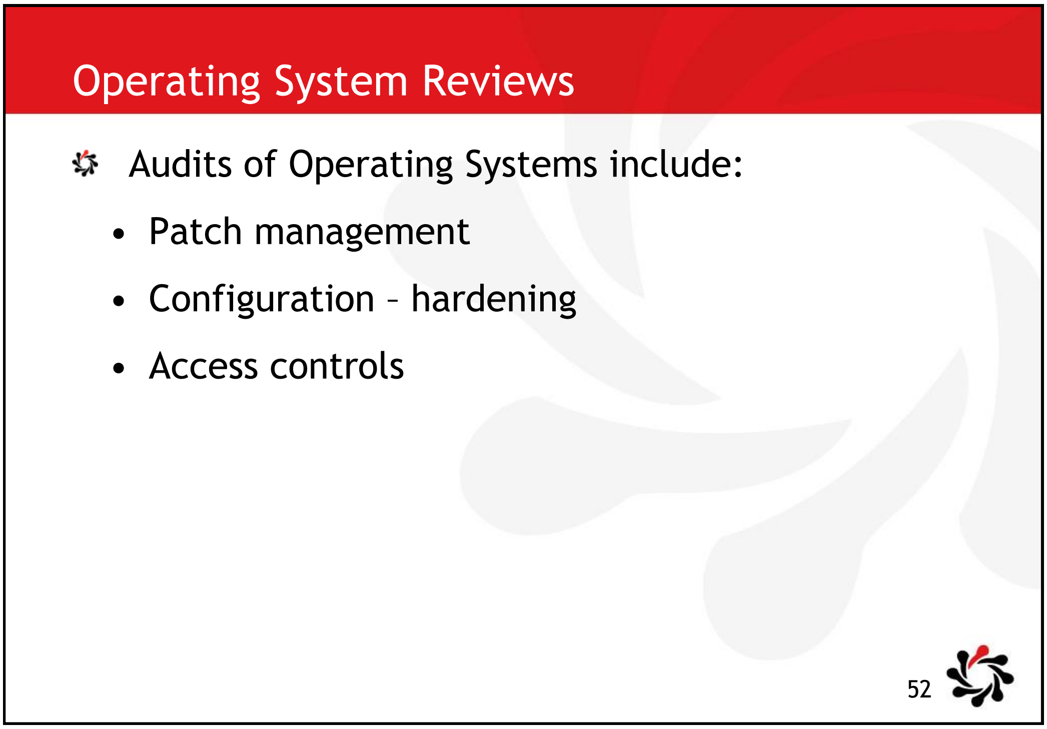
Auditing Infrastructure and Operations

- Client-server technology
- Middleware
- Cloud
- Database reviews
- Hardware reviews
- (see charts starting on page 296)



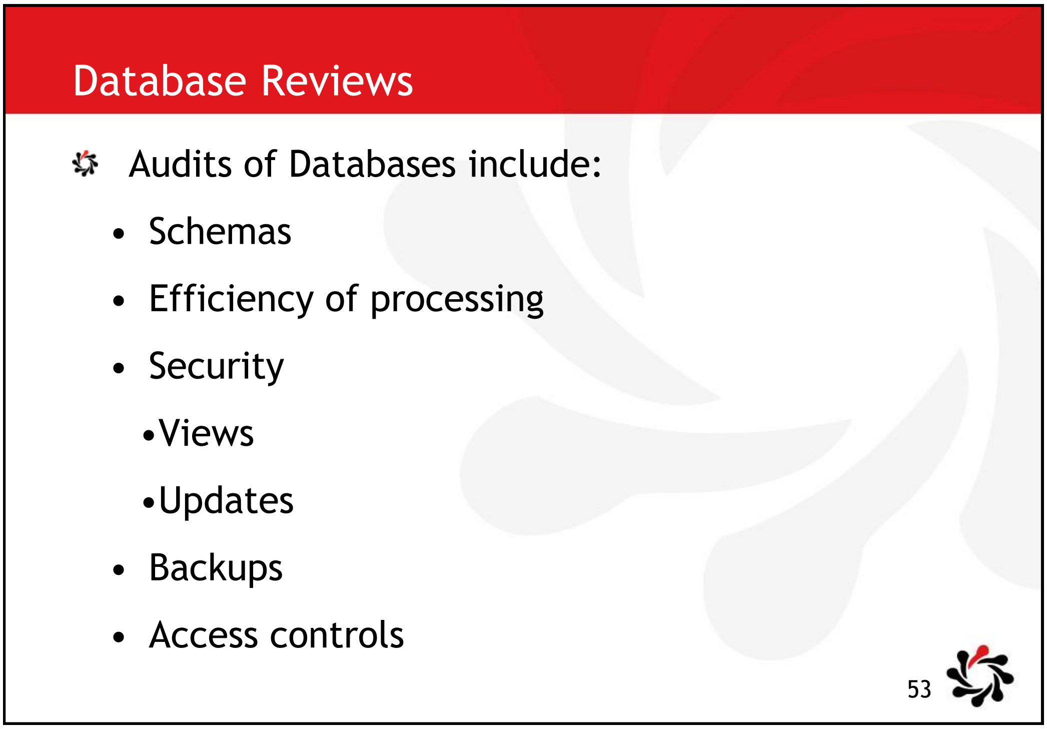
Hardware Reviews

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



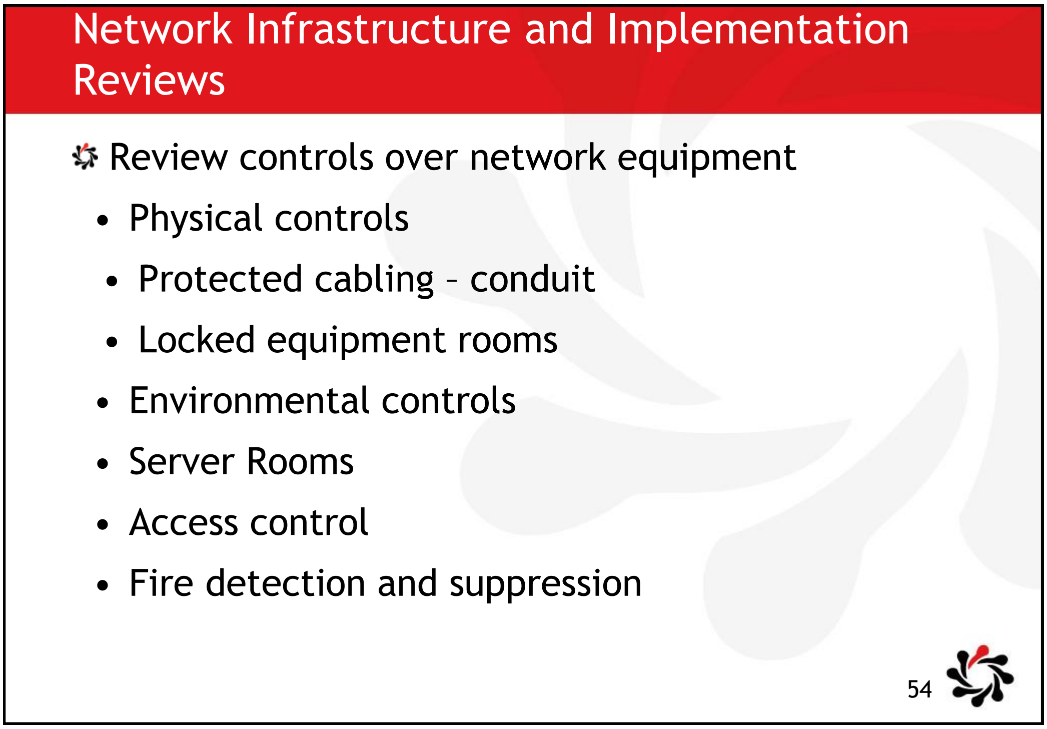
Operating System Reviews

- 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

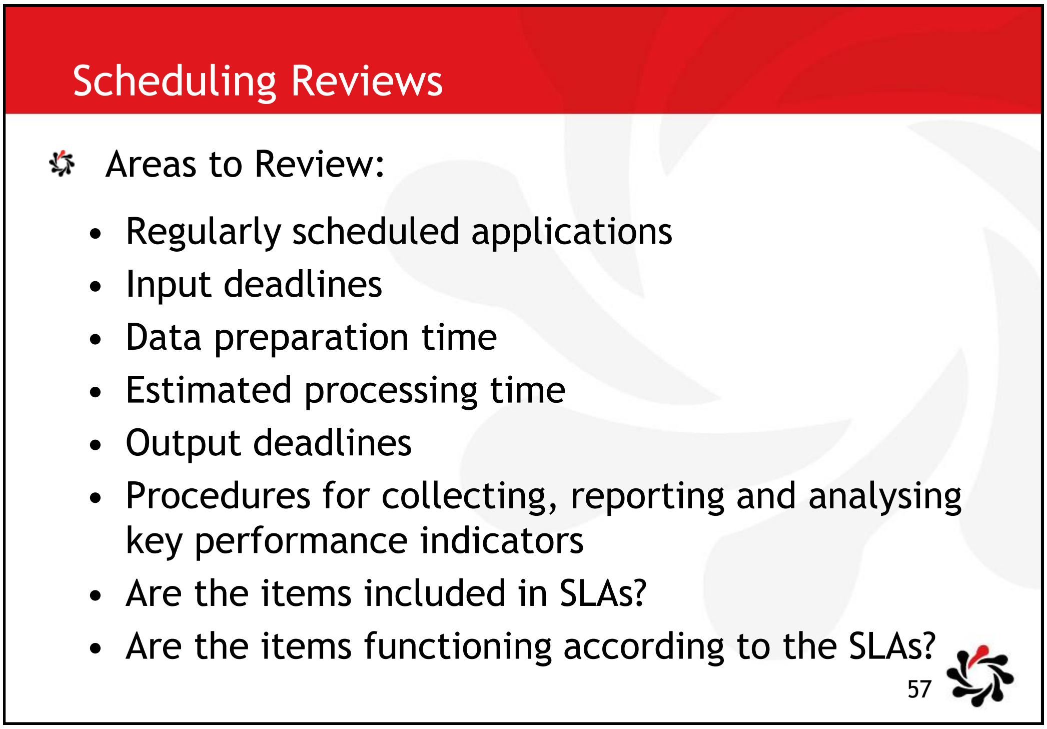
- Logical security controls
  - Network User and Administrator Access & Passwords
  - Network Access Change Requests
  - Test Plans
  - Security Reports
  - Performance and monitoring

55

Physical Security Audits

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

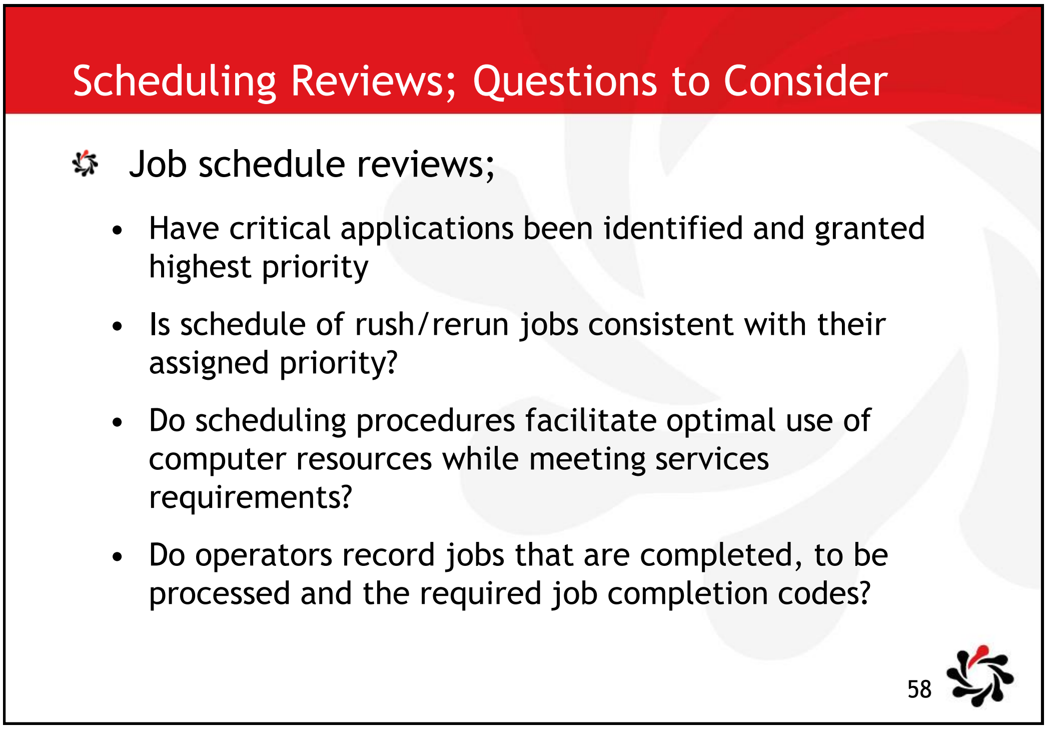
56



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?

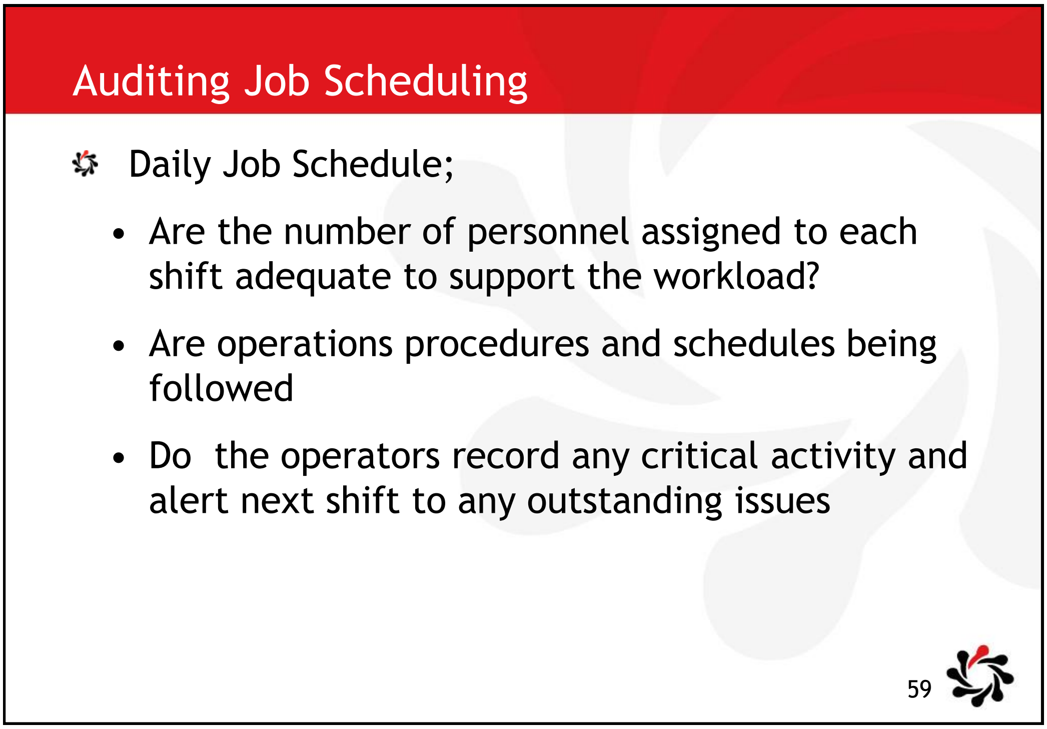
57



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?

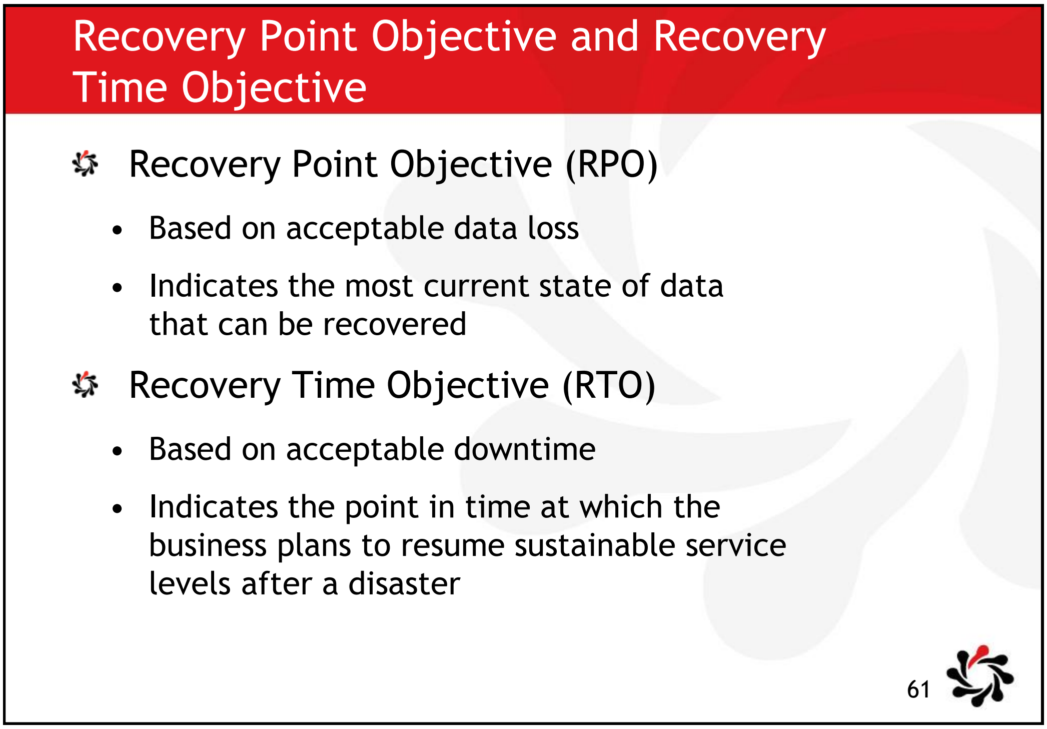
58



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

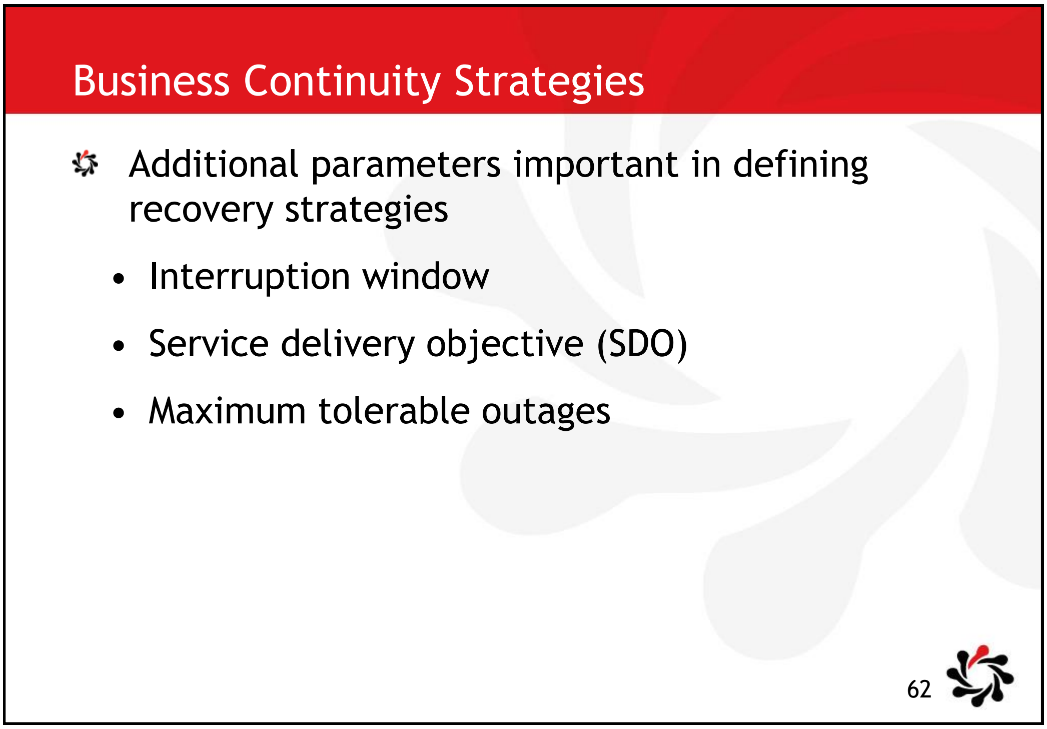
Disaster Recovery Planning



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

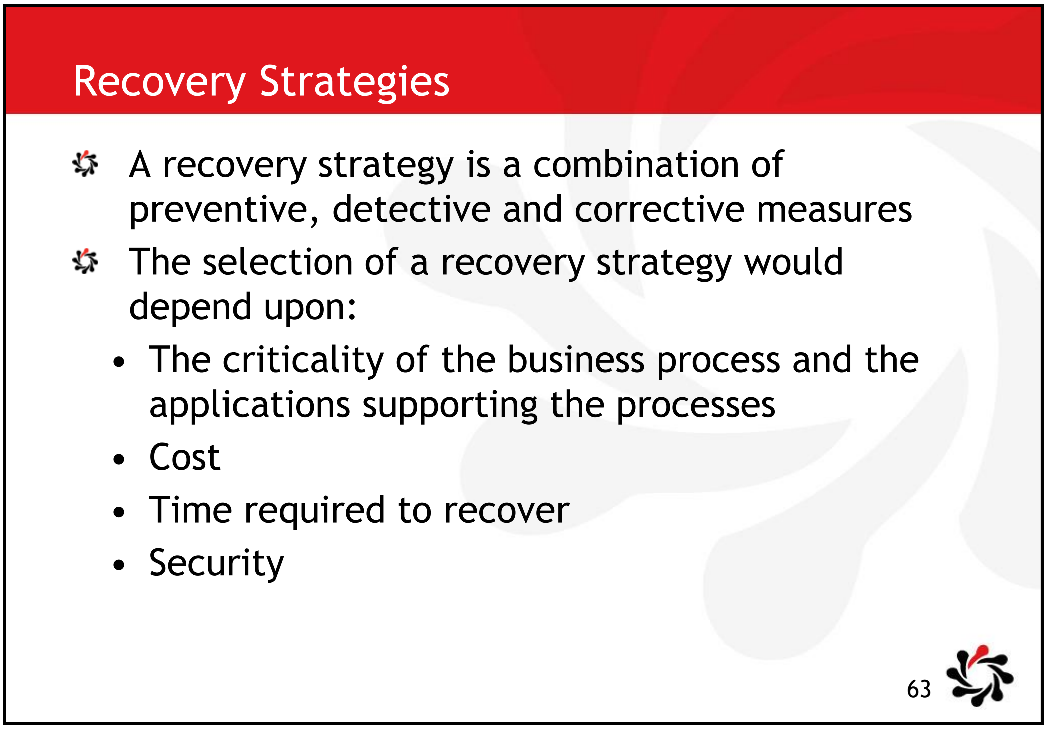
61



Business Continuity Strategies

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

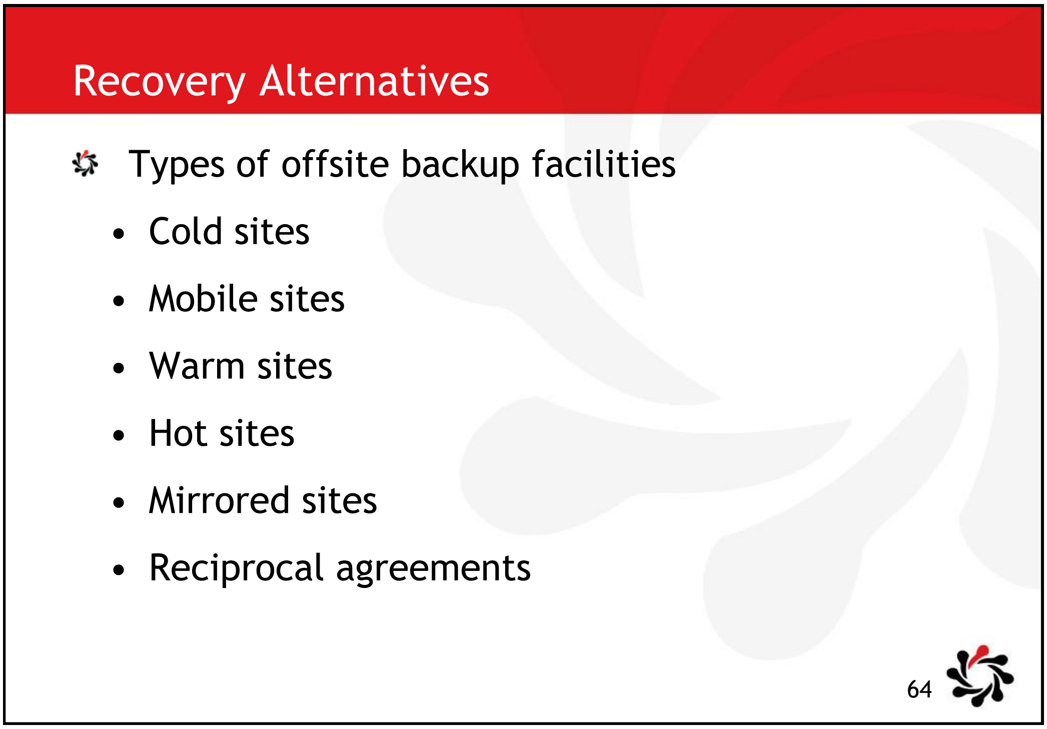
62



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

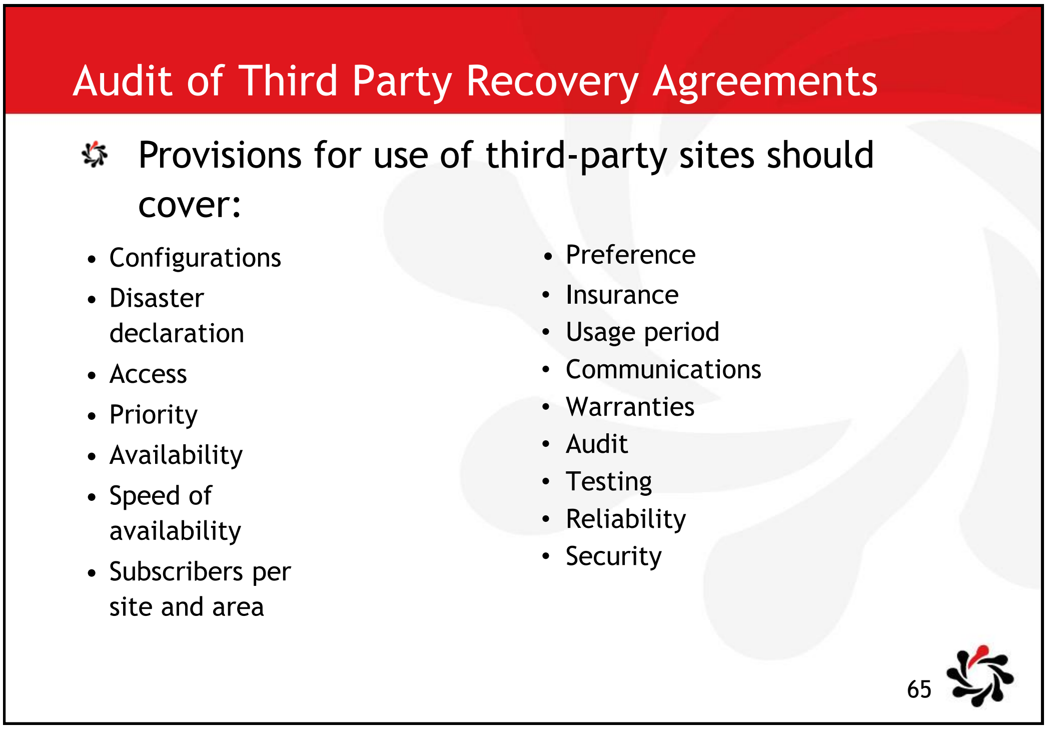
63



Recovery Alternatives

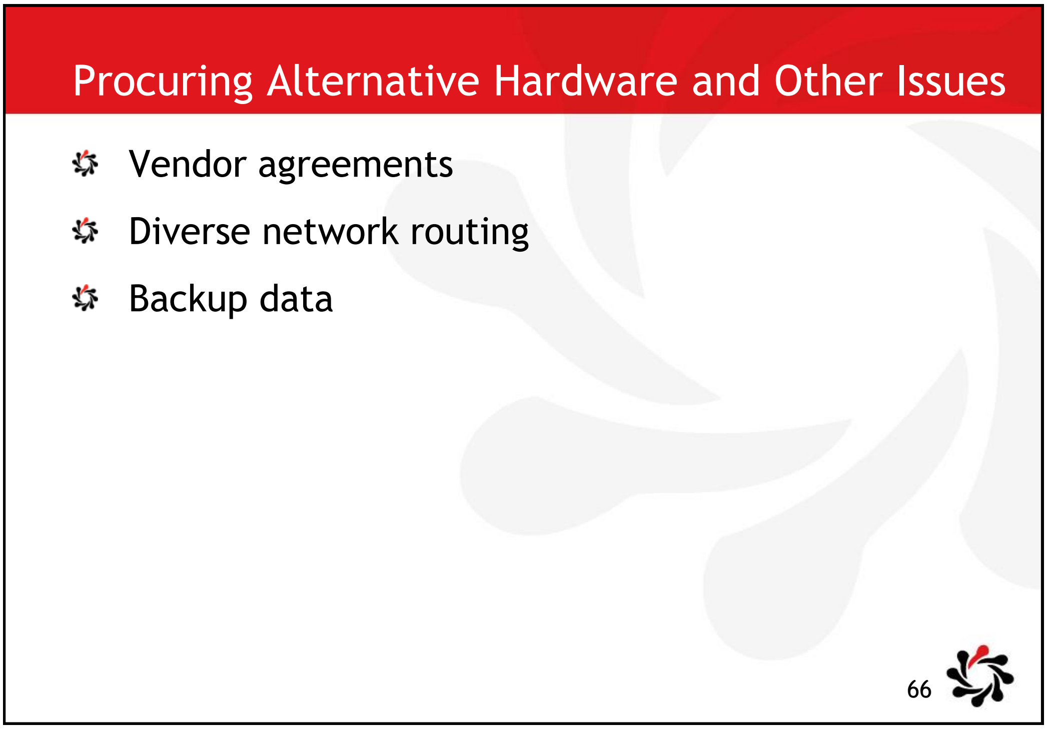
- Types of offsite backup facilities
  - Cold sites
  - Mobile sites
  - Warm sites
  - Hot sites
  - Mirrored sites
  - Reciprocal agreements

64



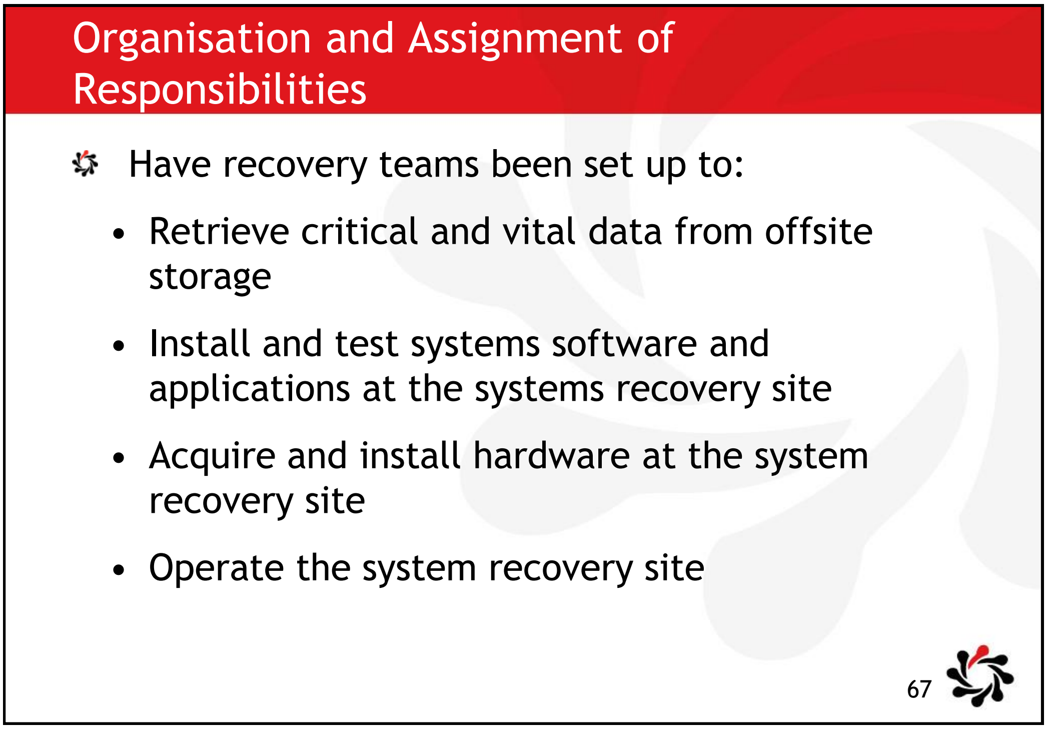
Audit of Third Party Recovery Agreements

- 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



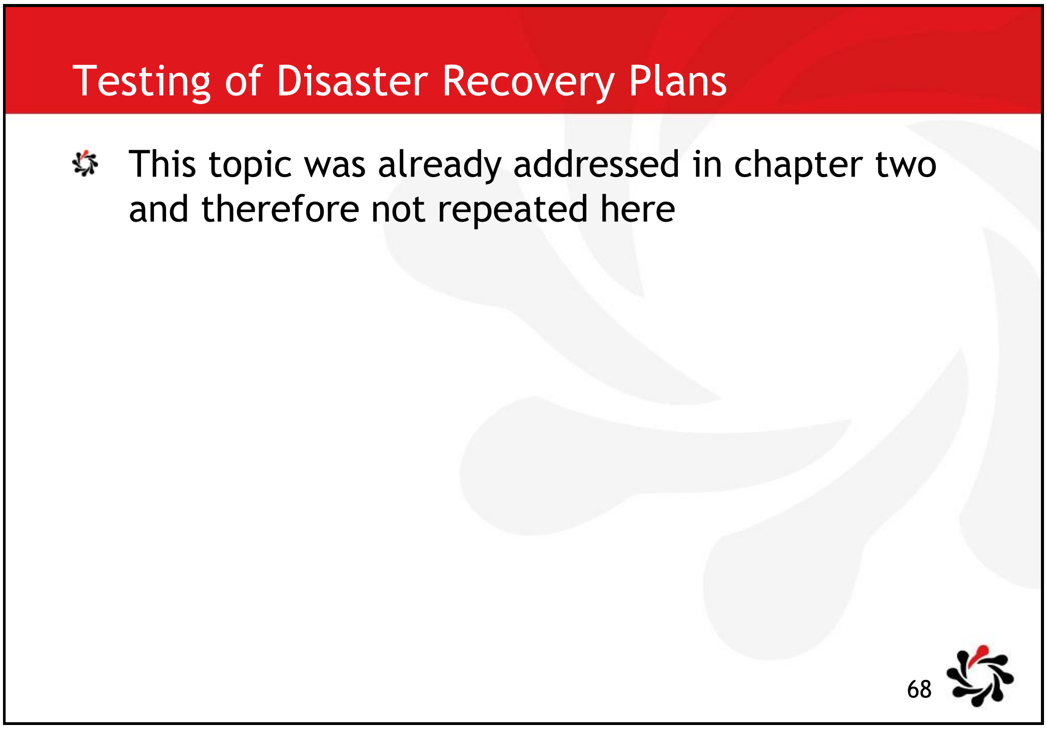
Procuring Alternative Hardware and Other Issues

- Vendor agreements
- Diverse network routing
- Backup data



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



Testing of Disaster Recovery Plans

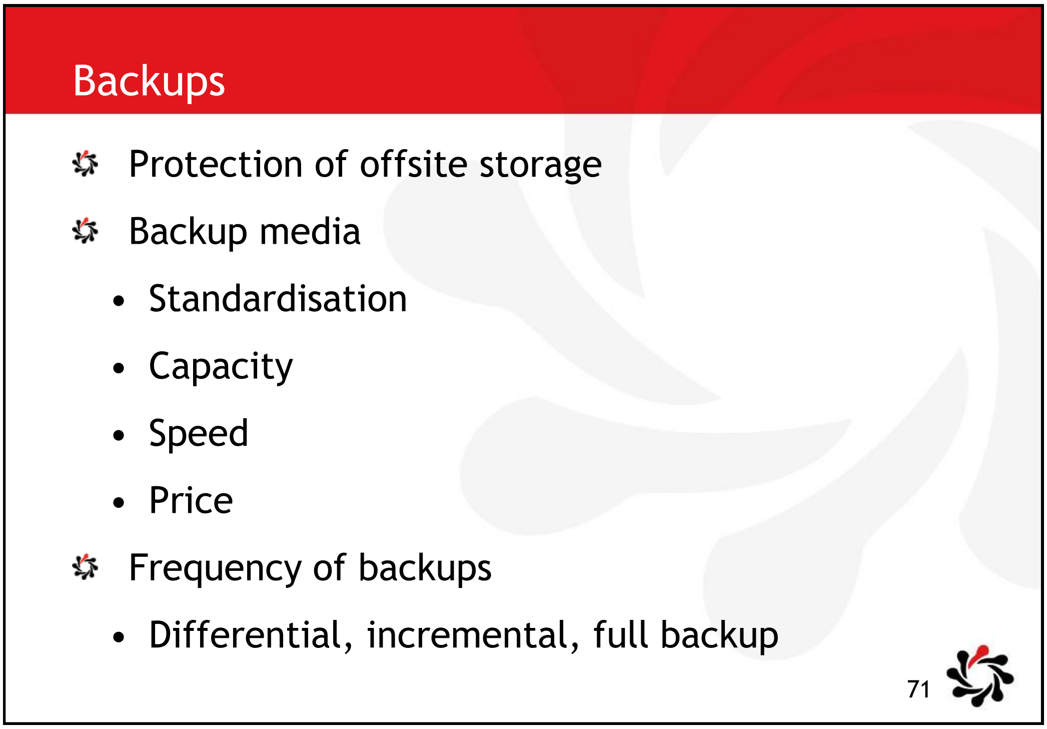
- This topic was already addressed in chapter two and therefore not repeated here

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

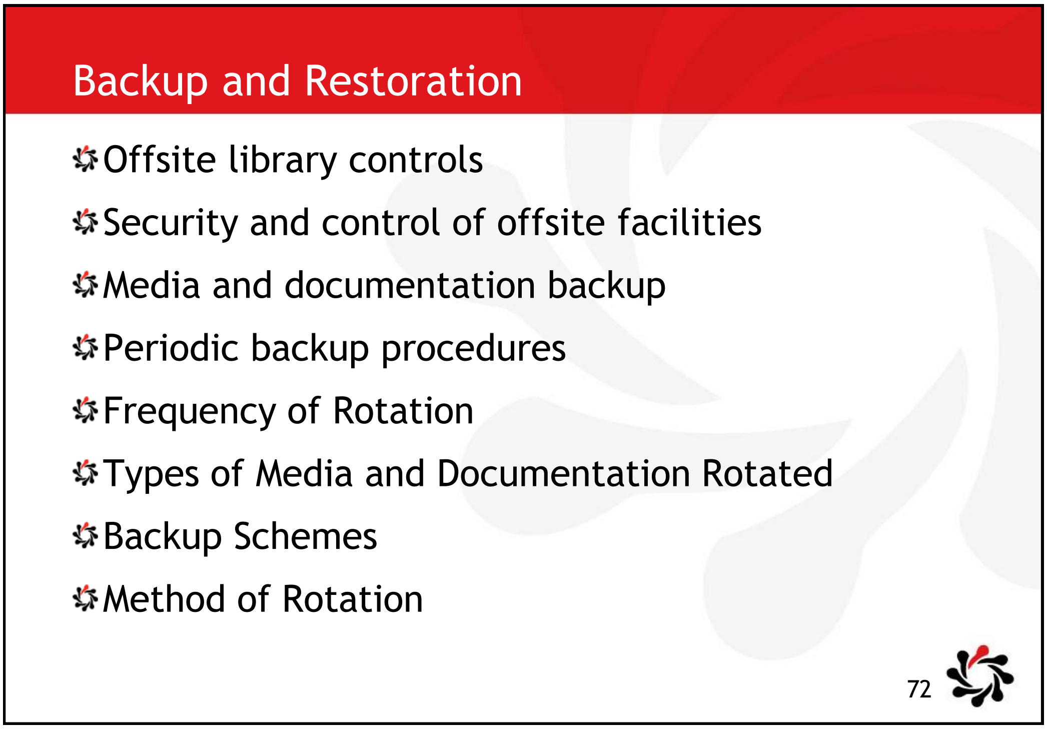
Team Responsibilities

- 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



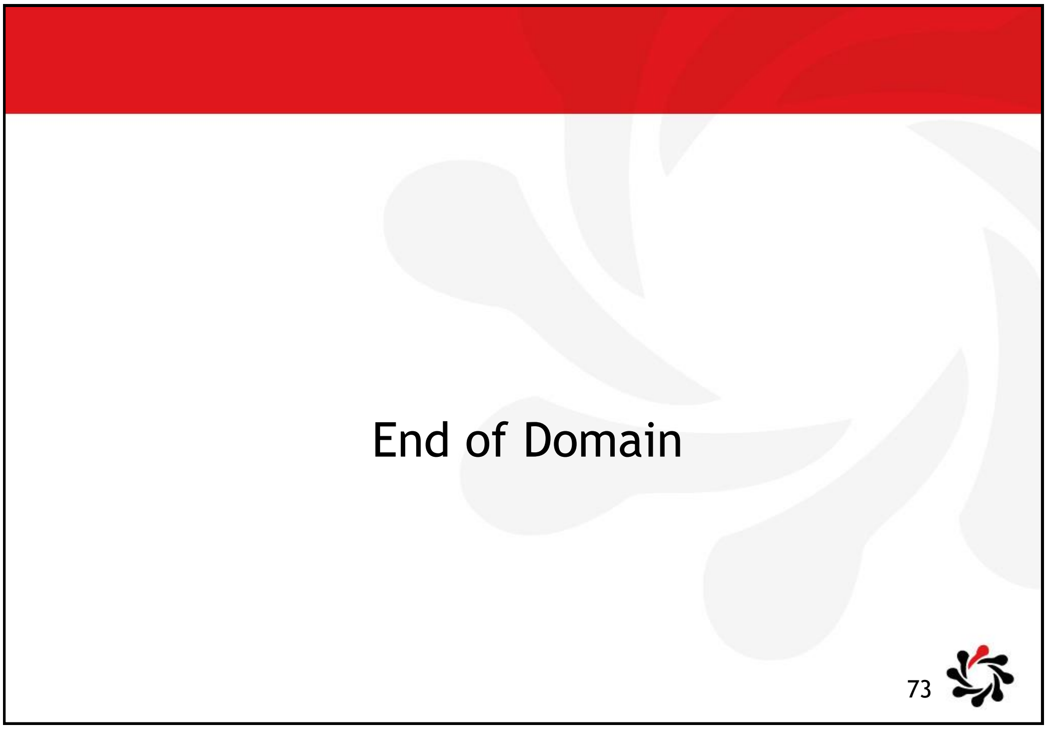
Backups

- Protection of offsite storage
- Backup media
  - Standardisation
  - Capacity
  - Speed
  - Price
- Frequency of backups
  - Differential, incremental, full backup



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

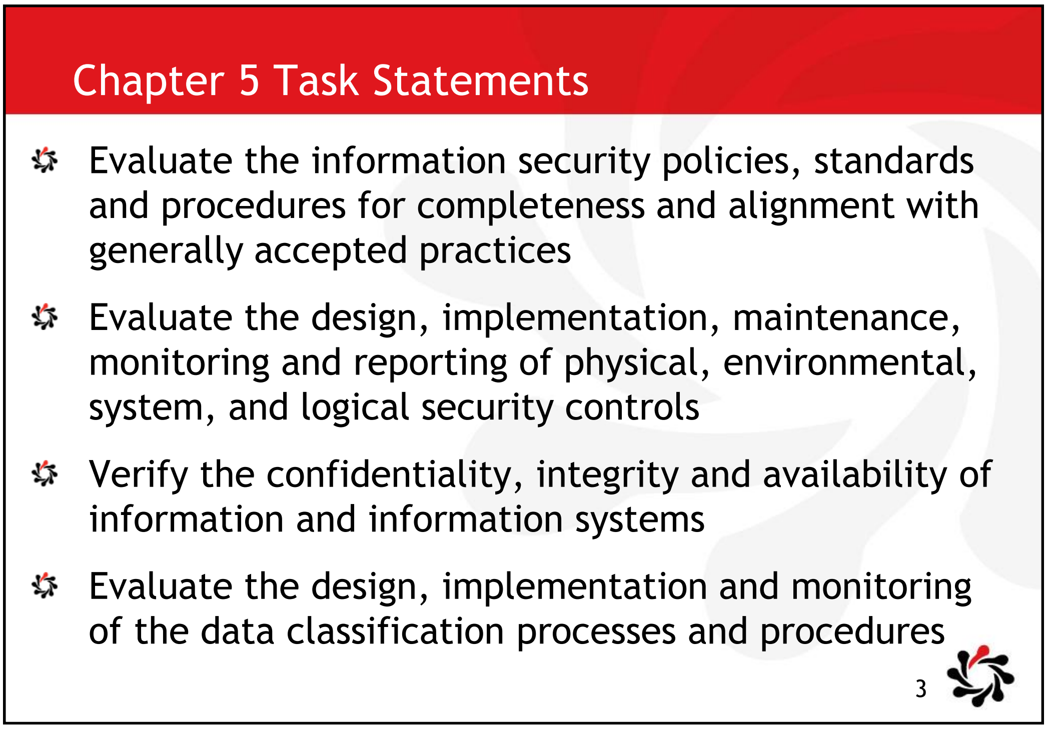
2017 Firebrand CISA® Review Course

Chapter 5 – Protection of Information Assets

Exam Relevance

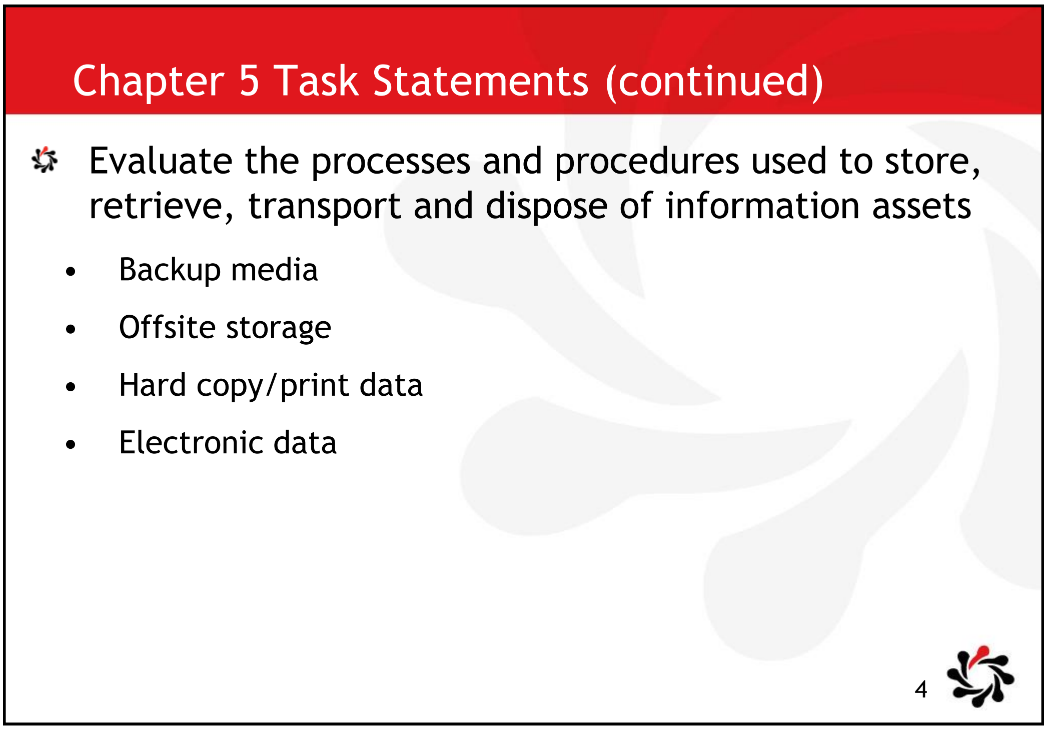
- Ensure that the CISA candidate…
  - “Understands and can provide assurance that the security policies, standards, procedures and controls ensures the confidentiality, integrity and availability of information assets.”
  - The content area in this chapter will represent approximately 25% of the CISA examination

  (approximately 38 questions)



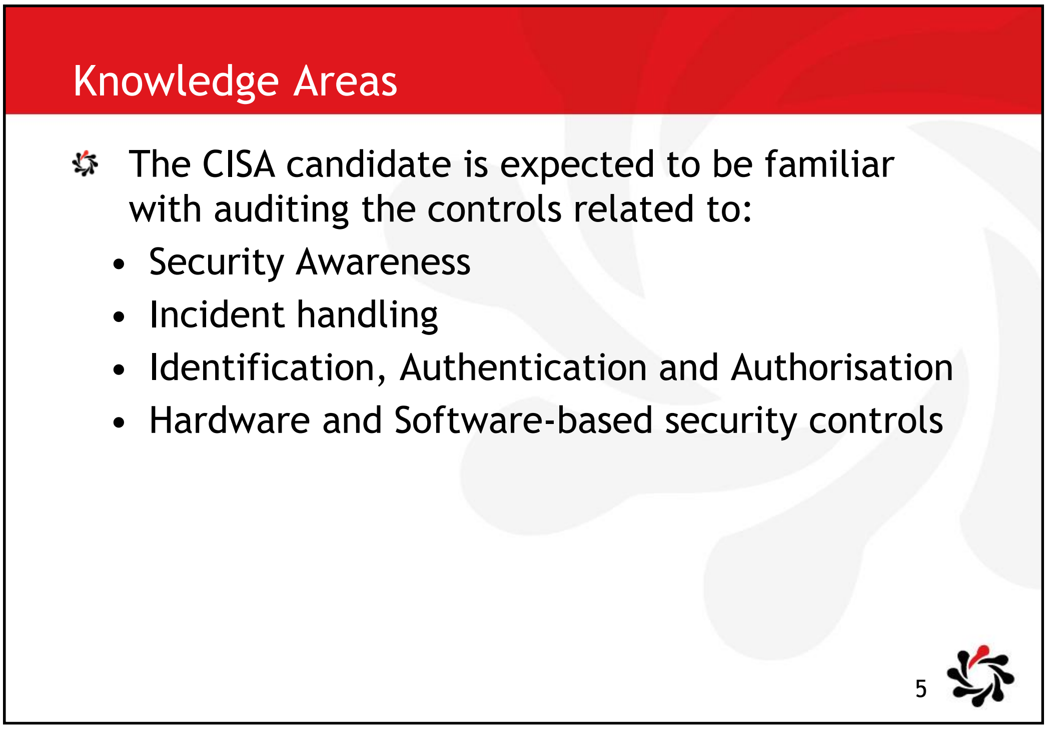
Chapter 5 Task Statements

- Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices
- Evaluate the design, implementation, maintenance, monitoring and reporting of physical, environmental, 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



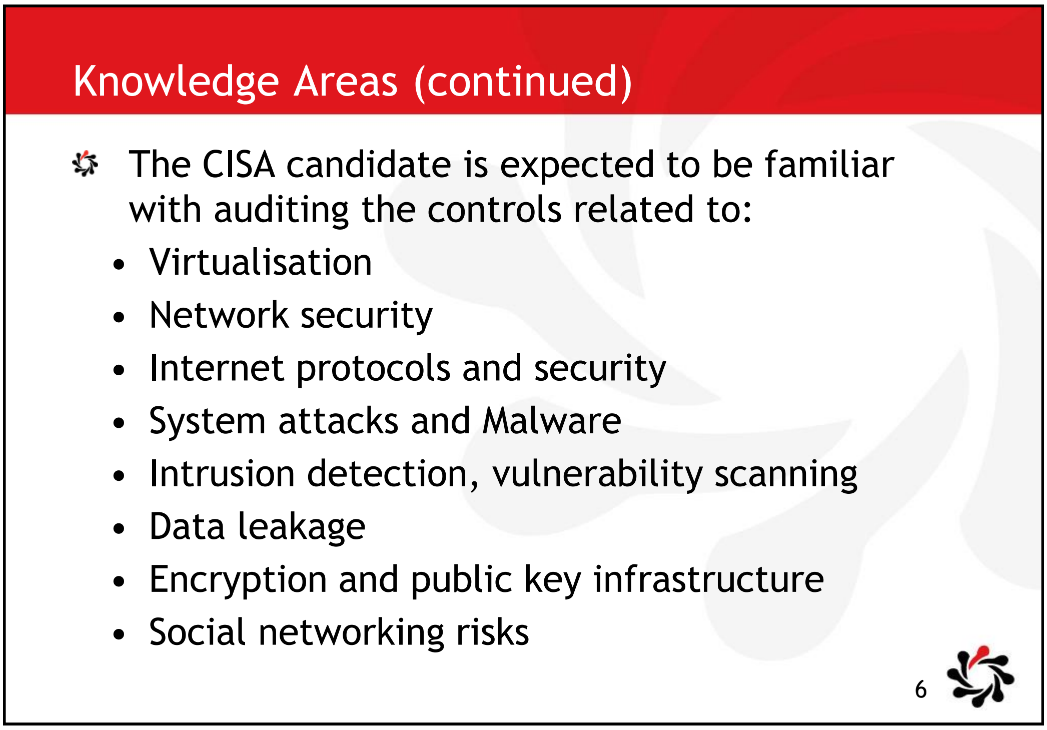
Chapter 5 Task Statements (continued)

- Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets
  - Backup media
  - Offsite storage
  - Hard copy/print data
  - Electronic data



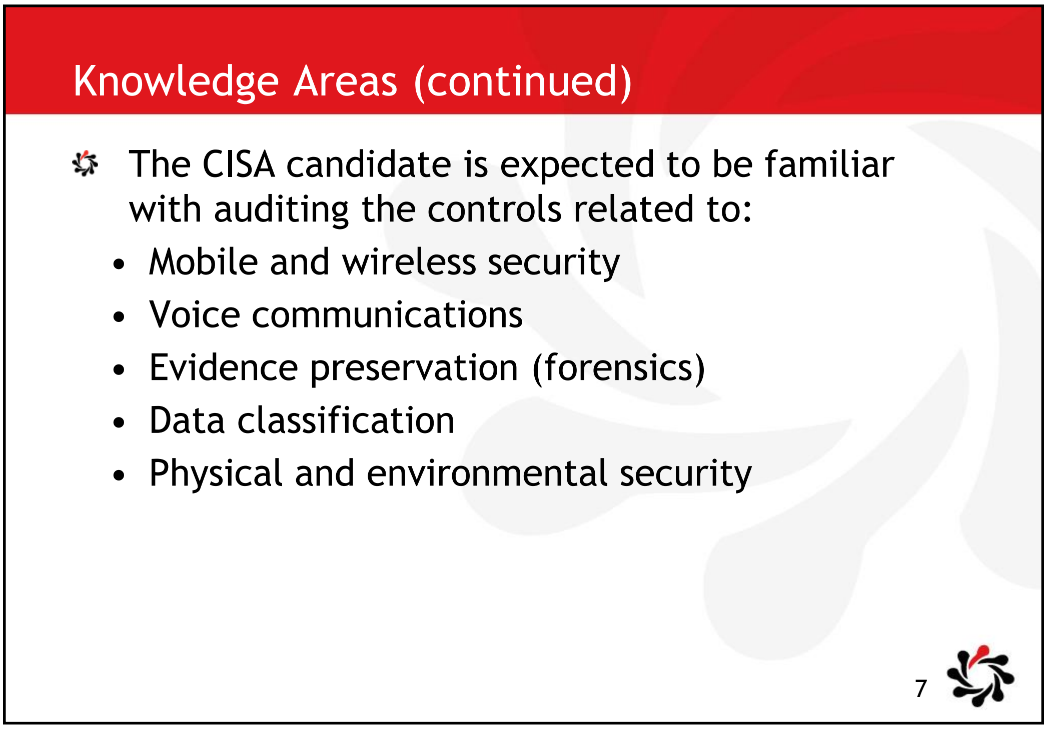
Knowledge Areas

- 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:
  - Virtualisation
  - Network security
  - Internet protocols and security
  - System attacks and Malware
  - Intrusion detection, vulnerability scanning
  - Data leakage
  - Encryption and public key infrastructure
  - Social networking risks



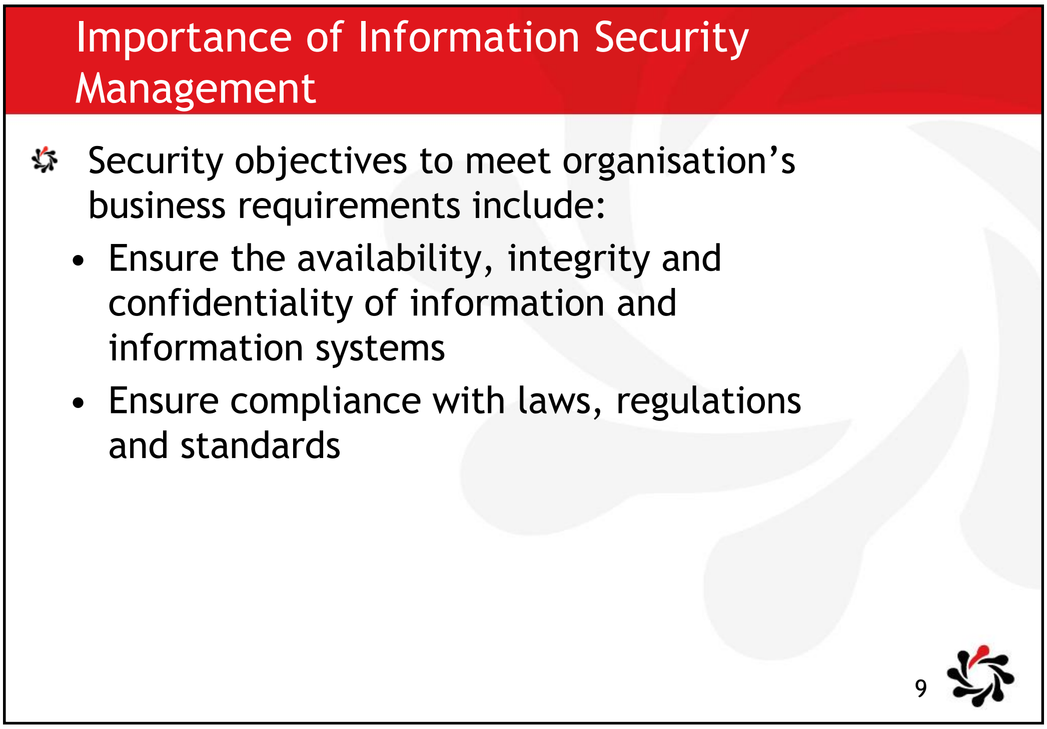
Knowledge Areas (continued)

- 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

7

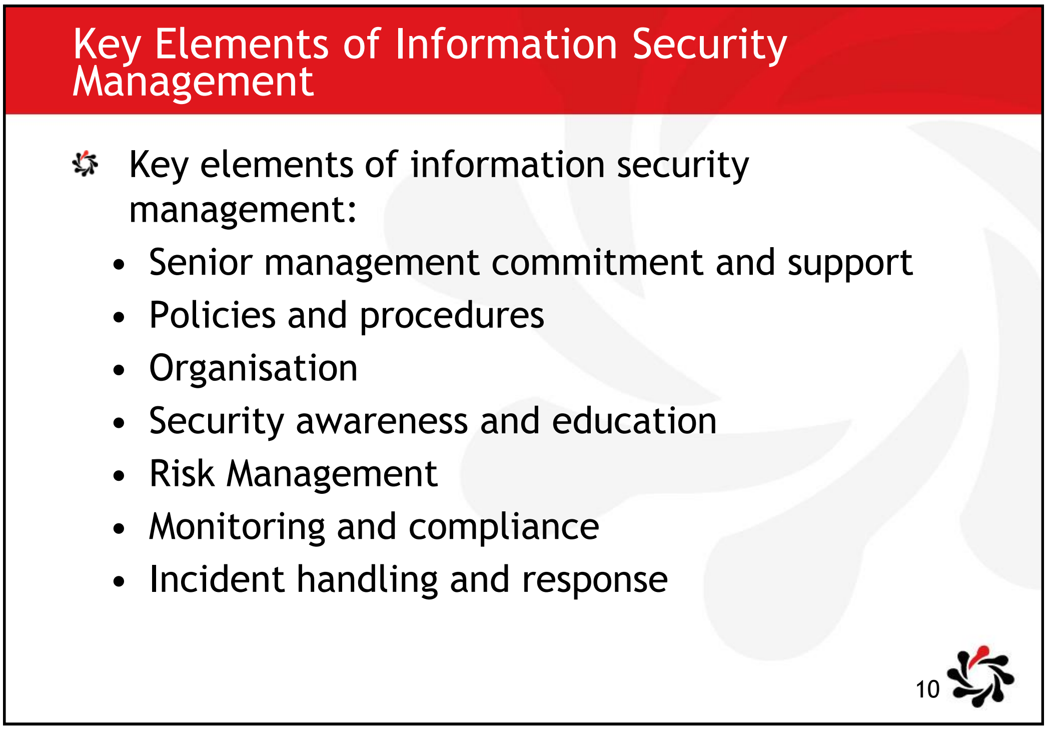
Information Security Management

8



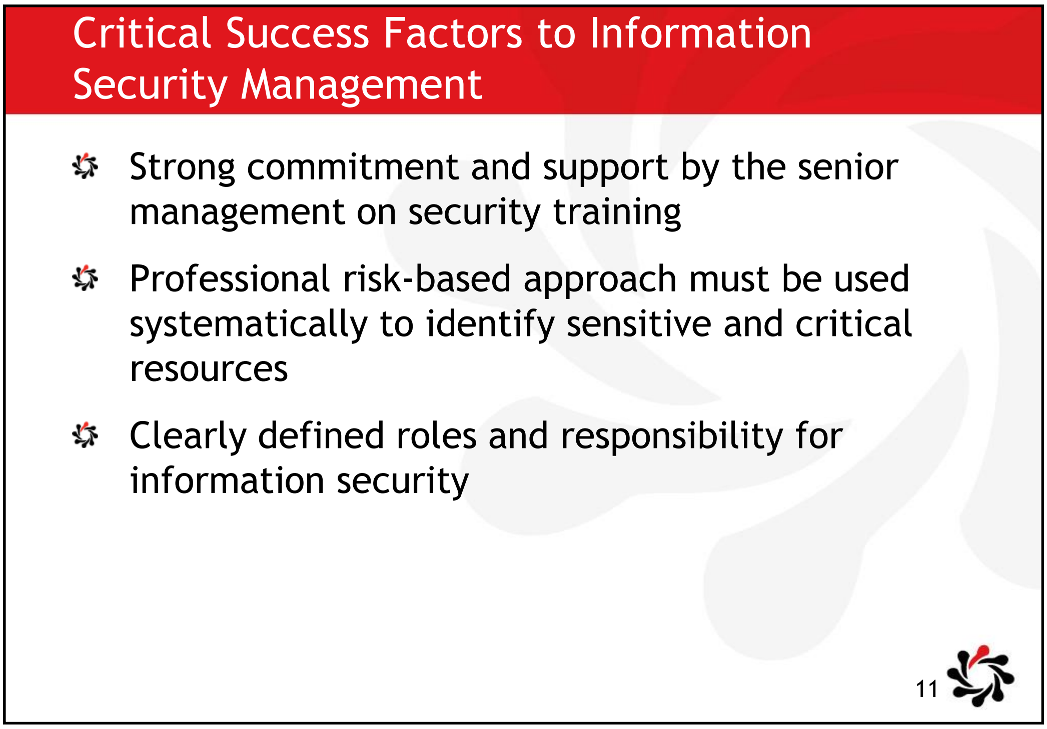
Importance of Information Security Management

- 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



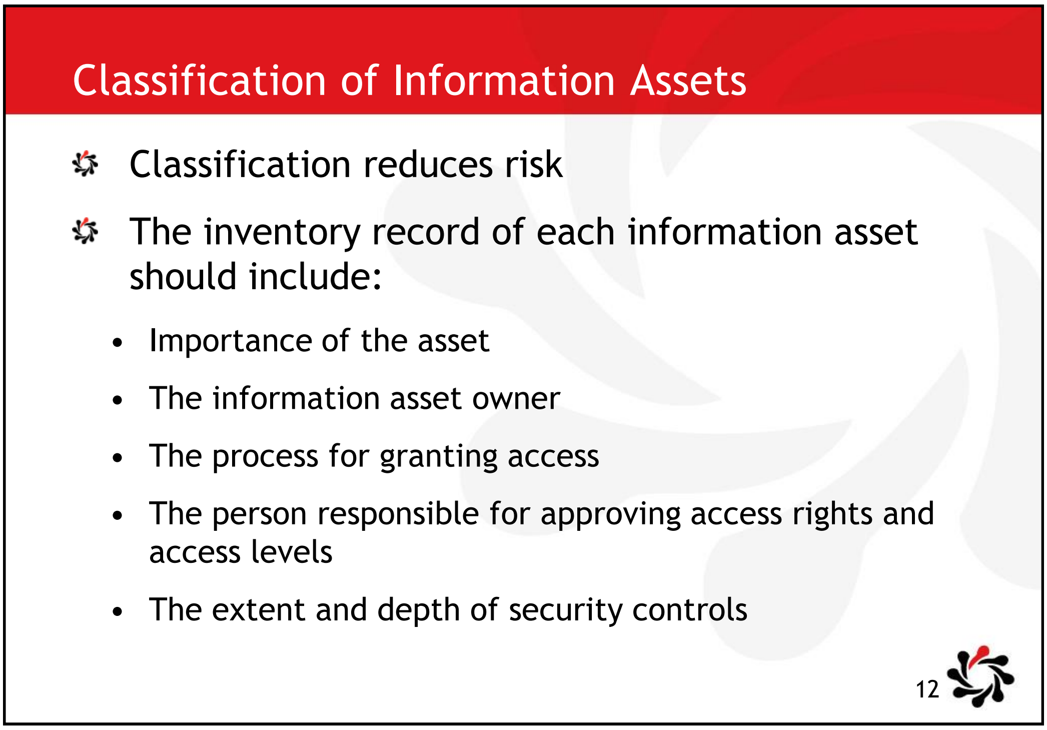
Key Elements of Information Security Management

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



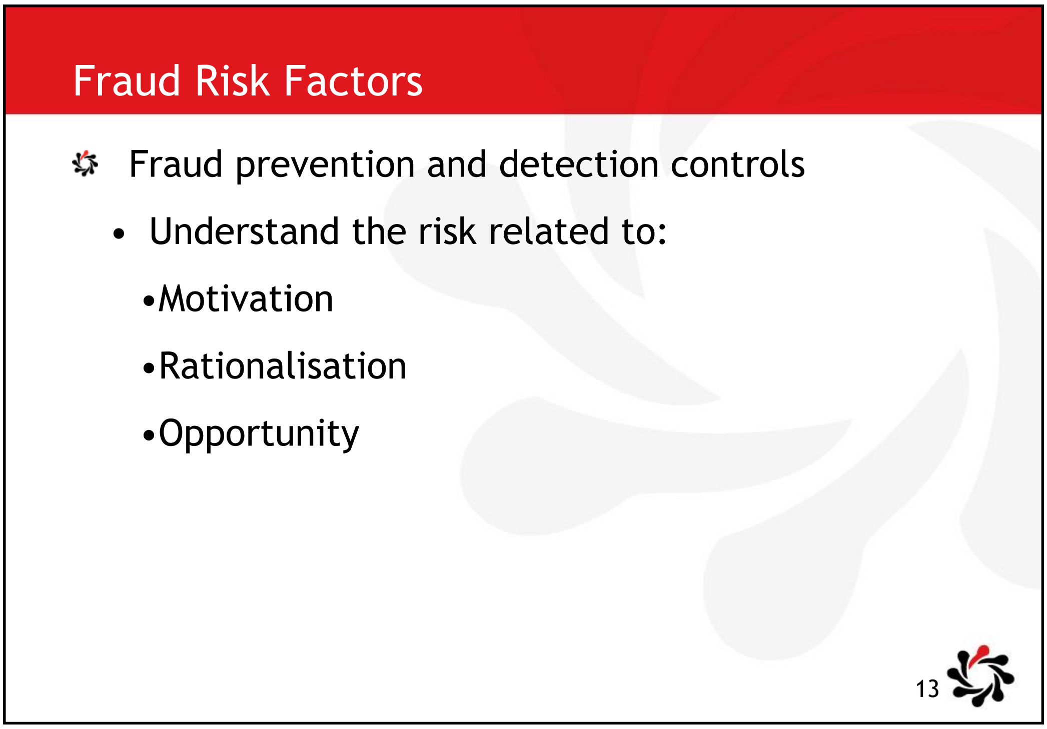
Critical Success Factors to Information Security Management

- 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
- Clearly defined roles and responsibility for information security



Classification of Information Assets

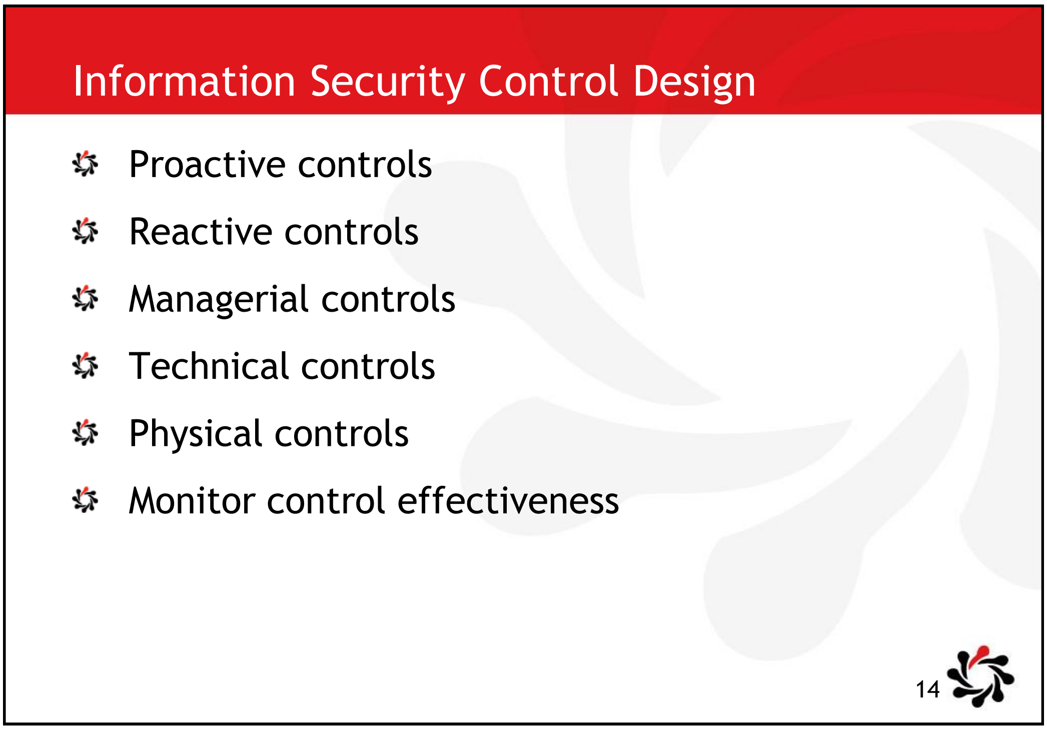
- Classification reduces risk
- The inventory record of each information asset should include:
  - Importance of the asset
  - The information asset owner
  - The process for granting access
  - The person responsible for approving access rights and access levels
  - The extent and depth of security controls



Fraud Risk Factors

- Fraud prevention and detection controls
  - Understand the risk related to:
    - Motivation
    - Rationalisation
    - Opportunity

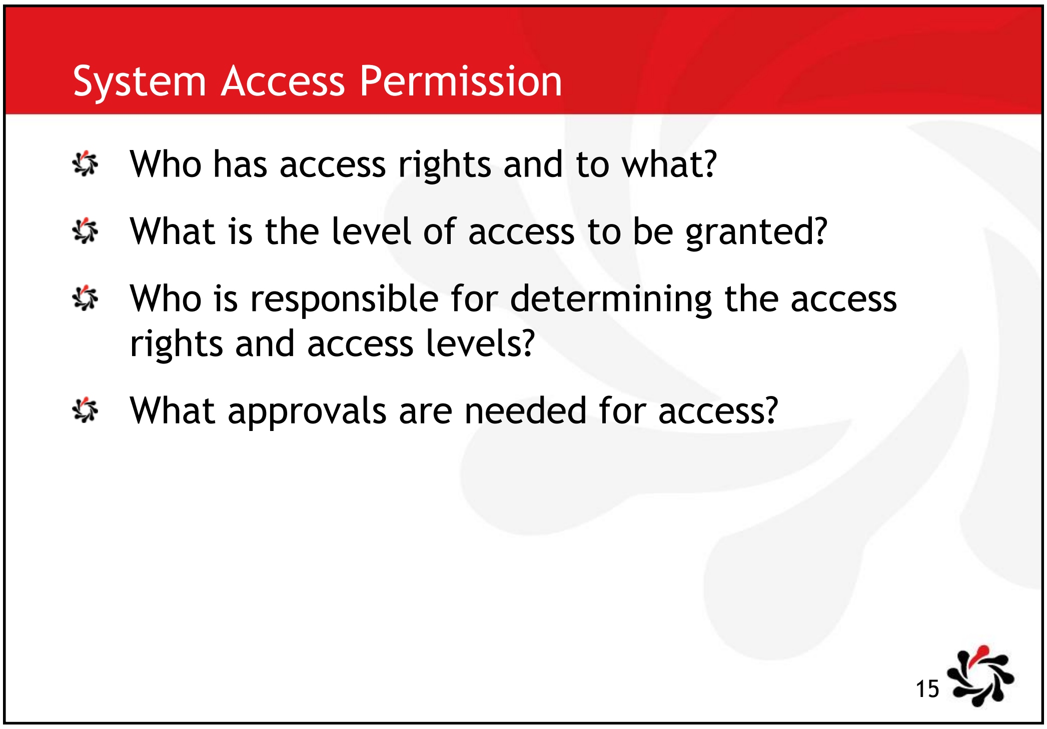
13



Information Security Control Design

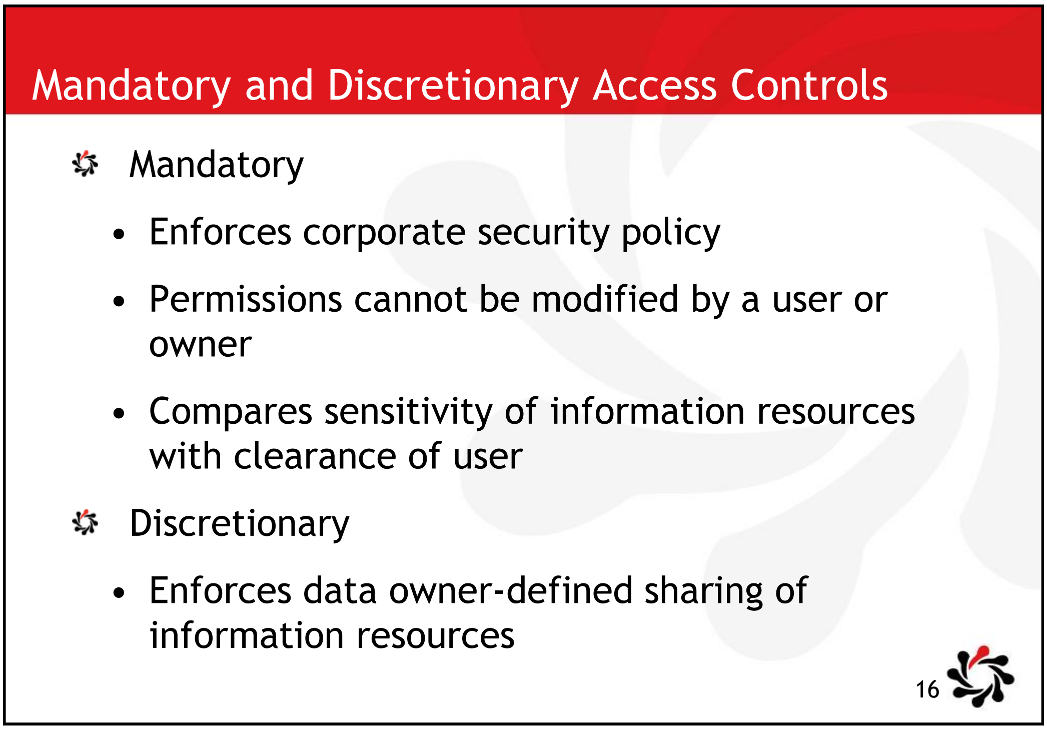
- Proactive controls
- Reactive controls
- Managerial controls
- Technical controls
- Physical controls
- Monitor control effectiveness

14



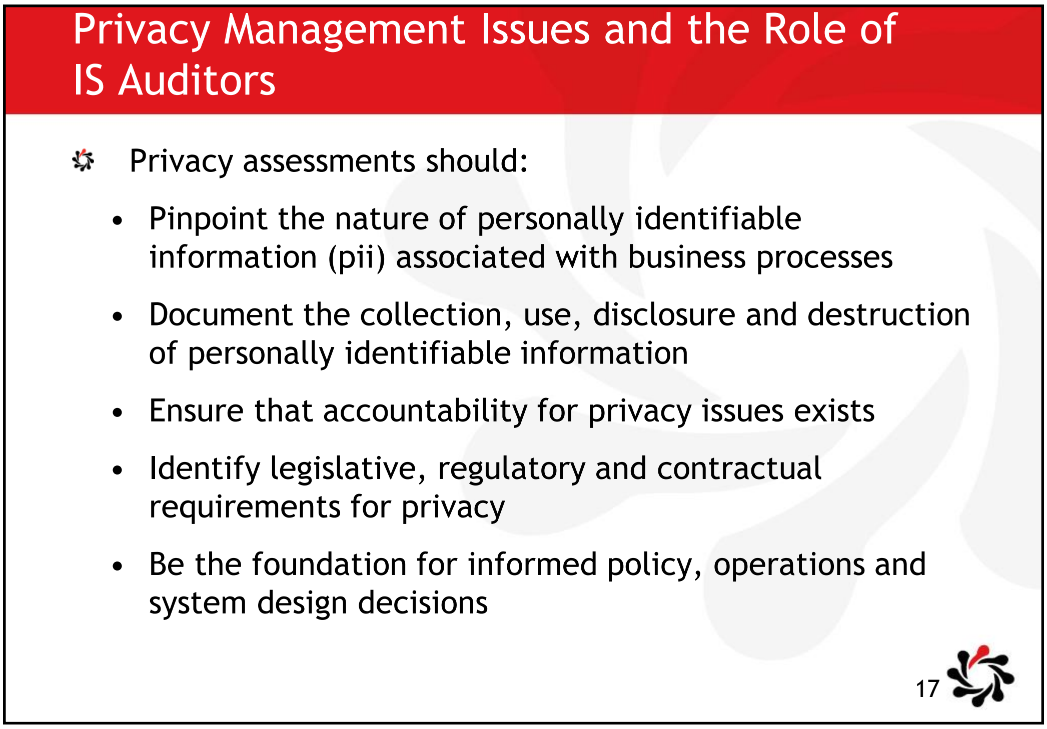
System Access Permission

- 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

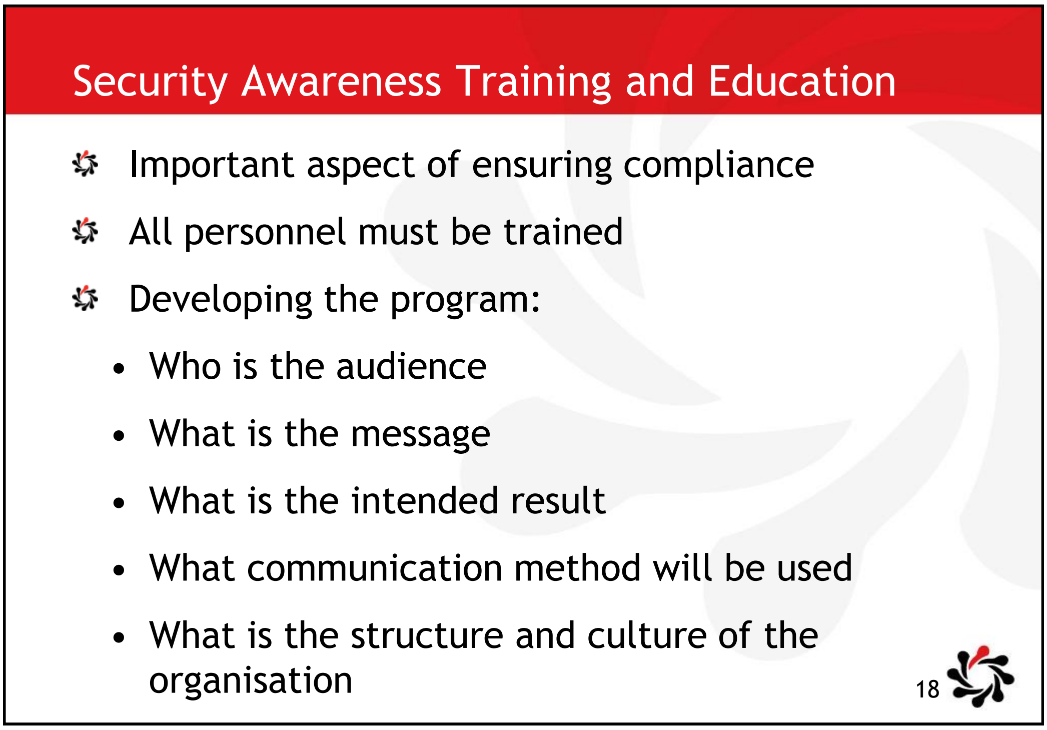
- Mandatory
  - Enforces corporate security policy
  - Permissions cannot be modified by a user or owner
  - Compares sensitivity of information resources with clearance of user
- Discretionary
  - Enforces data owner-defined sharing of information resources



Privacy Management Issues and the Role of IS Auditors

- Privacy assessments should:
  - Pinpoint the nature of personally 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
  - Identify legislative, regulatory and contractual requirements for privacy
  - Be the foundation for informed policy, operations and system design decisions

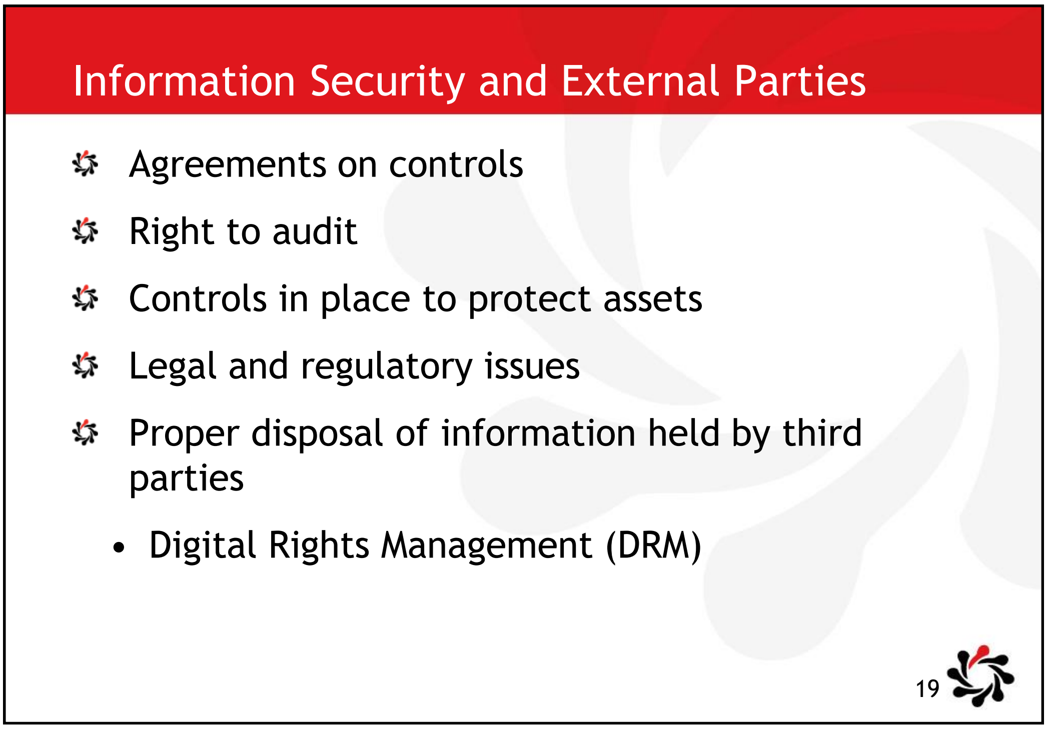
17



Security Awareness Training and Education

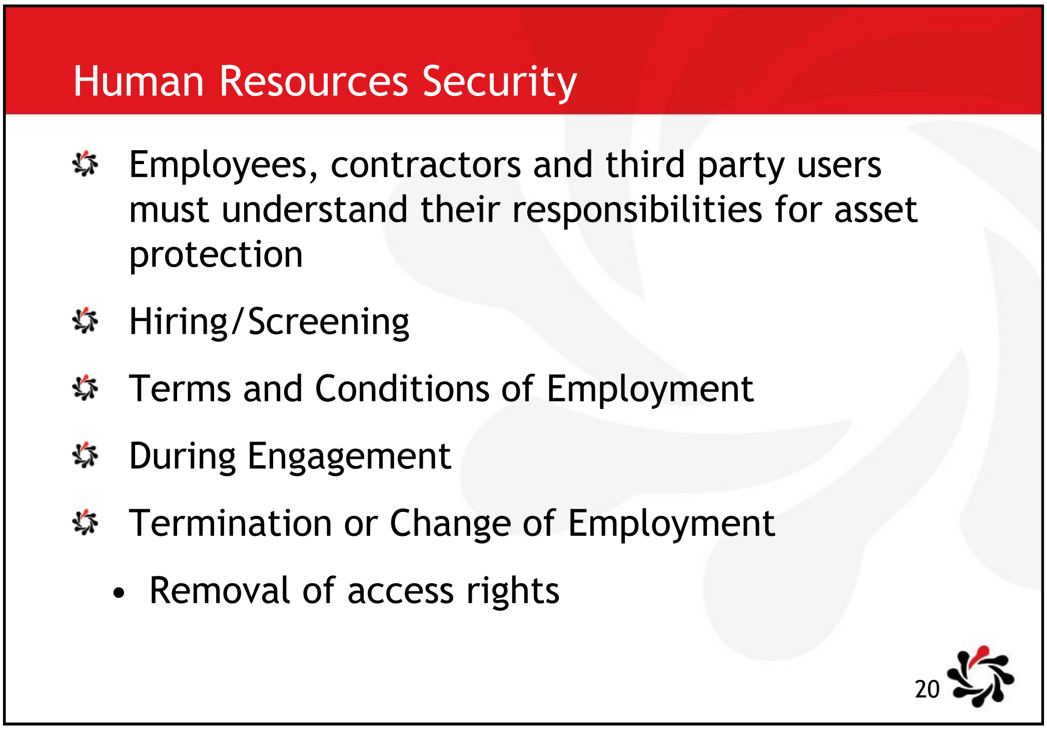
- Important aspect of ensuring compliance
- All personnel must be trained
- Developing the program:
  - Who is the audience
  - What is the message
  - What is the intended result
  - What communication method will be used
  - What is the structure and culture of the organisation

18



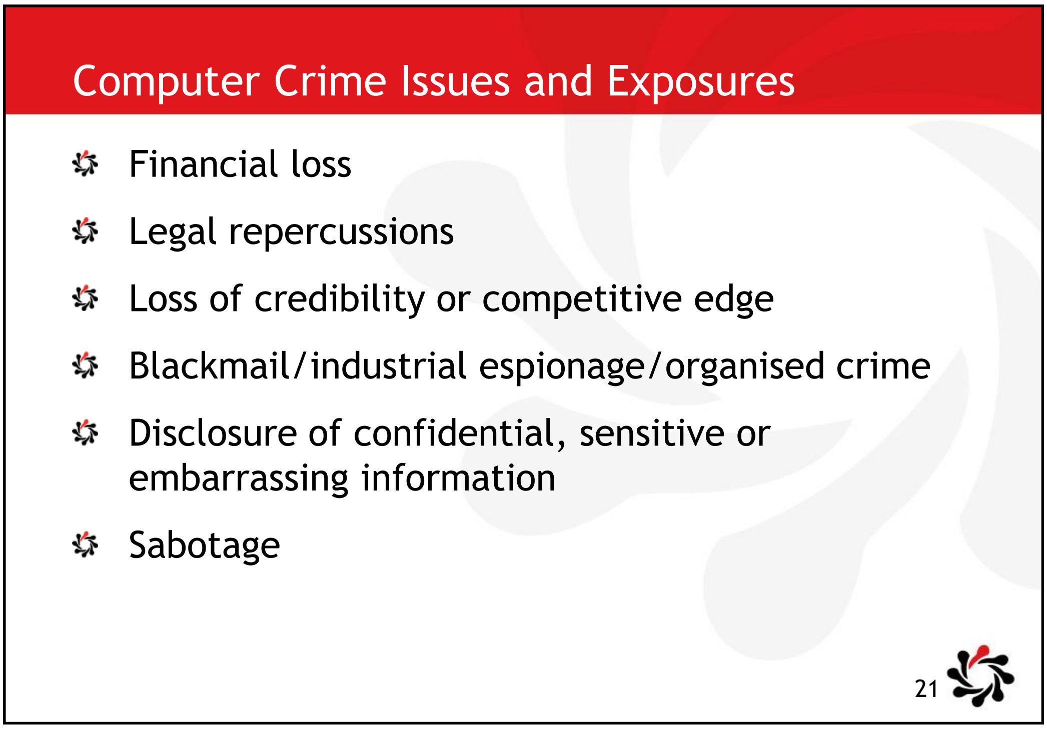
Information Security and External Parties

- Agreements on controls
- Right to audit
- Controls in place to protect assets
- Legal and regulatory issues
- Proper disposal of information held by third parties
  - Digital Rights Management (DRM)



Human Resources Security

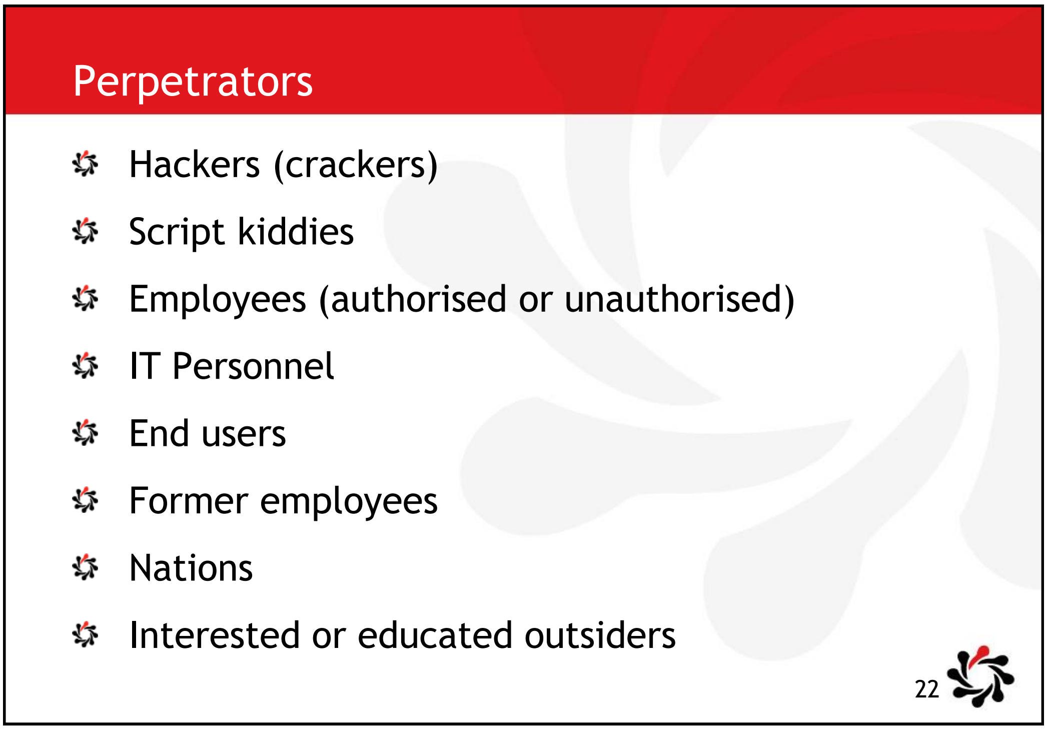
- Employees, contractors and third party users must understand their responsibilities for asset protection
- Hiring/Screening
- Terms and Conditions of Employment
- During Engagement
- Termination or Change of Employment
  - Removal of access rights



Computer Crime Issues and Exposures

- Financial loss
- Legal repercussions
- Loss of credibility or competitive edge
- Blackmail/industrial espionage/organised crime
- Disclosure of confidential, sensitive or embarrassing information
- Sabotage

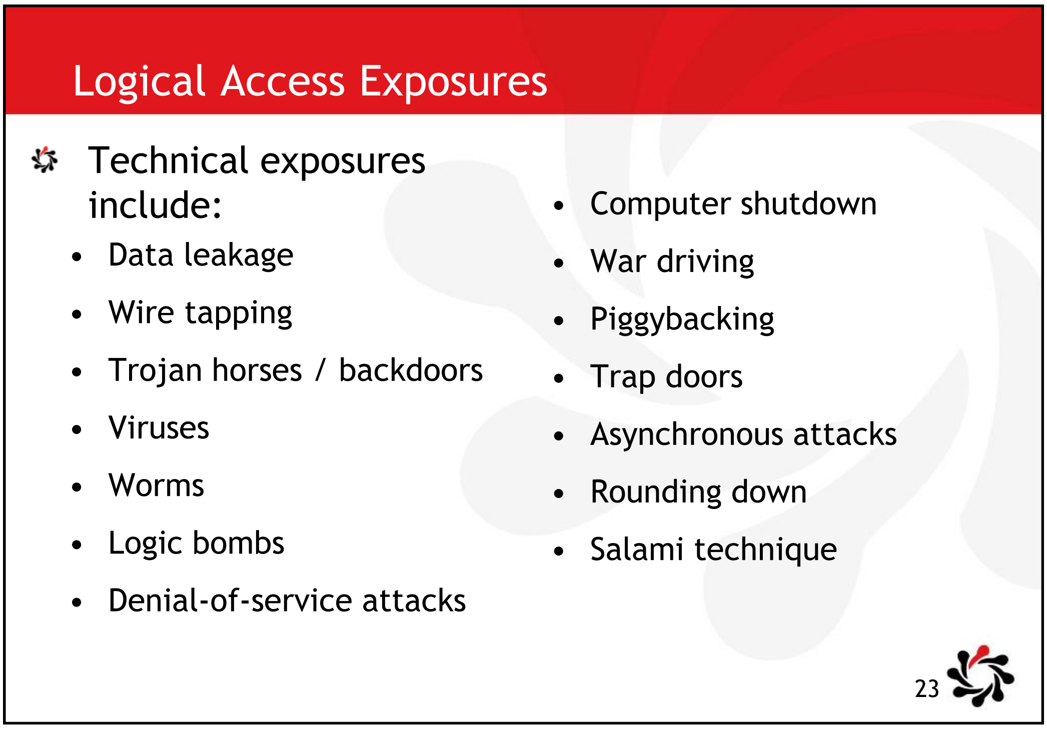
21



Perpetrators

- Hackers (crackers)
- Script kiddies
- Employees (authorised or unauthorised)
- IT Personnel
- End users
- Former employees
- Nations
- Interested or educated outsiders

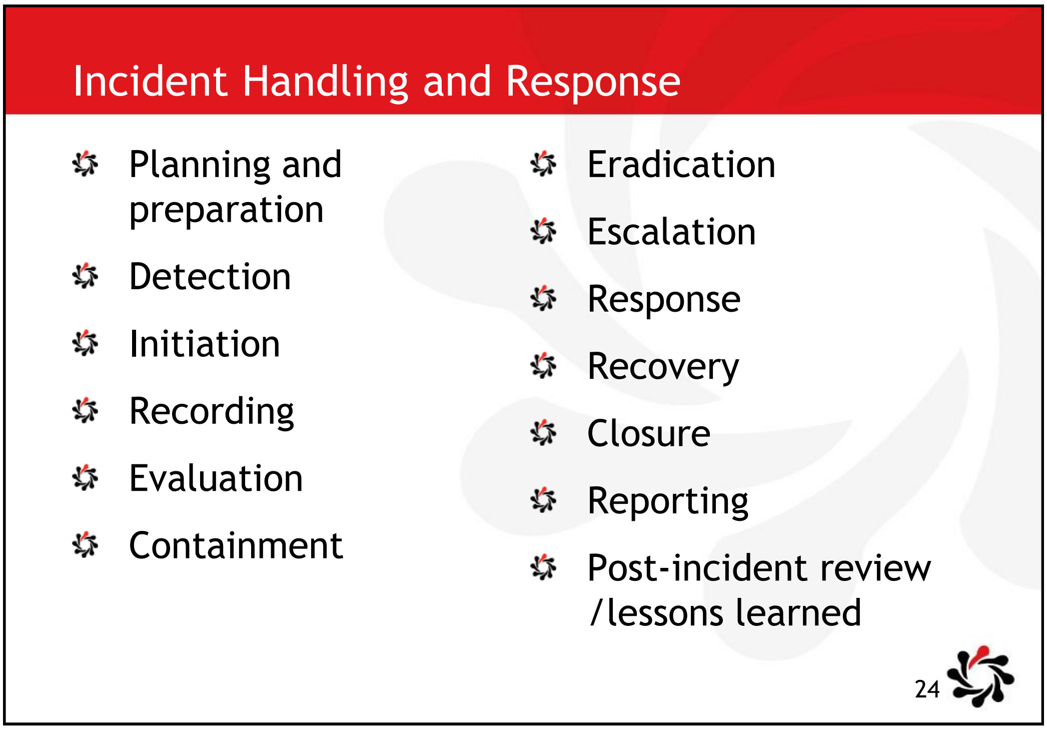
22



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

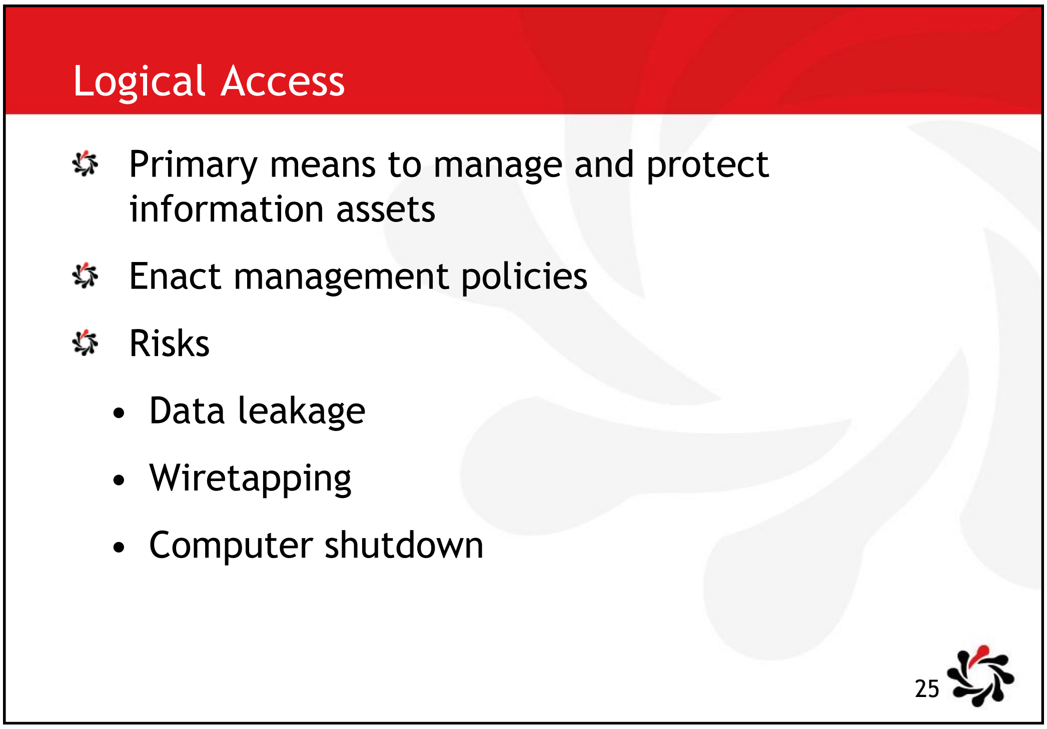
23



Incident Handling and Response

- Planning and preparation
- Detection
- Initiation
- Recording
- Evaluation
- Containment
- Eradication
- Escalation
- Response
- Recovery
- Closure
- Reporting
- Post-incident review /lessons learned

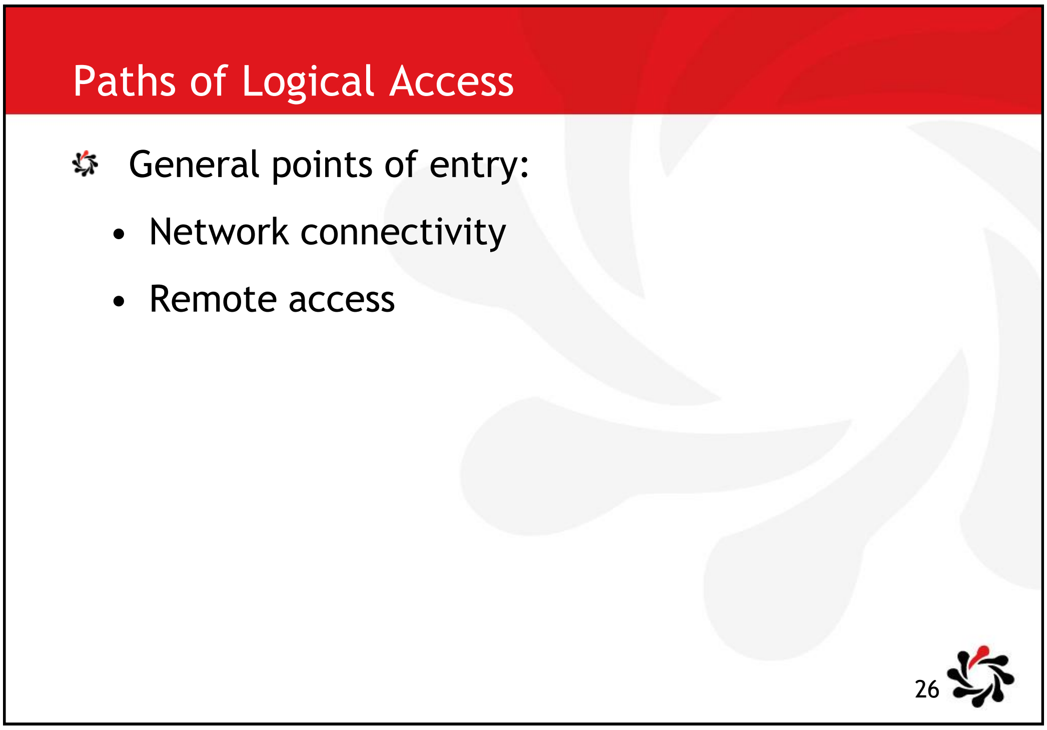
24



Logical Access

- Primary means to manage and protect information assets
- Enact management policies
- Risks
  - Data leakage
  - Wiretapping
  - Computer shutdown

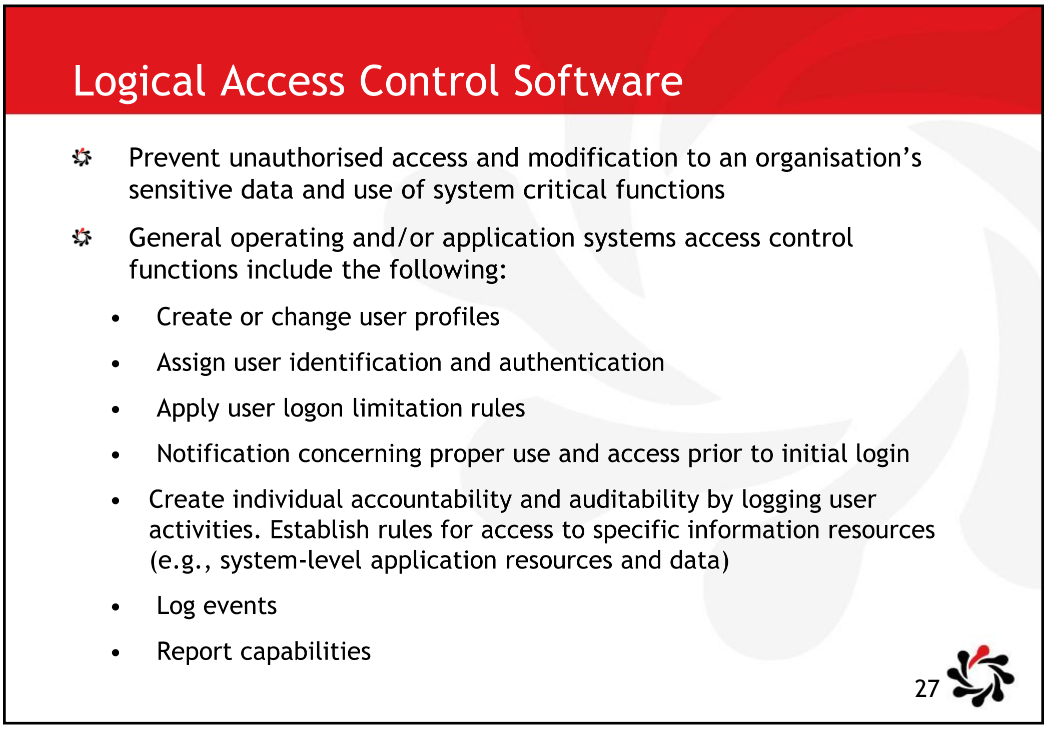
25



Paths of Logical Access

- General points of entry:
  - Network connectivity
  - Remote access

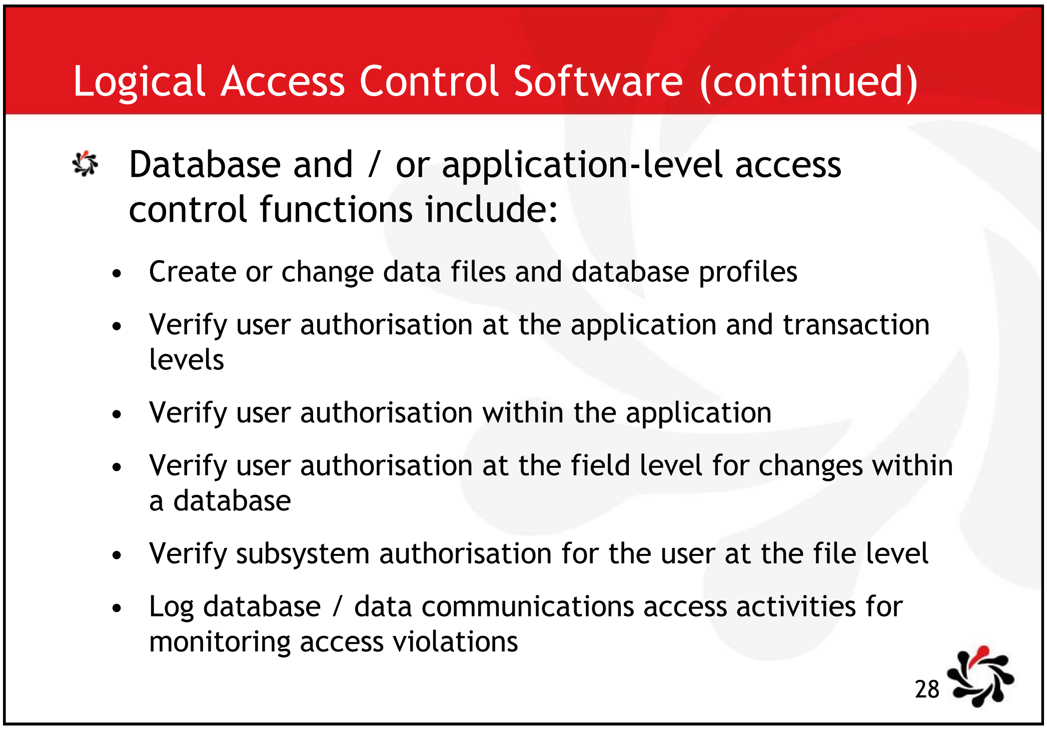
26



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

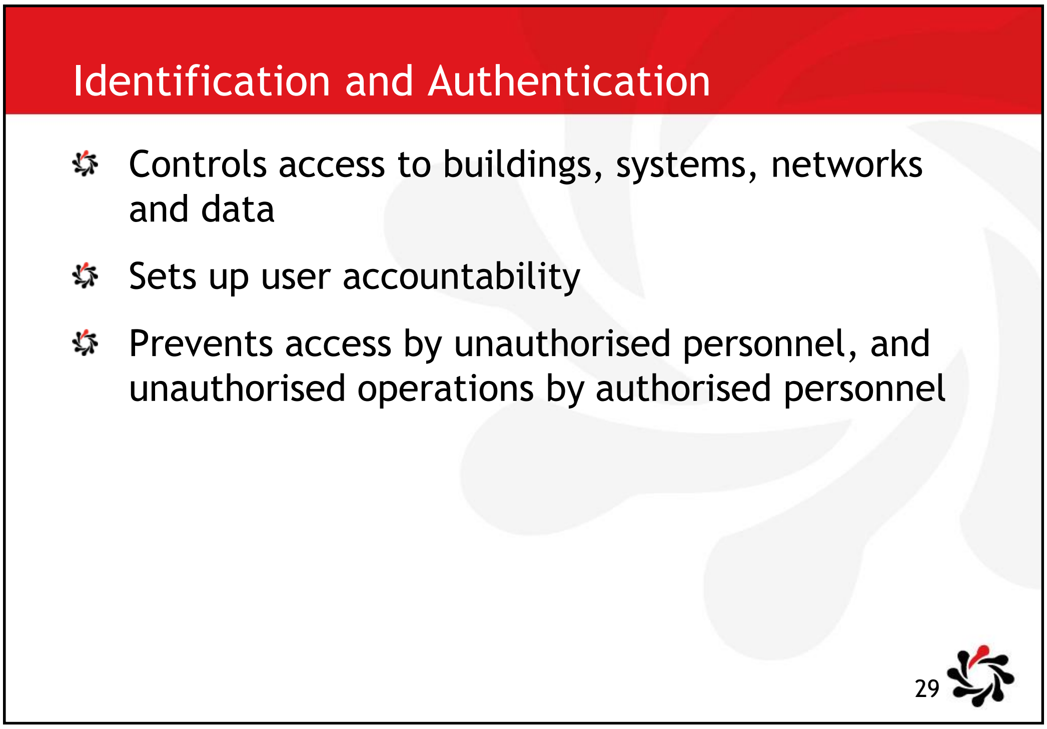
27



Logical Access Control Software (continued)

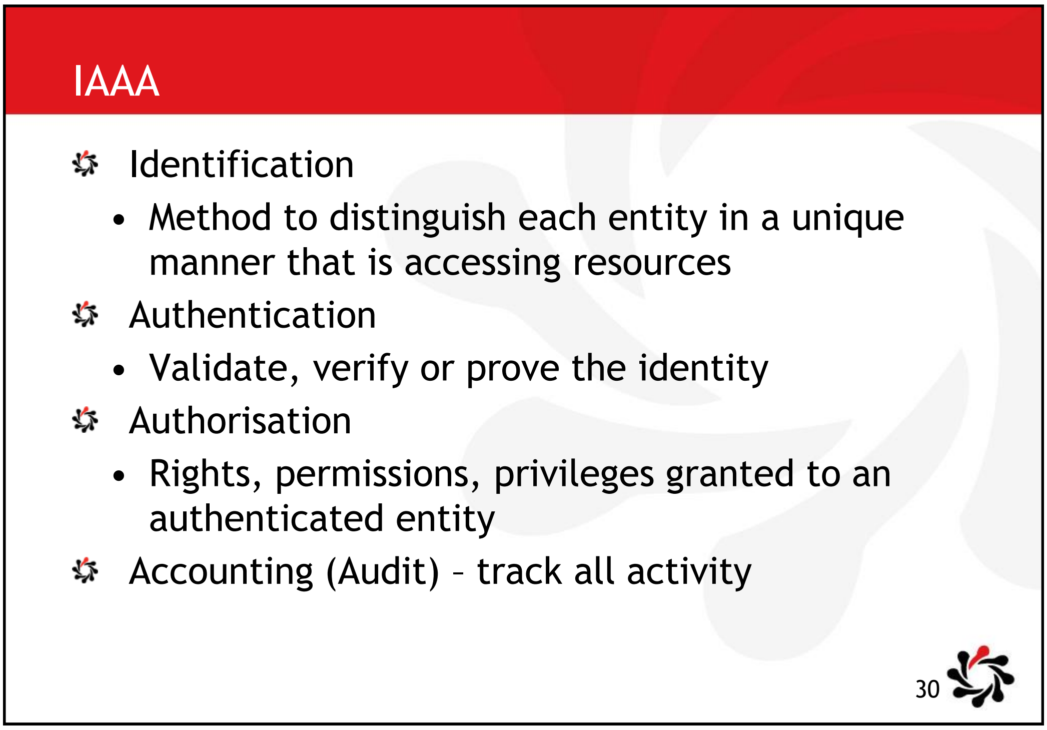
- Database and / or application-level access control functions include:
  - Create or change data files and database profiles
  - Verify user authorisation at the application and transaction levels
  - Verify user authorisation within the application
  - Verify user authorisation at the field level for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

28



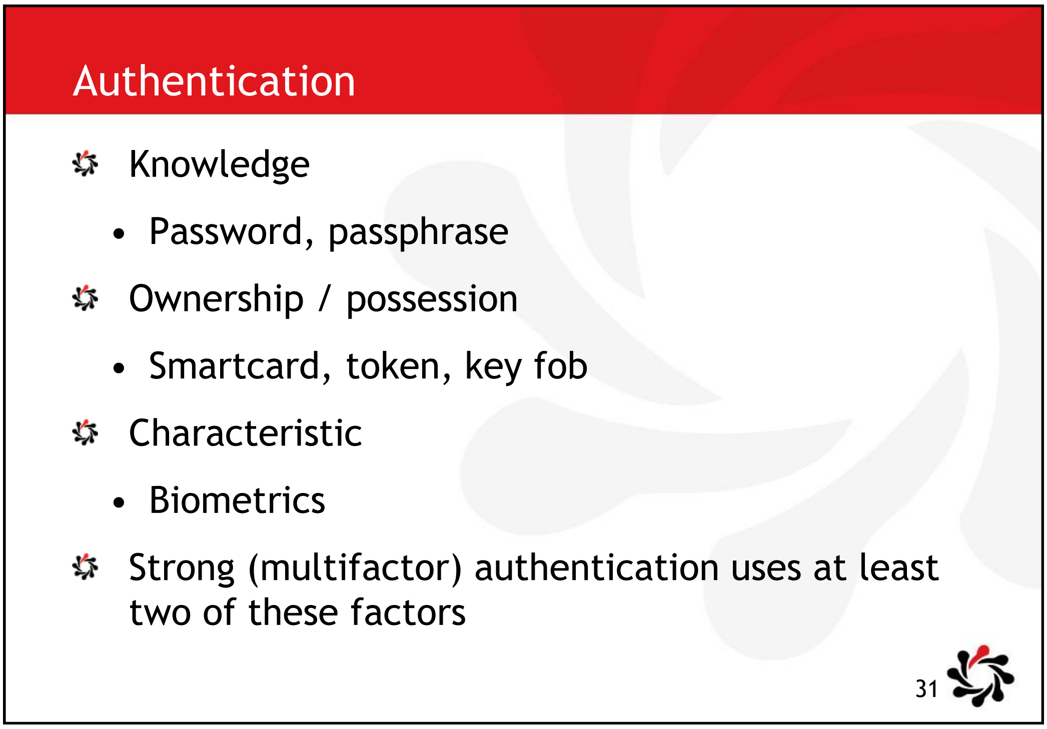
Identification and Authentication

- Controls access to buildings, systems, networks and data
- Sets up user accountability
- Prevents access by unauthorised personnel, and unauthorised operations by authorised personnel



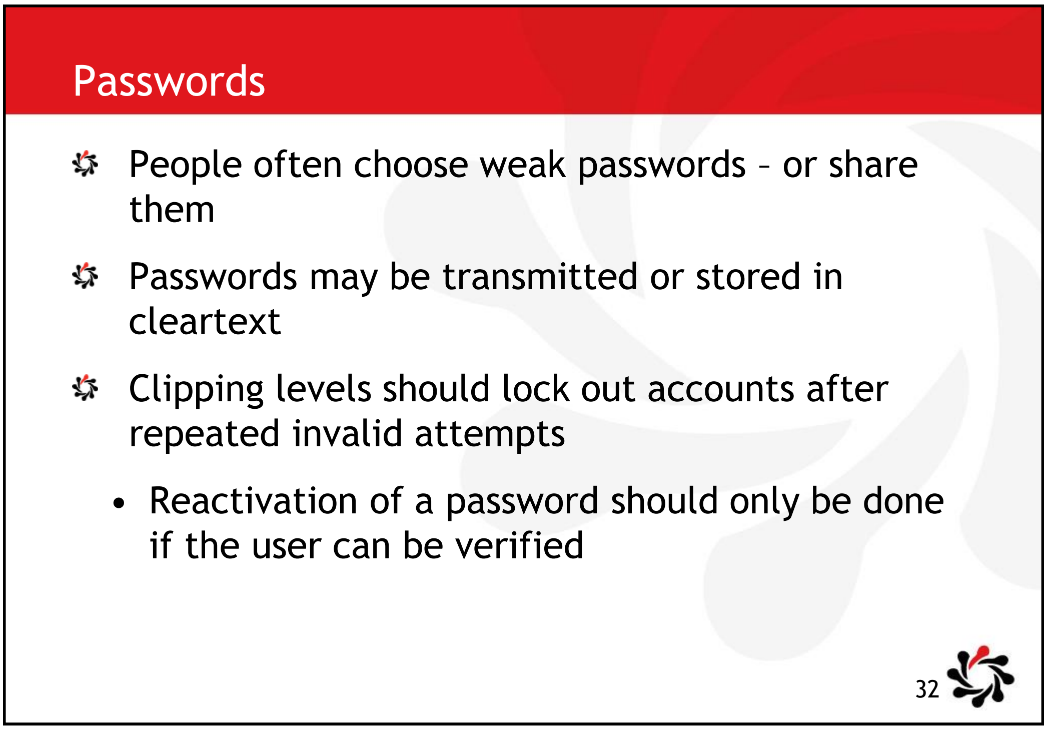
IAAA

- 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



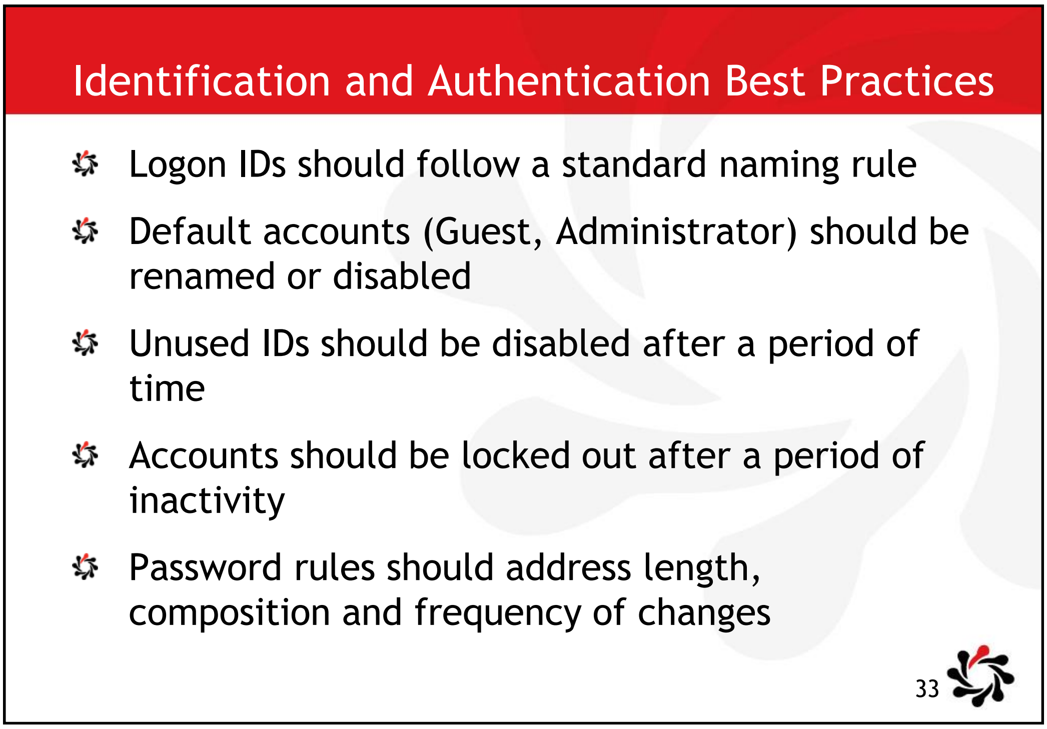
Authentication

- Knowledge
  - Password, passphrase
- Ownership / possession
  - Smartcard, token, key fob
- Characteristic
  - Biometrics
- Strong (multifactor) authentication uses at least two of these factors



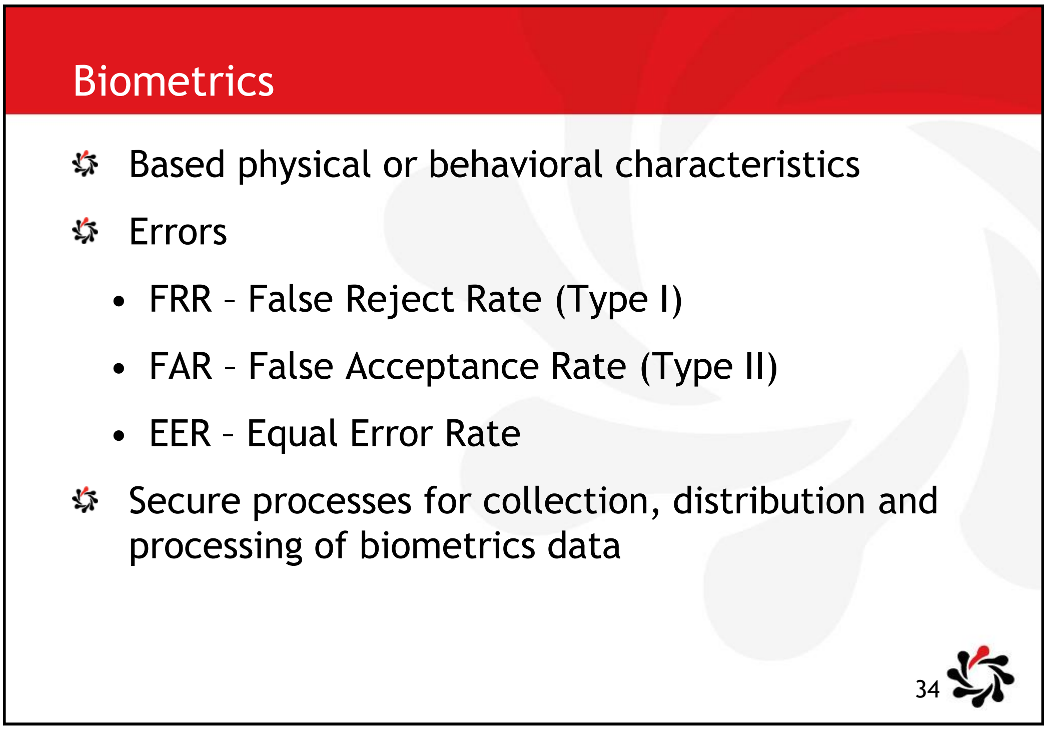
Passwords

- People often choose weak passwords – or share them
- Passwords may be transmitted or stored in cleartext
- Clipping levels should lock out accounts after repeated invalid attempts
  - Reactivation of a password should only be done if the user can be verified



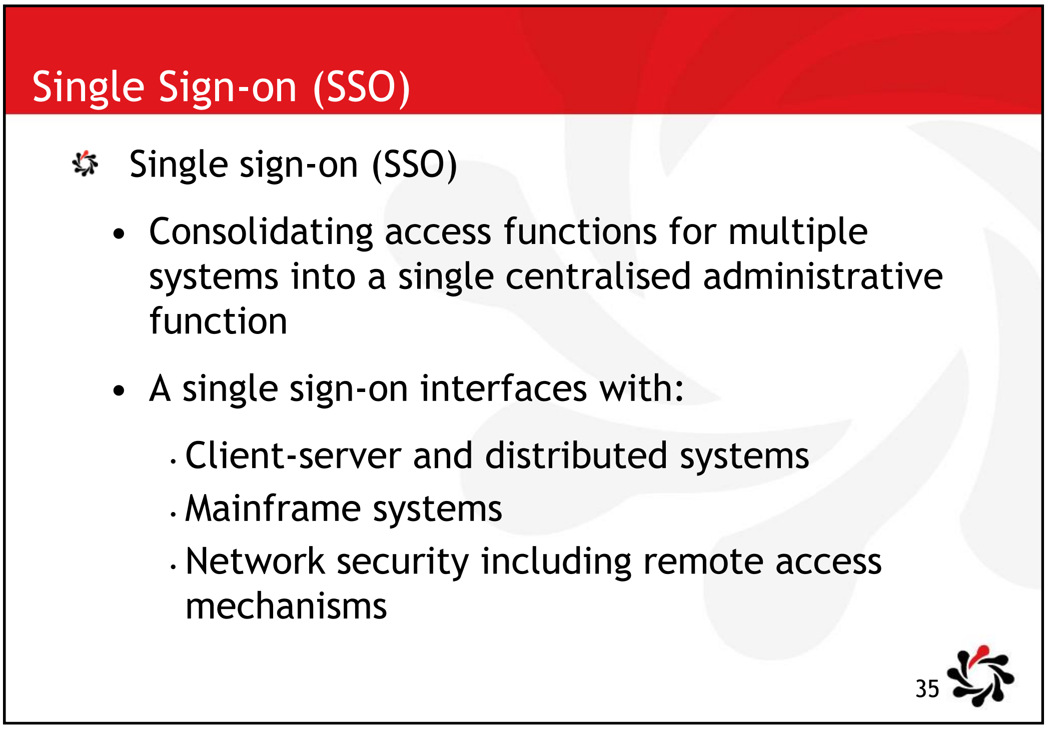
Identification and Authentication Best Practices

- Logon IDs should follow a standard naming rule
- Default accounts (Guest, Administrator) should be renamed or disabled
- Unused IDs should be disabled after a period of time
- Accounts should be locked out after a period of inactivity
- Password rules should address length, composition and frequency of changes



Biometrics

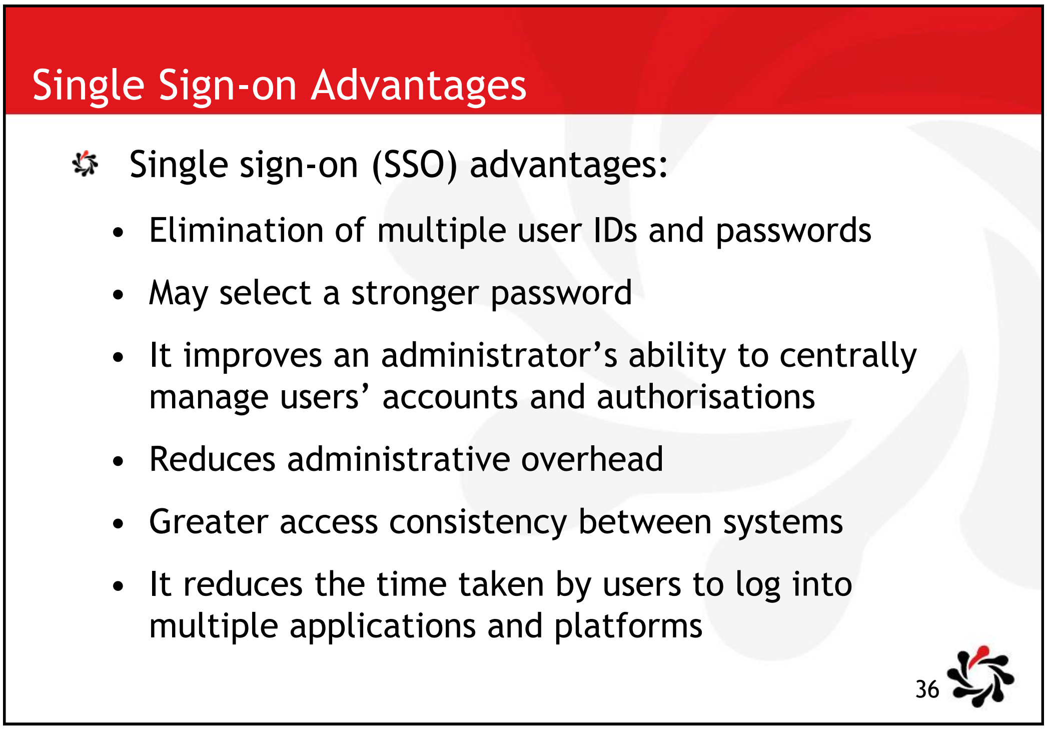
- Based physical or behavioral characteristics
- Errors
  - FRR – False Reject Rate (Type I)
  - FAR – False Acceptance Rate (Type II)
  - EER – Equal Error Rate
- Secure processes for collection, distribution and processing of biometrics data



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

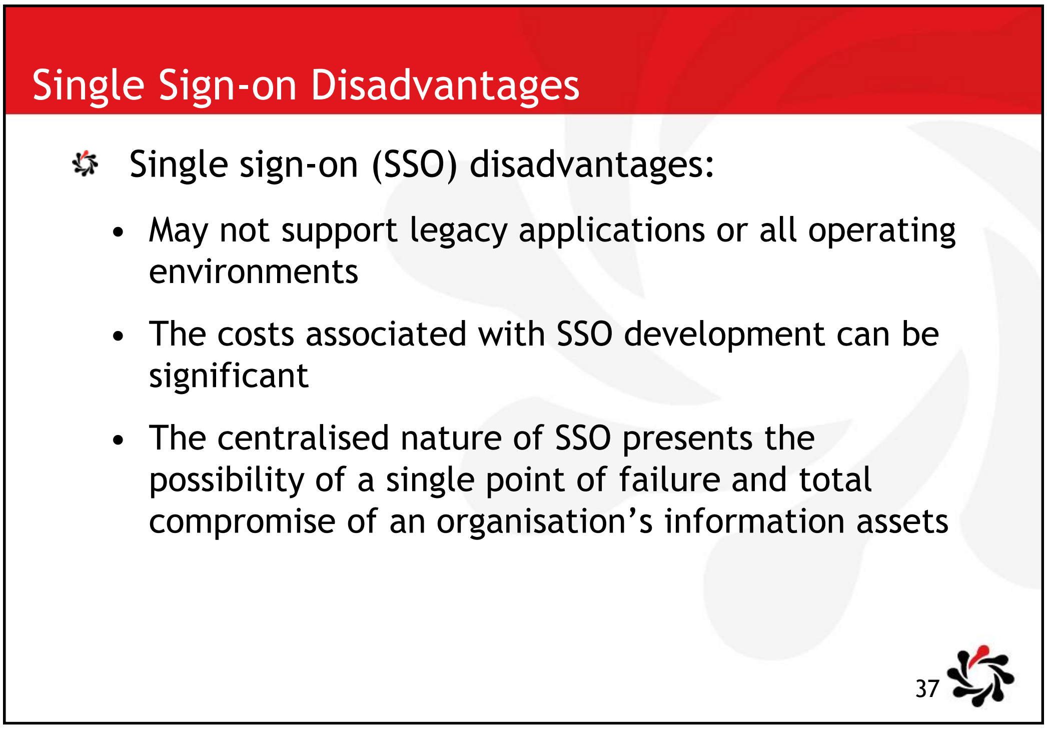
35



Single Sign-on Advantages

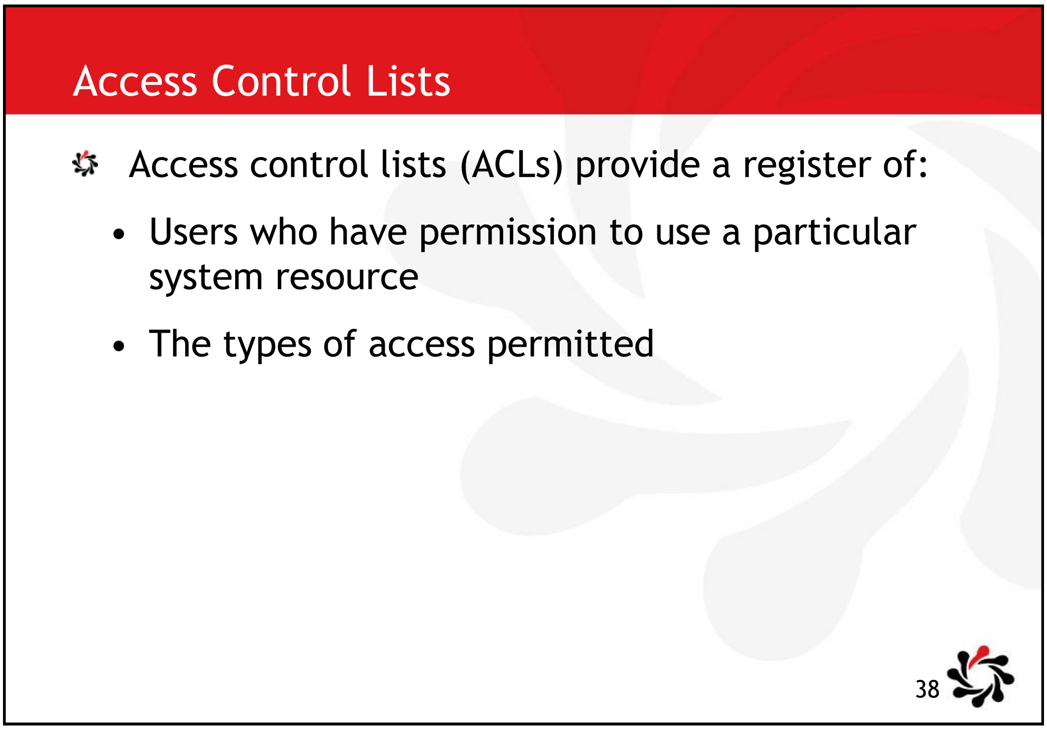
- Single sign-on (SSO) advantages:
  - Elimination of multiple user IDs and passwords
  - May select a stronger password
  - It improves an administrator’s ability to centrally manage users’ accounts and authorisations
  - Reduces administrative overhead
  - Greater access consistency between systems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

36



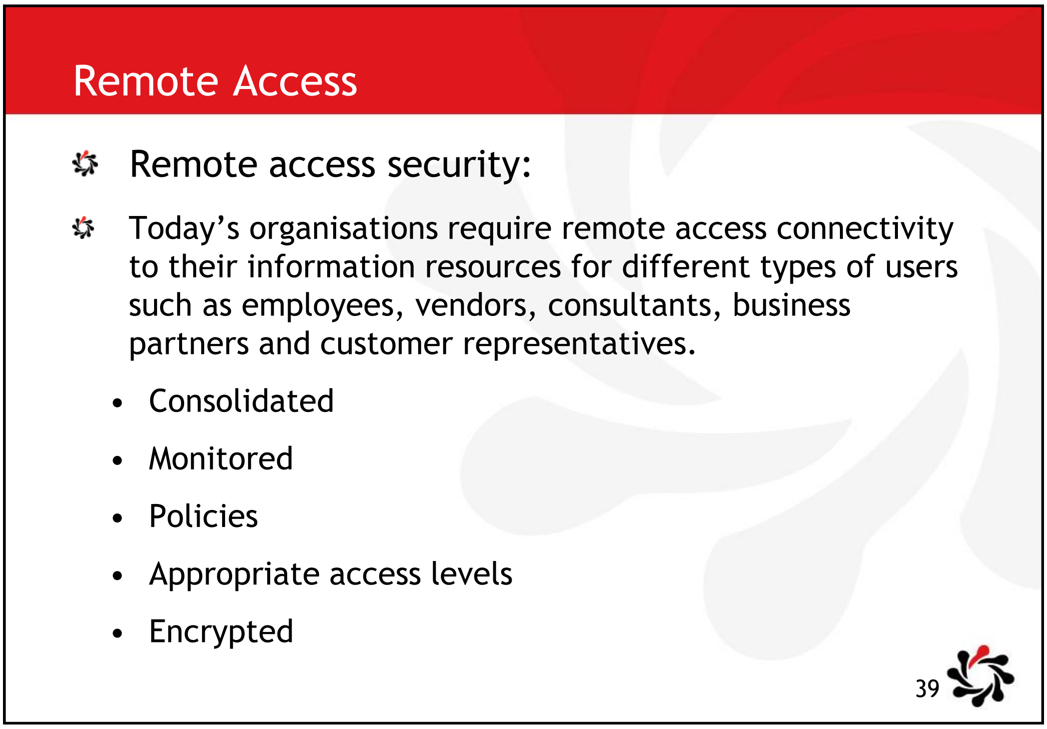
Single Sign-on Disadvantages

- 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



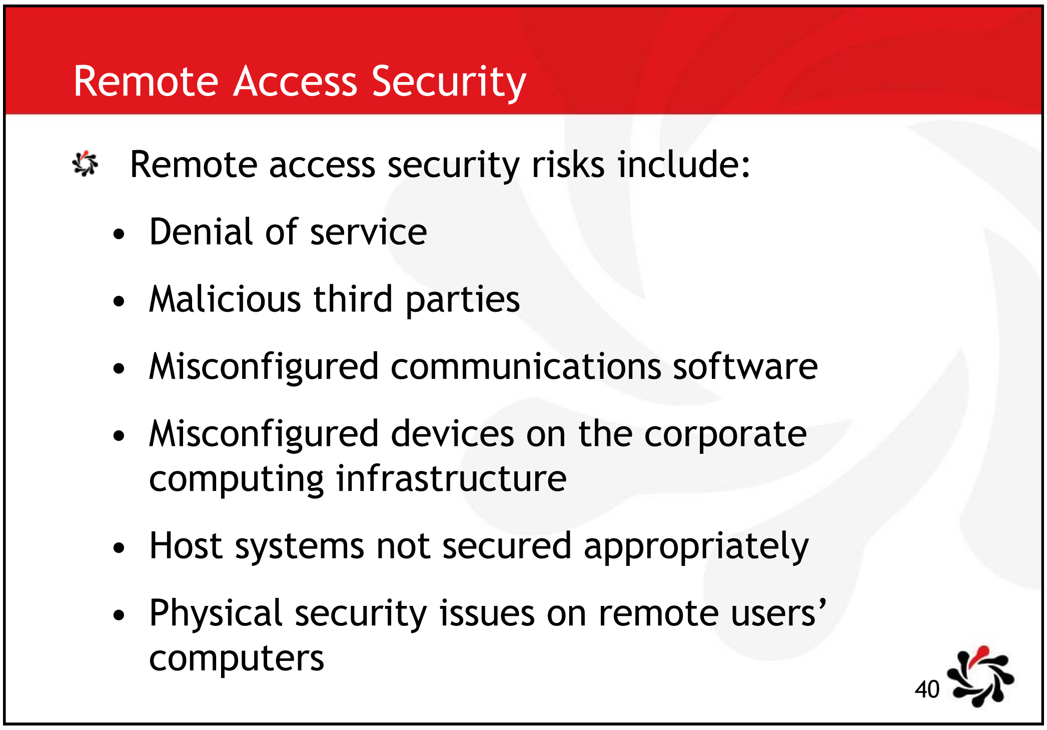
Access Control Lists

- Access control lists (ACLs) provide a register of:
  - Users who have permission to use a particular system resource
  - The types of access permitted



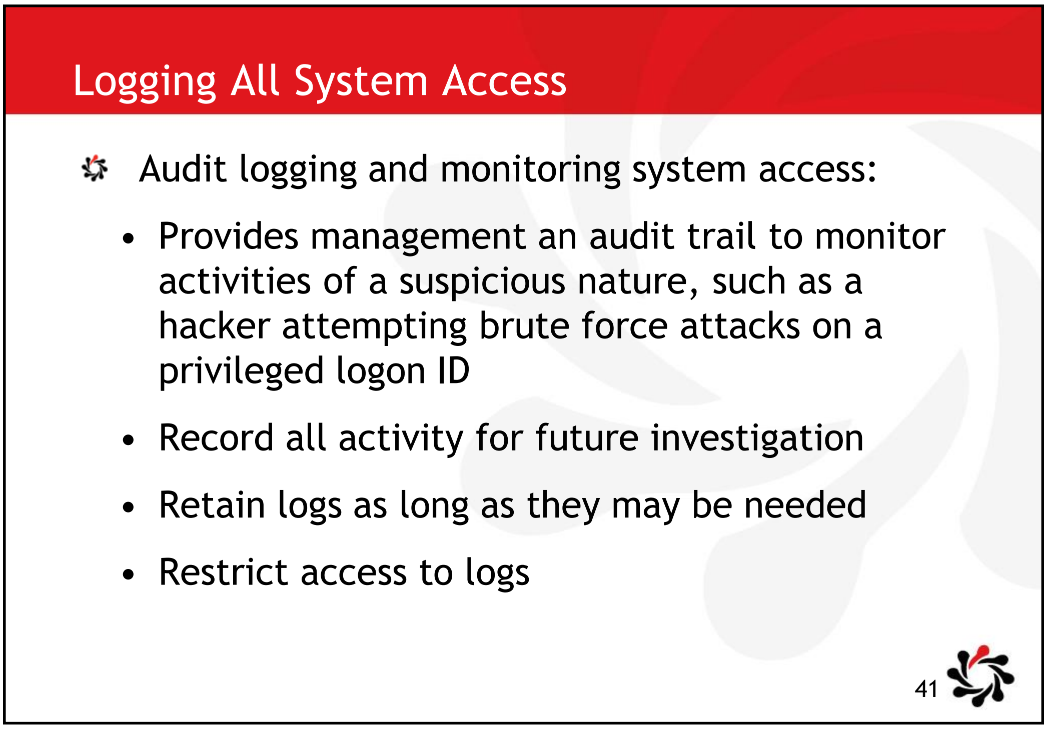
Remote Access

- 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



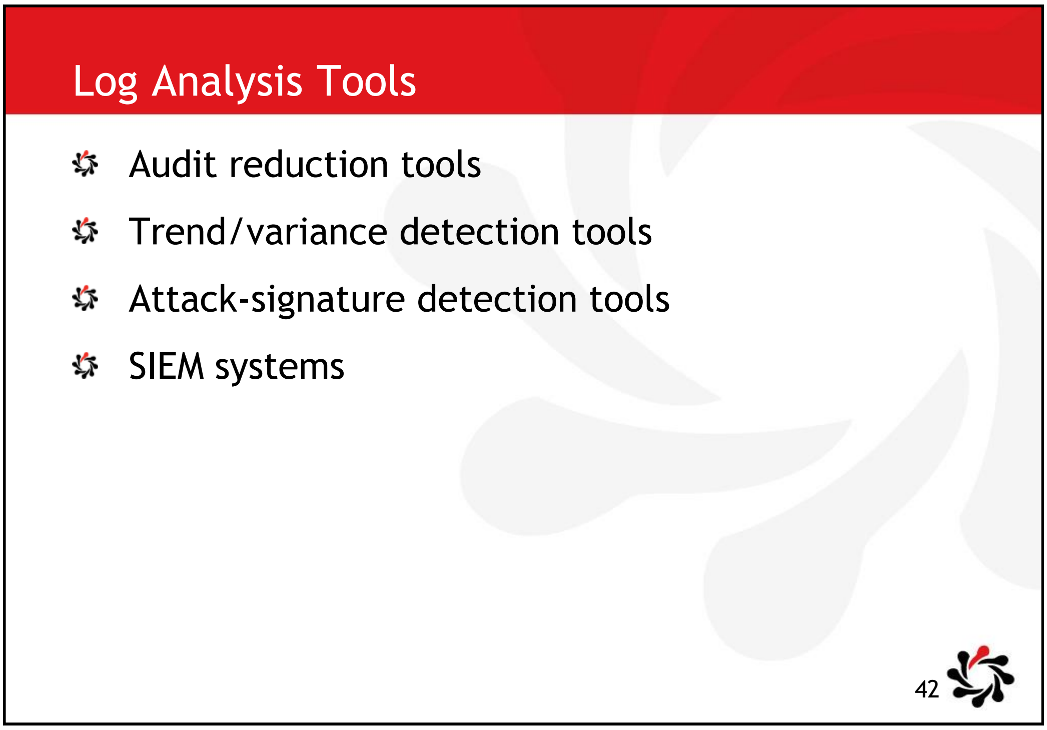
Remote Access Security

- 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



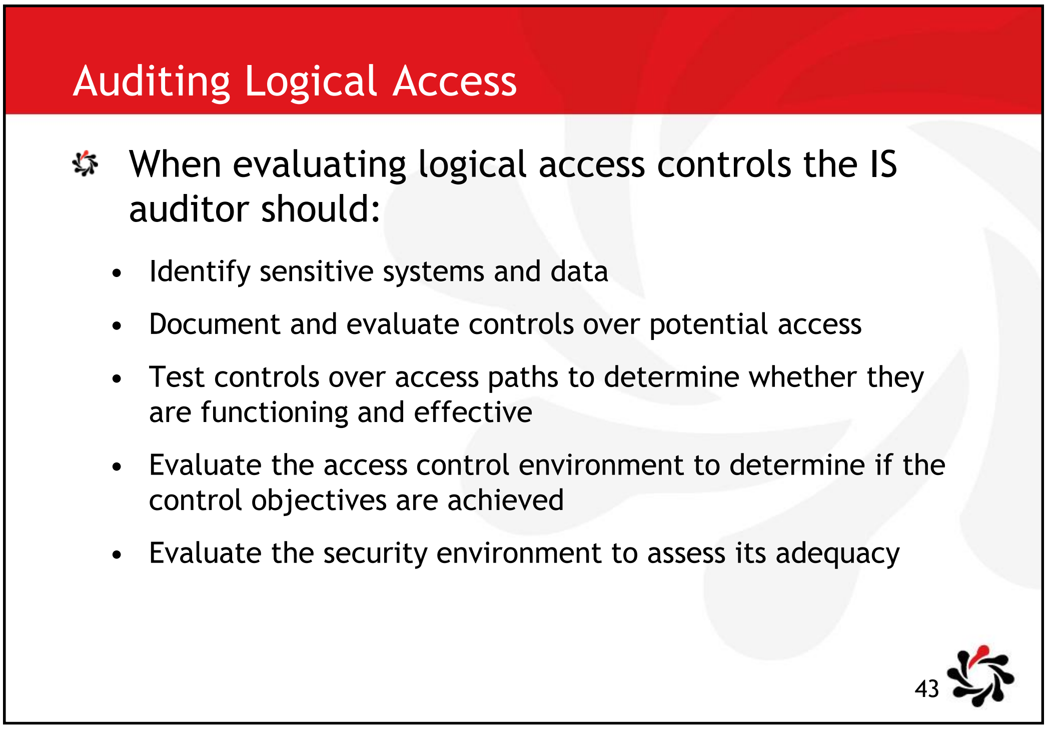
Logging All System Access

- 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
  - Retain logs as long as they may be needed
  - Restrict access to logs



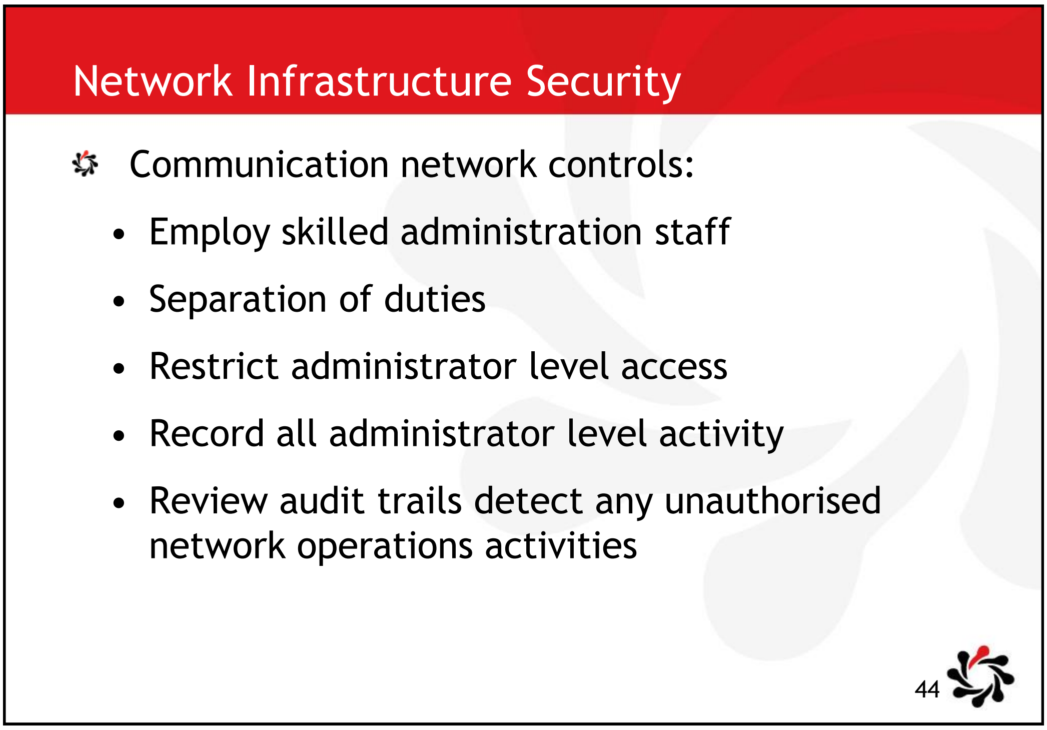
Log Analysis Tools

- Audit reduction tools
- Trend/variance detection tools
- Attack-signature detection tools
- SIEM systems



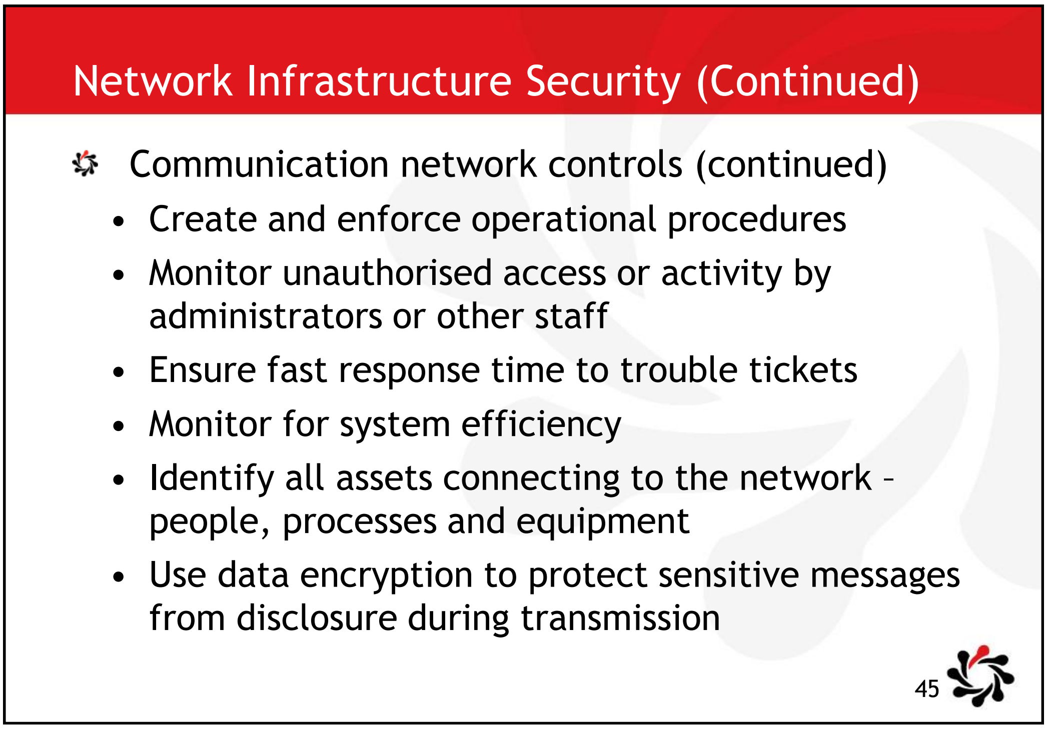
Auditing Logical Access

- 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



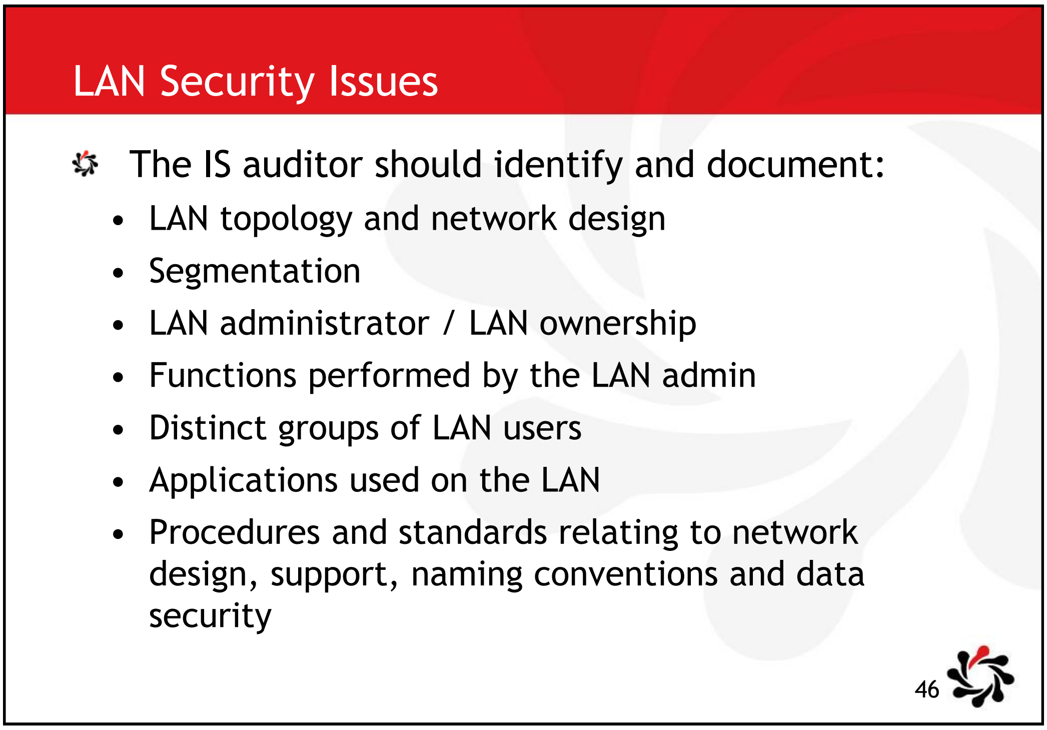
Network Infrastructure Security

- 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



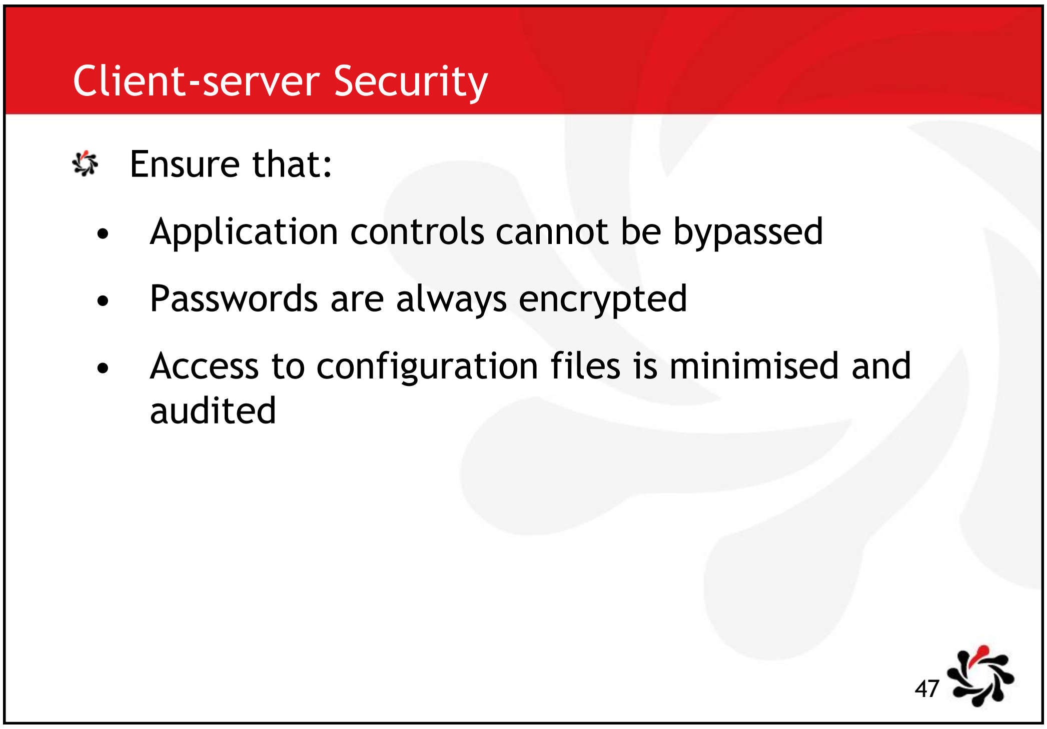
Network Infrastructure Security (Continued)

- 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



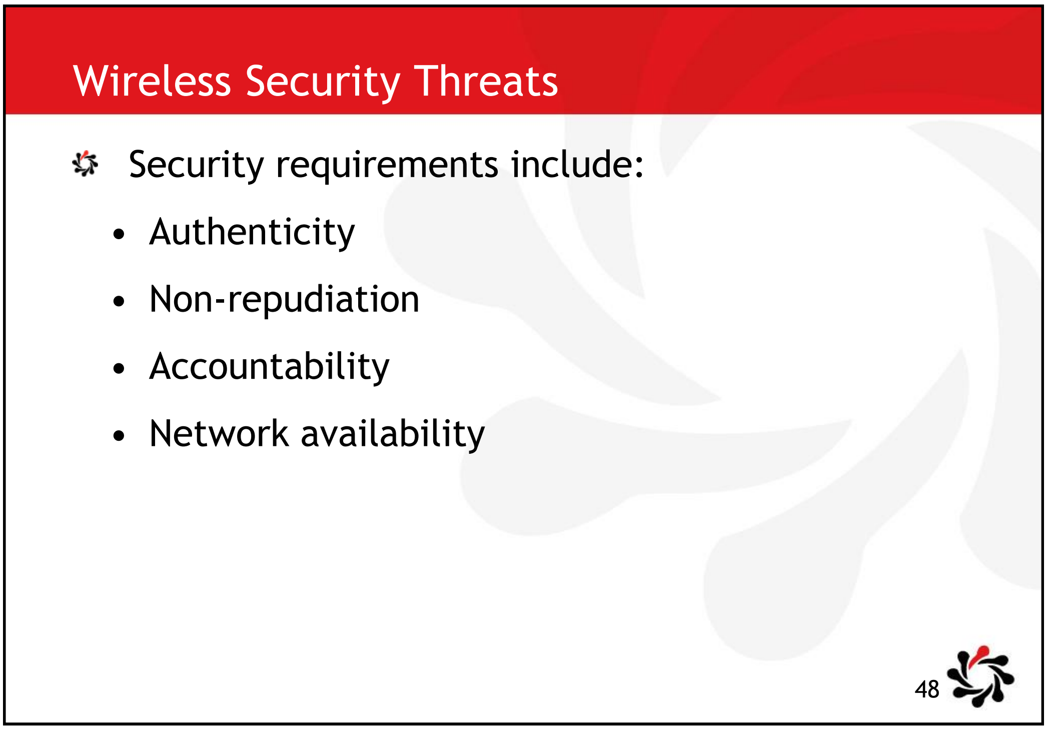
LAN Security Issues

- 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



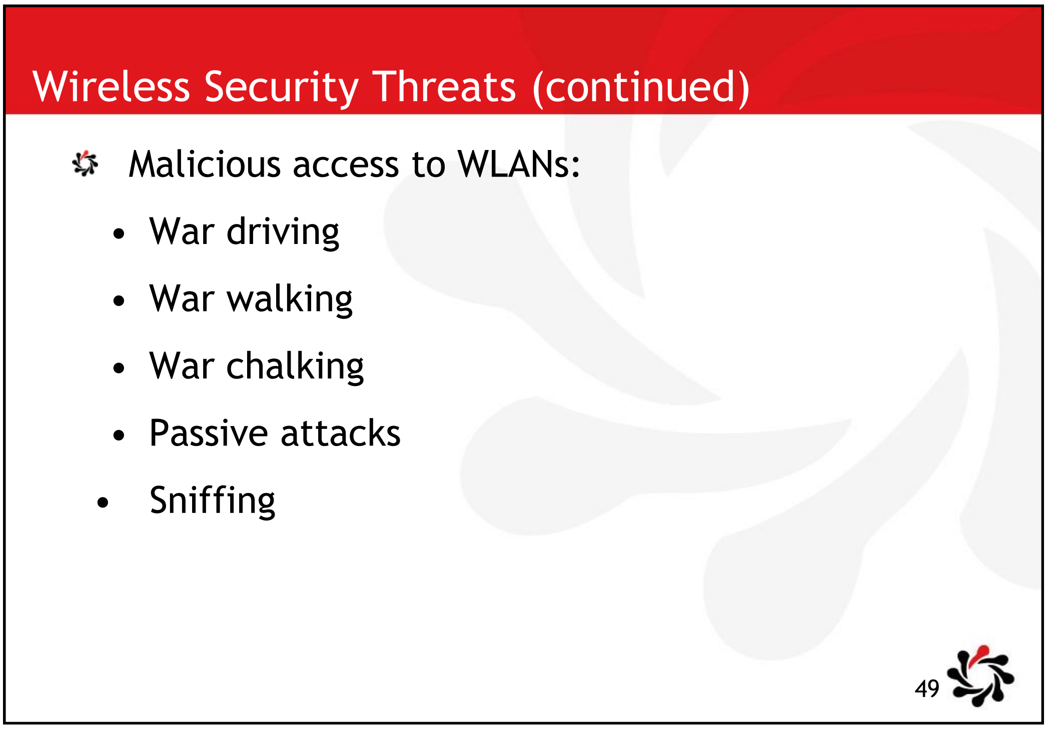
Client-server Security

- Ensure that:
  - Application controls cannot be bypassed
  - Passwords are always encrypted
  - Access to configuration files is minimised and audited



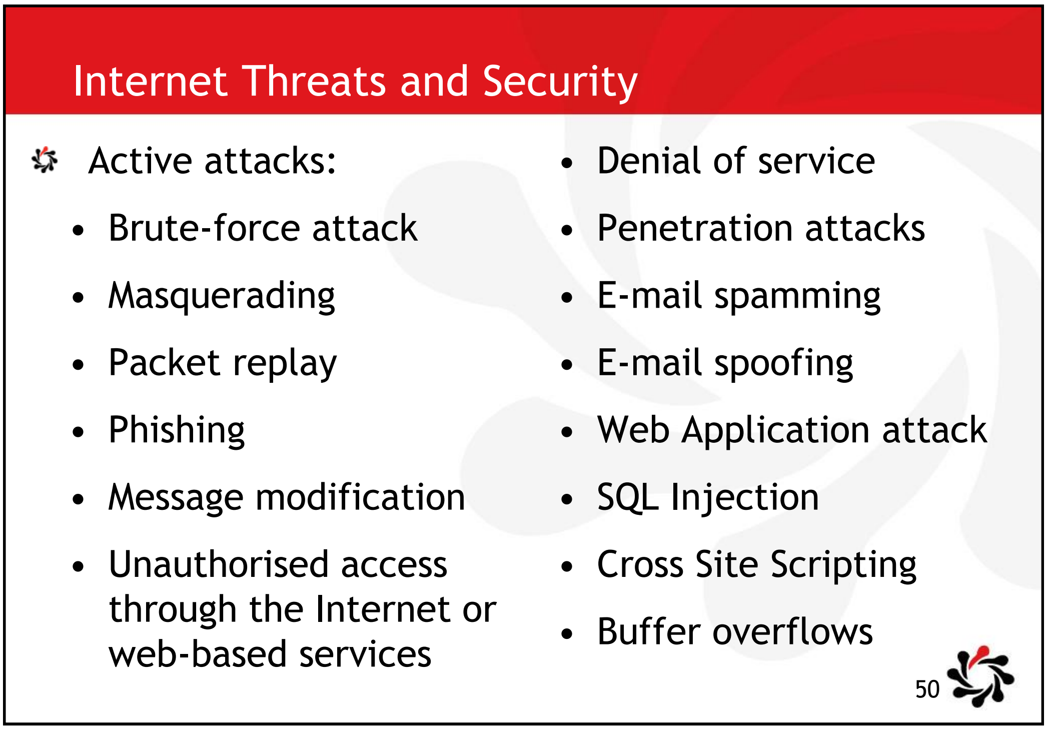
Wireless Security Threats

- Security requirements include:
  - Authenticity
  - Non-repudiation
  - Accountability
  - Network availability



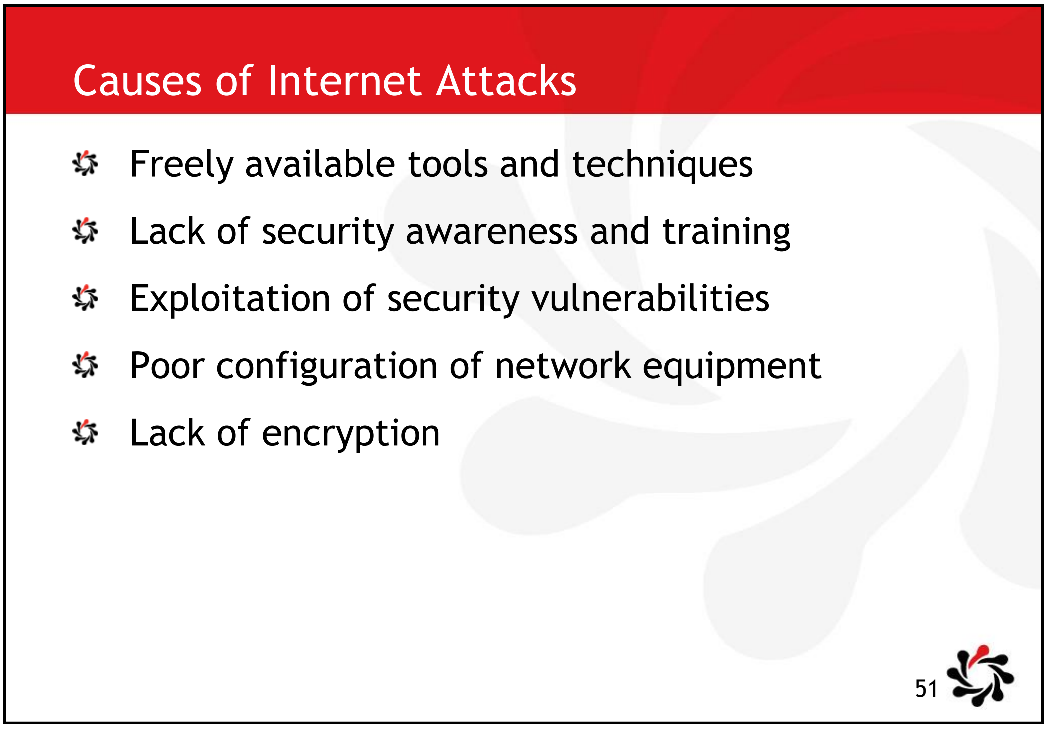
Wireless Security Threats (continued)

- Malicious access to WLANs:
  - War driving
  - War walking
  - War chalking
  - Passive attacks
  - Sniffing



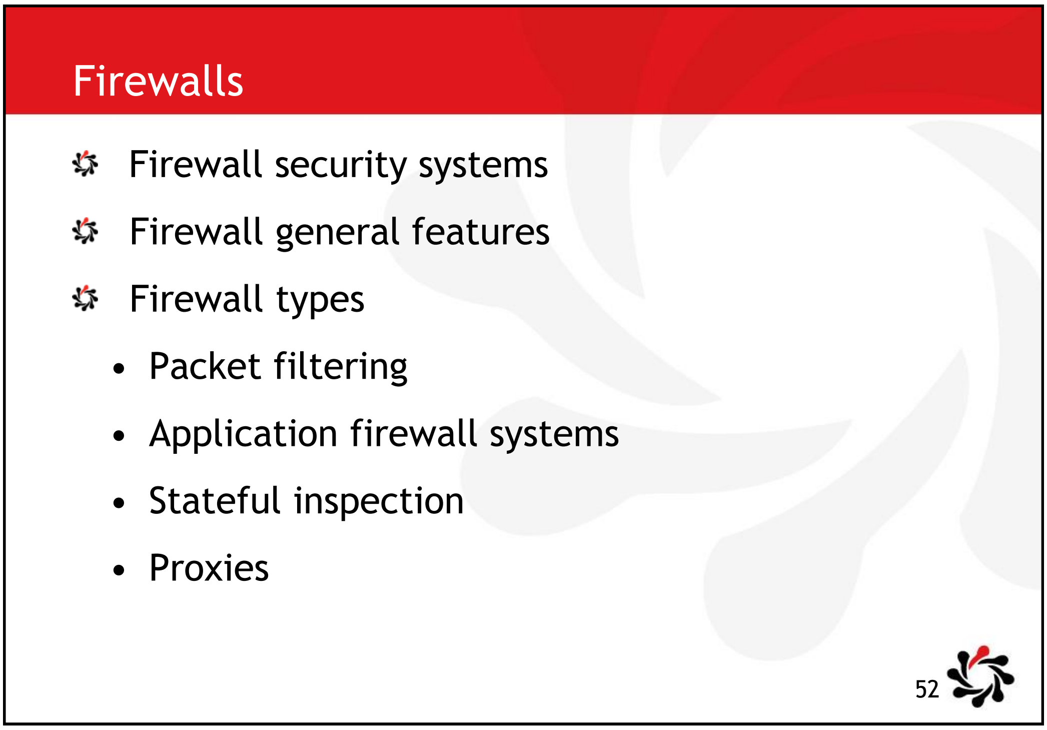
Internet Threats and Security

- 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



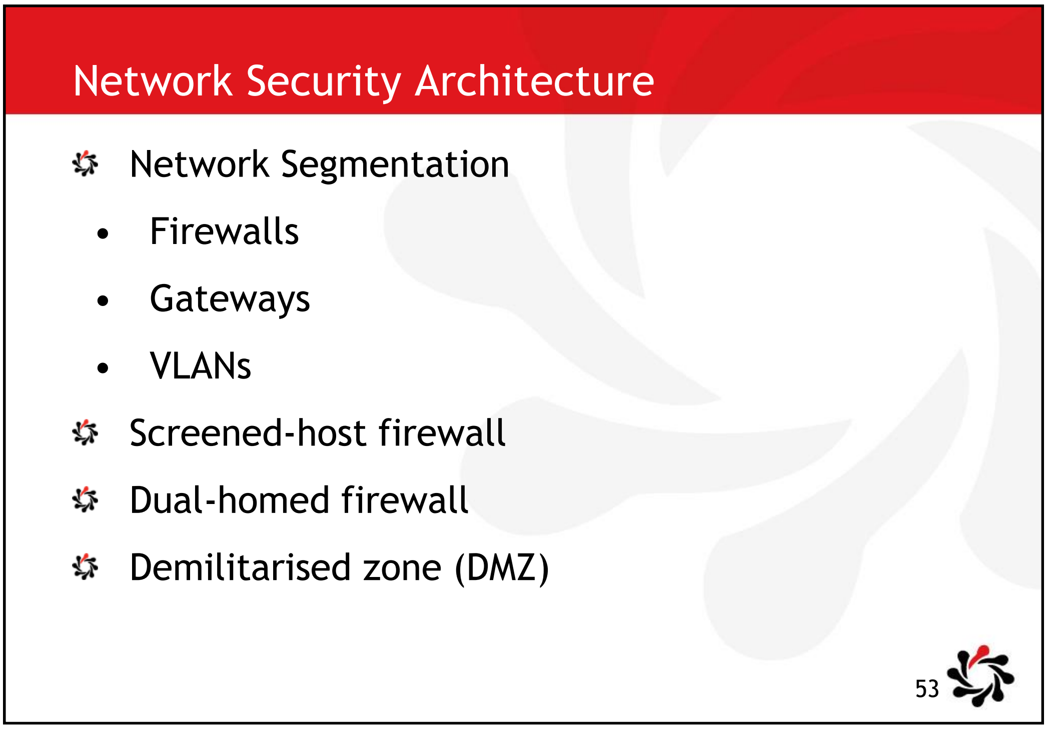
Causes of Internet Attacks

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



Firewalls

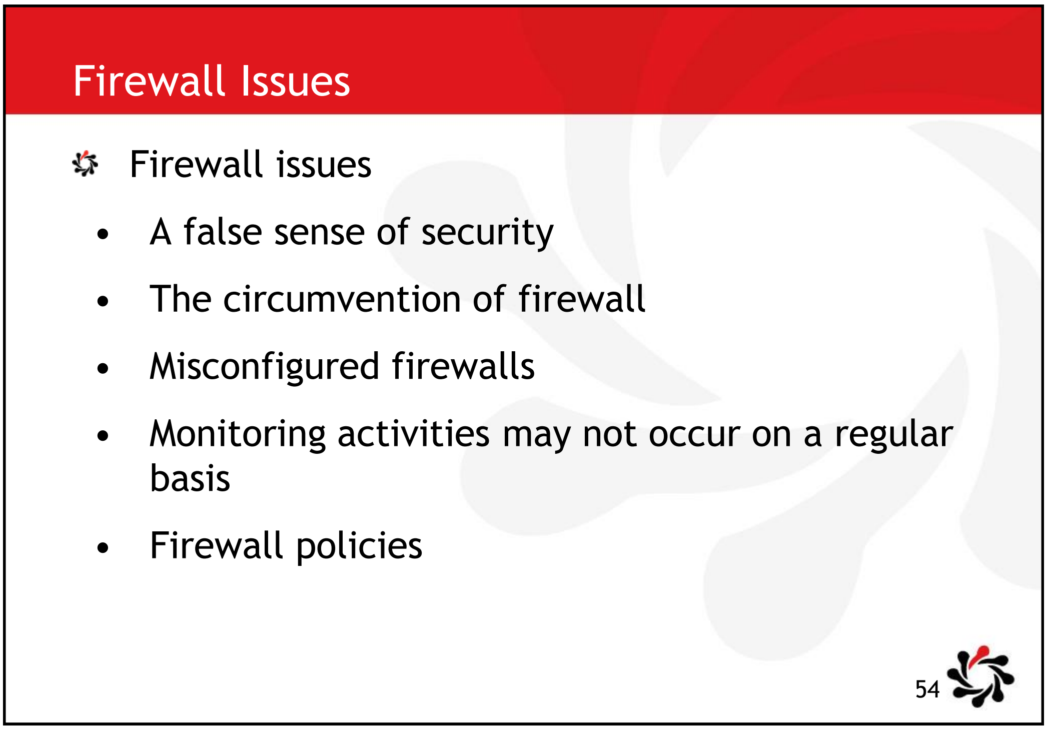
- Firewall security systems
- Firewall general features
- Firewall types
  - Packet filtering
  - Application firewall systems
  - Stateful inspection
  - Proxies



Network Security Architecture

- Network Segmentation
  - Firewalls
  - Gateways
  - VLANs
- Screened-host firewall
- Dual-homed firewall
- Demilitarised zone (DMZ)

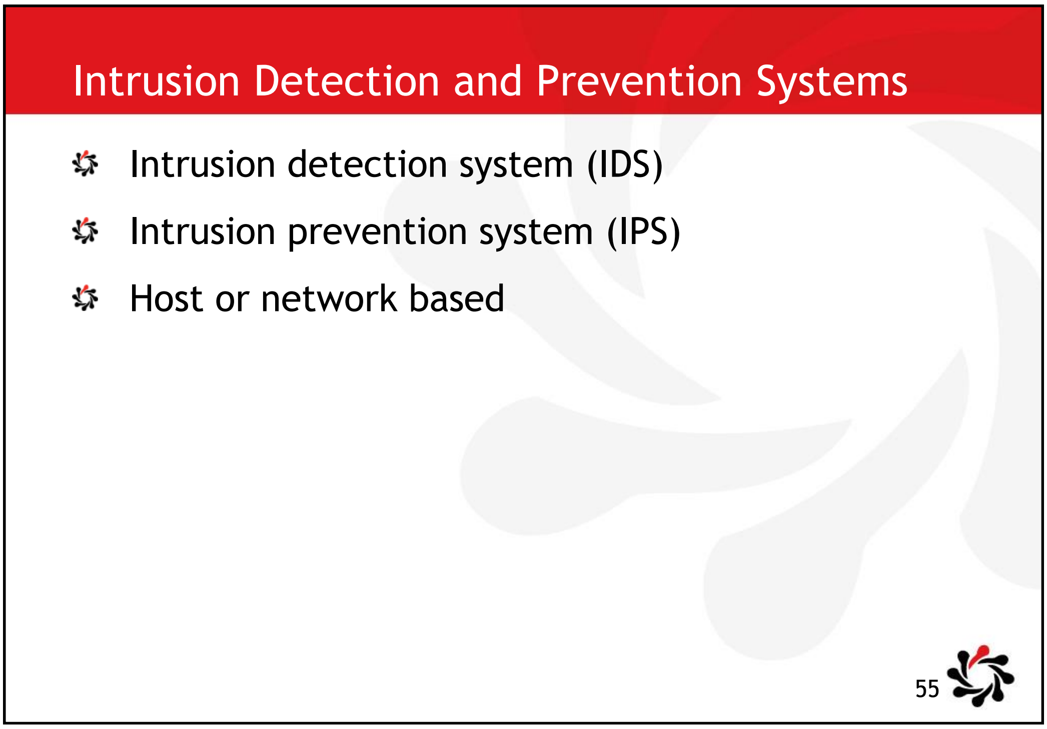
53



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

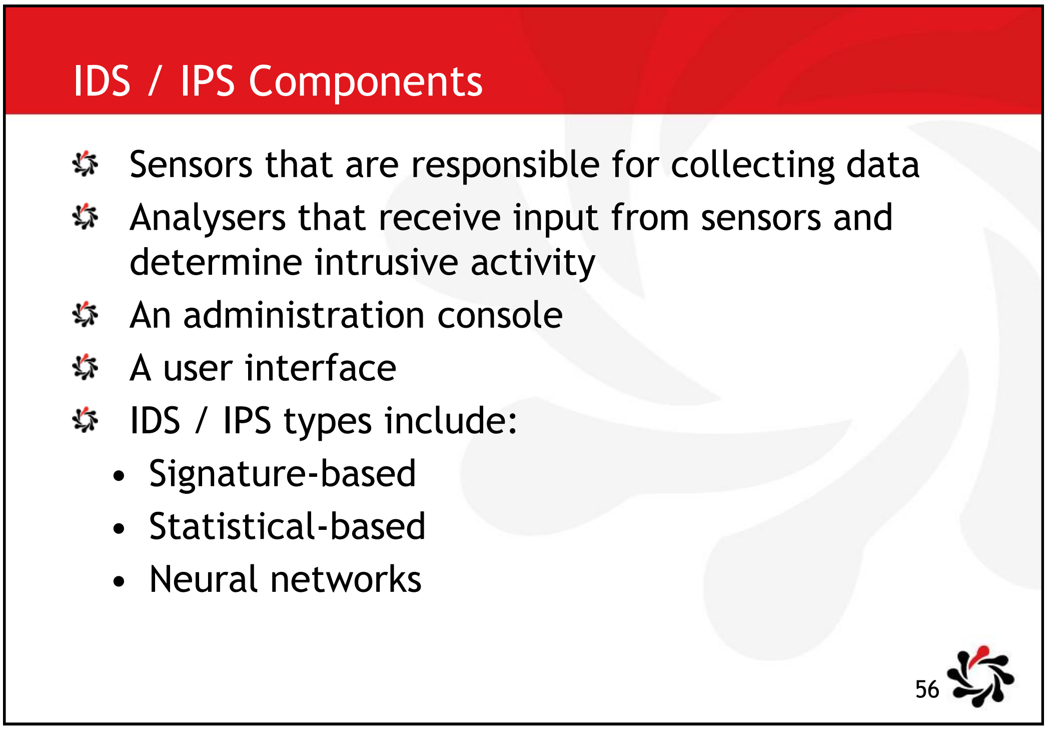
54



Intrusion Detection and Prevention Systems

- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Host or network based

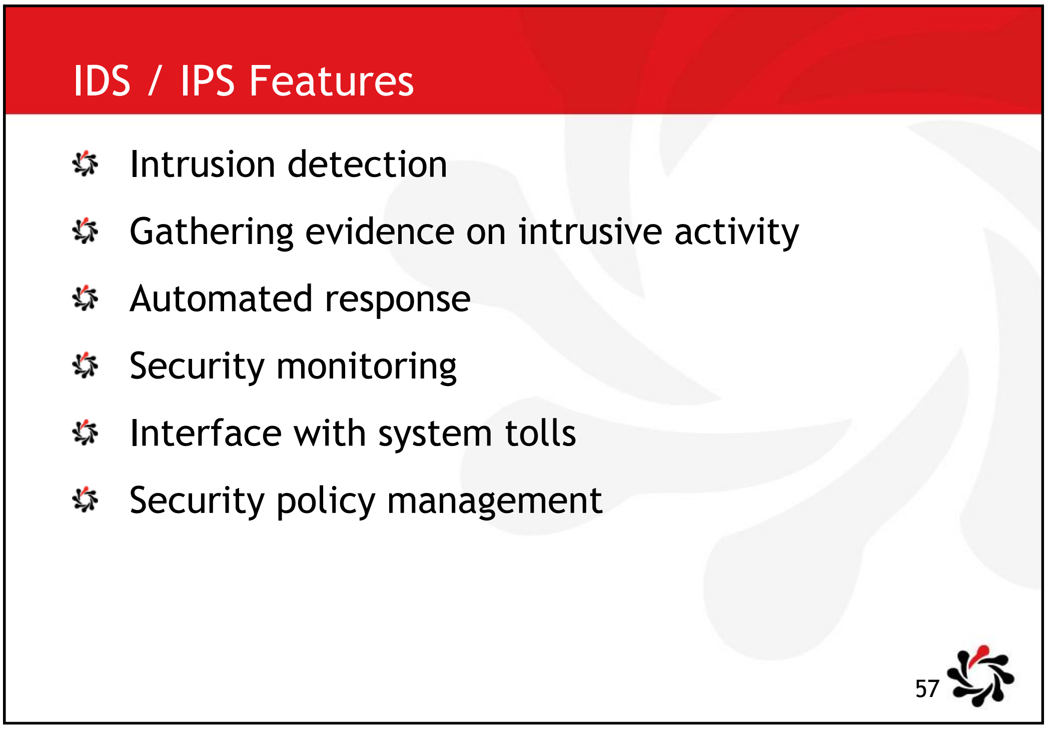
55



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

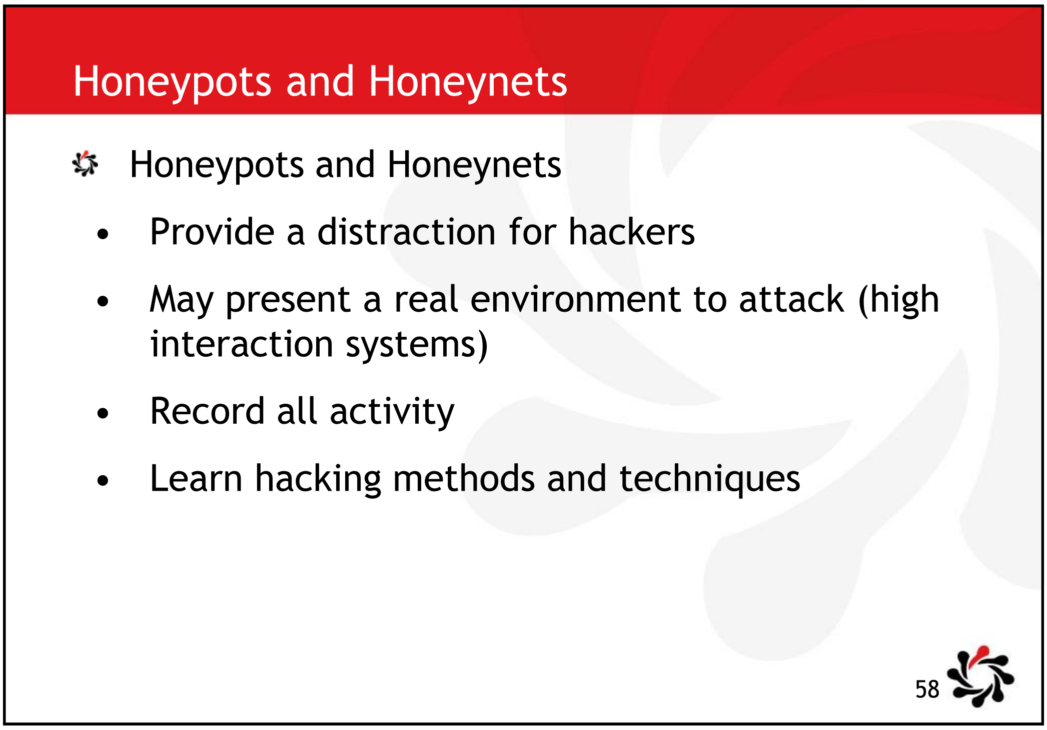
56



IDS / IPS Features

- Intrusion detection
- Gathering evidence on intrusive activity
- Automated response
- Security monitoring
- Interface with system tolls
- Security policy management

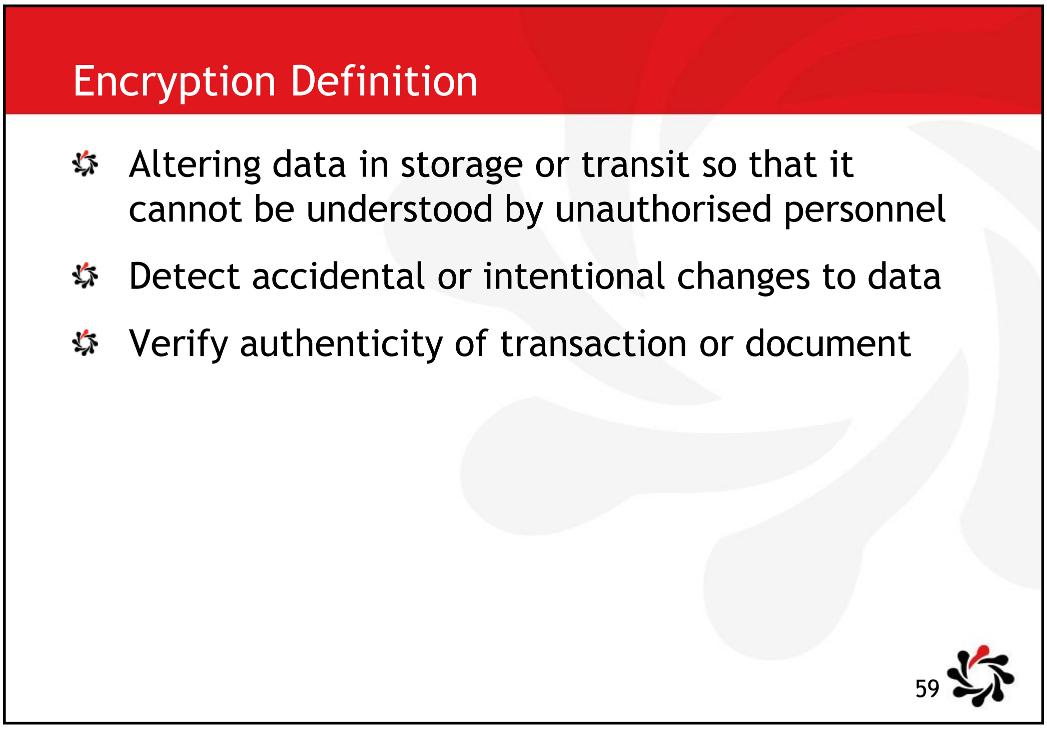
57



Honeypots and Honeynets

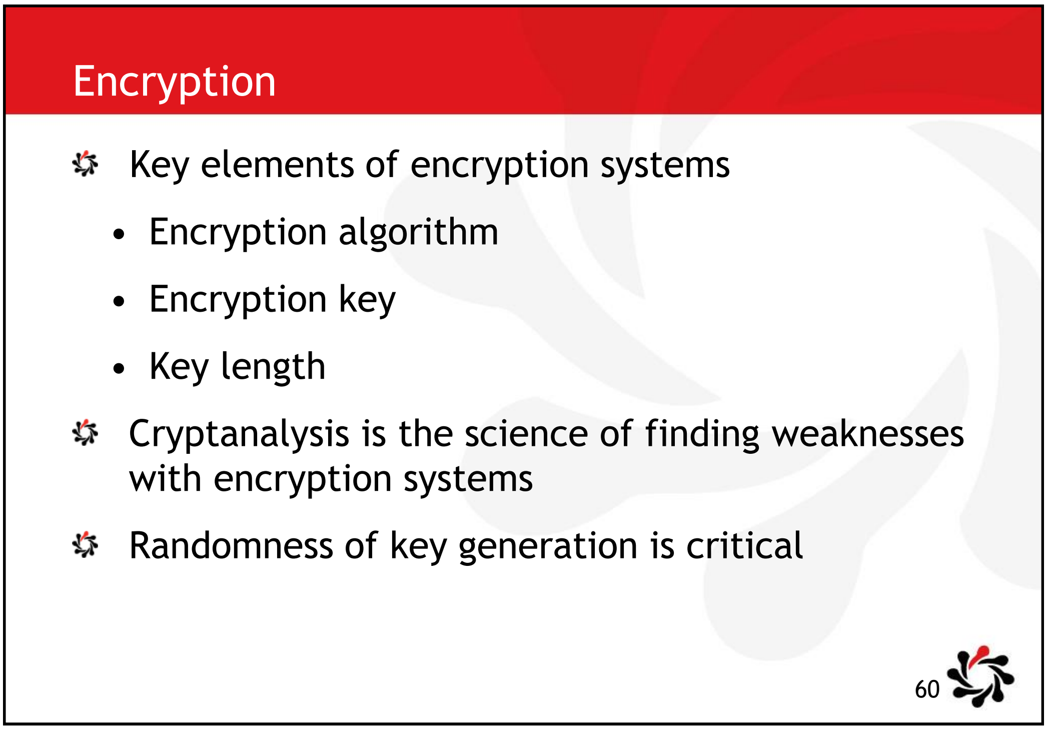
- Honeypots and Honeynets
  - Provide a distraction for hackers
  - May present a real environment to attack (high interaction systems)
  - Record all activity
  - Learn hacking methods and techniques

58



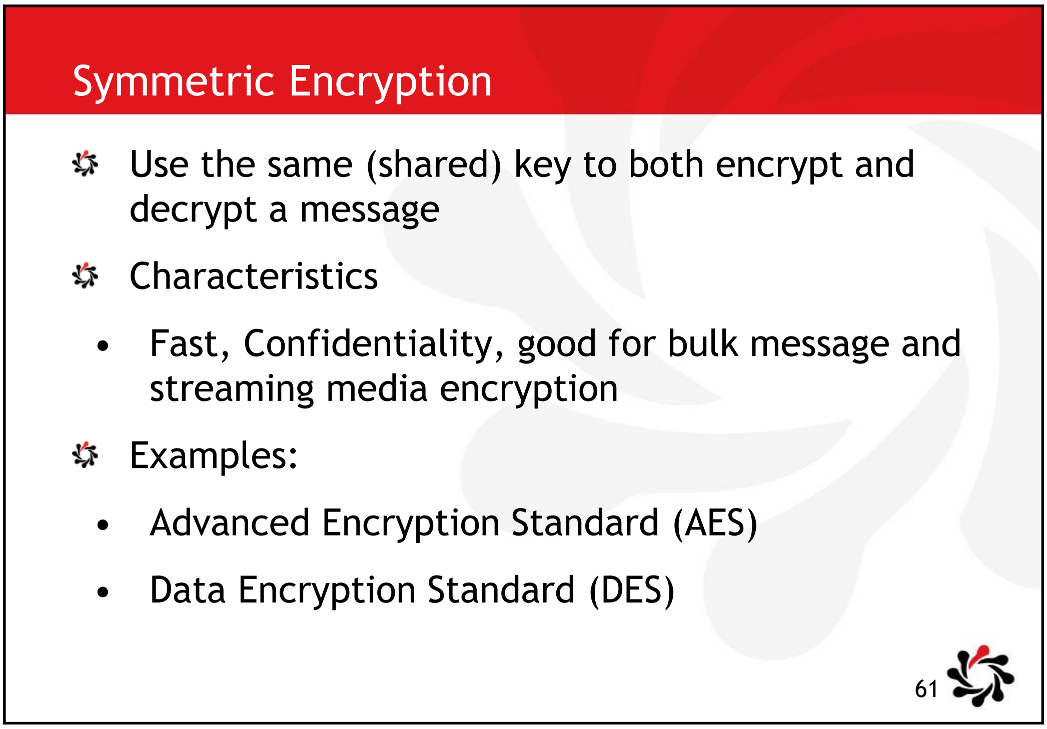
Encryption Definition

- Altering data in storage or transit so that it cannot be understood by unauthorised personnel
- Detect accidental or intentional changes to data
- Verify authenticity of transaction or document



Encryption

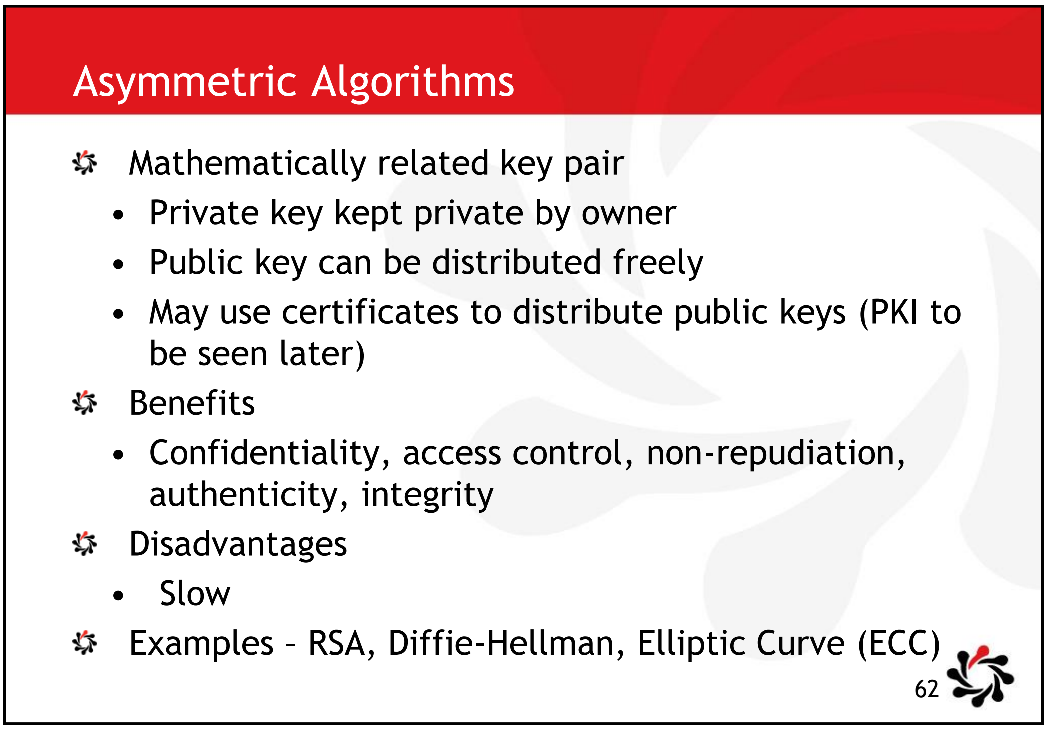
- Key elements of encryption systems
  - Encryption algorithm
  - Encryption key
  - Key length
- Cryptanalysis is the science of finding weaknesses with encryption systems
- Randomness of key generation is critical



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)

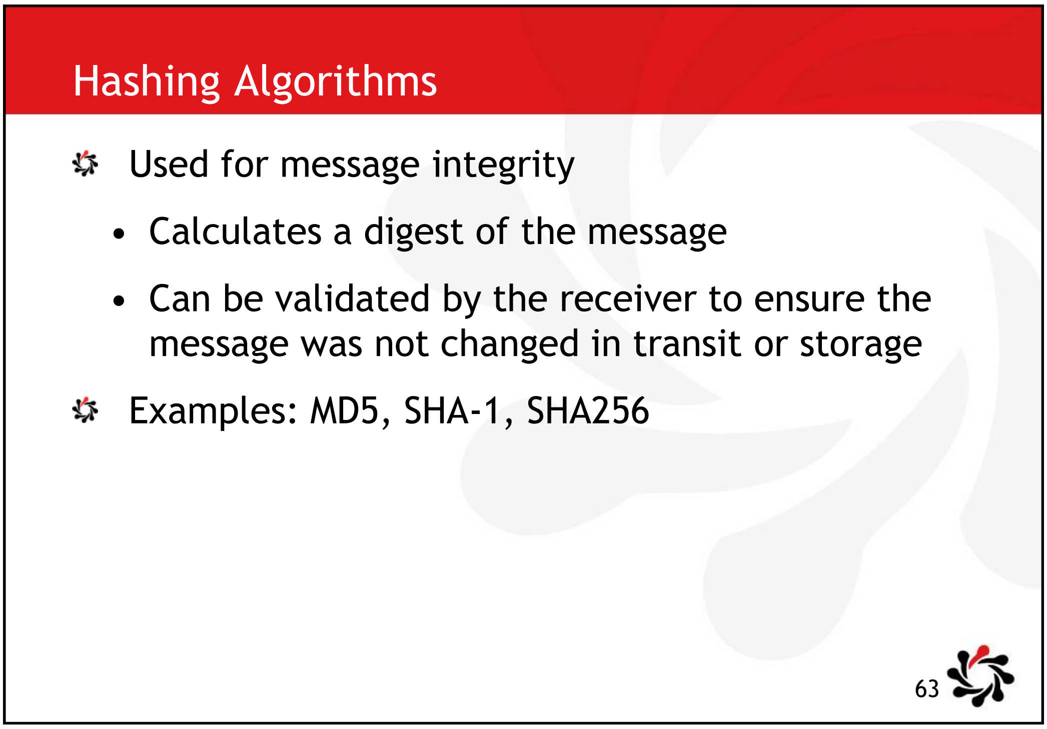
61



Asymmetric Algorithms

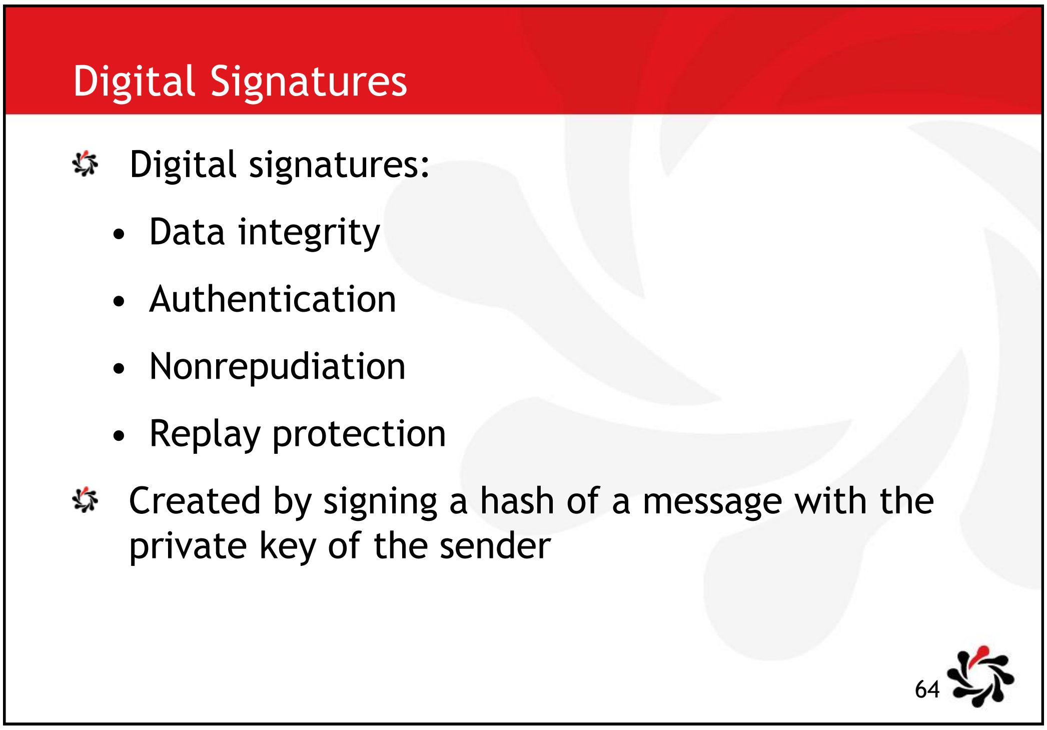
- Mathematically related key pair
  - Private key kept private by owner
  - Public key can be distributed freely
  - May use certificates to distribute public keys (PKI to be seen later)
- Benefits
  - Confidentiality, access control, non-repudiation, authenticity, integrity
- Disadvantages
  - Slow
- Examples – RSA, Diffie-Hellman, Elliptic Curve (ECC)

62



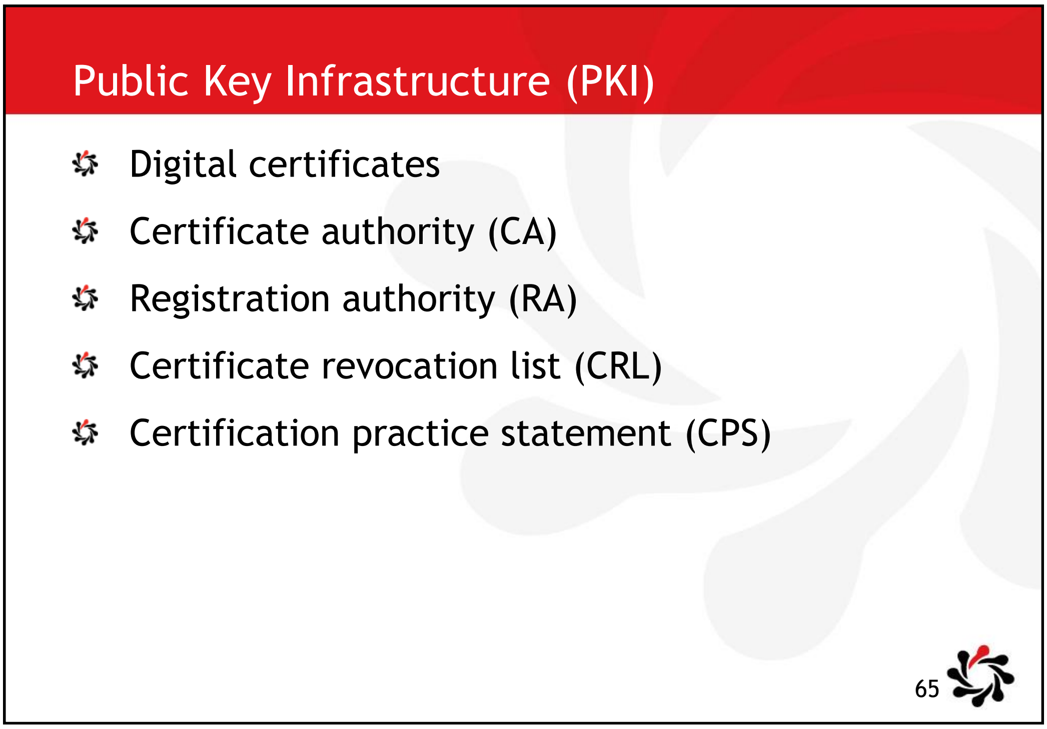
Hashing Algorithms

- 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



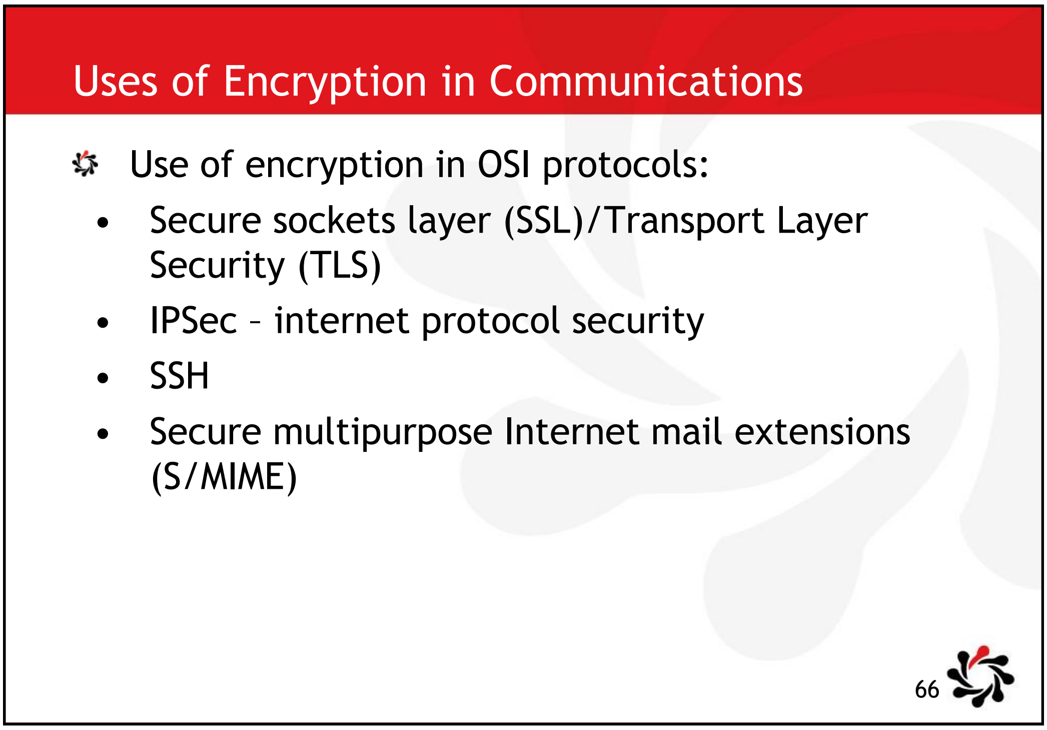
Digital Signatures

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



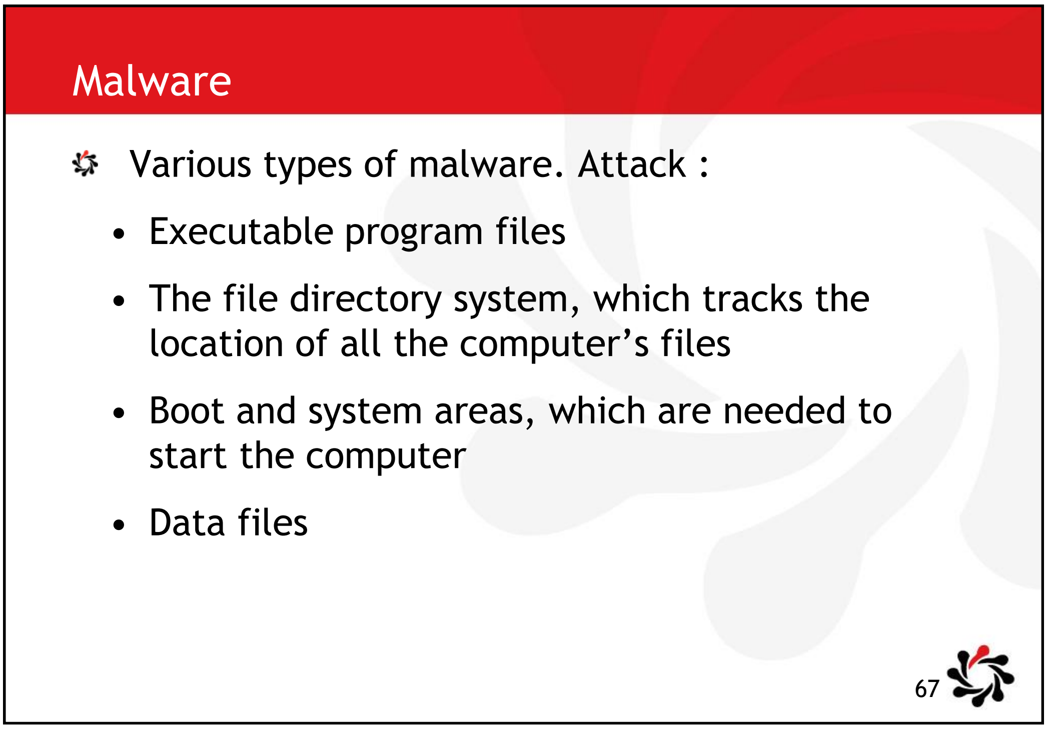
Public Key Infrastructure (PKI)

- Digital certificates
- Certificate authority (CA)
- Registration authority (RA)
- Certificate revocation list (CRL)
- Certification practice statement (CPS)



Uses of Encryption in Communications

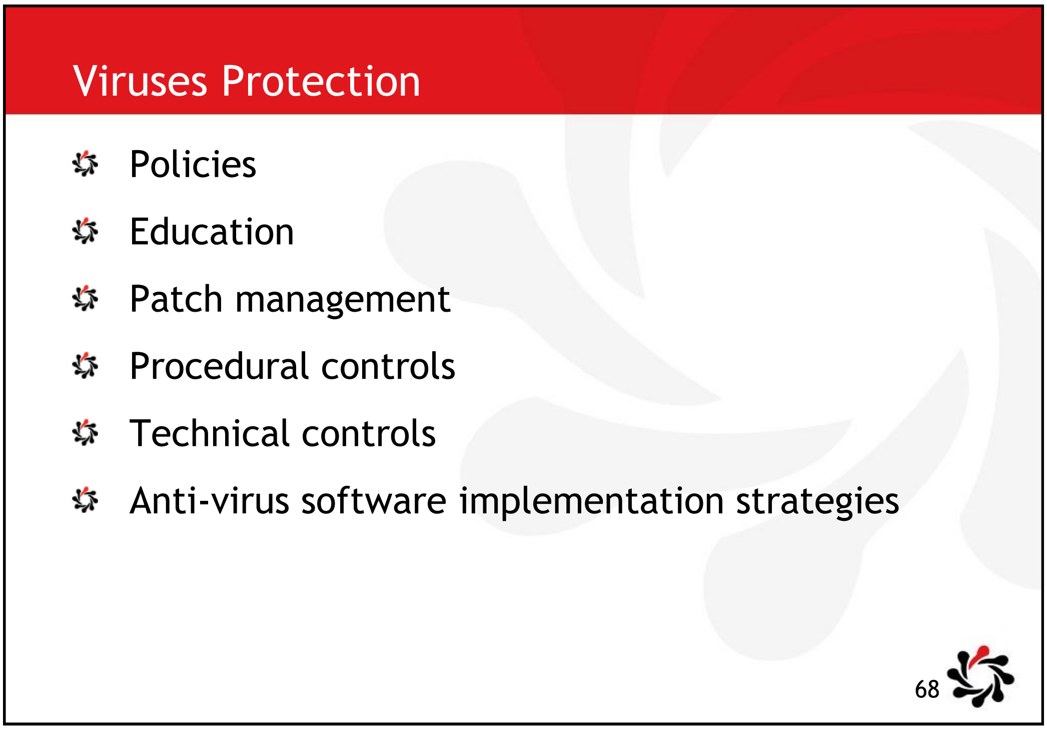
- Use of encryption in OSI protocols:
  - Secure sockets layer (SSL)/Transport Layer Security (TLS)
  - IPSec – internet protocol security
  - SSH
  - Secure multipurpose Internet mail extensions (S/MIME)



Malware

- Various types of malware. 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

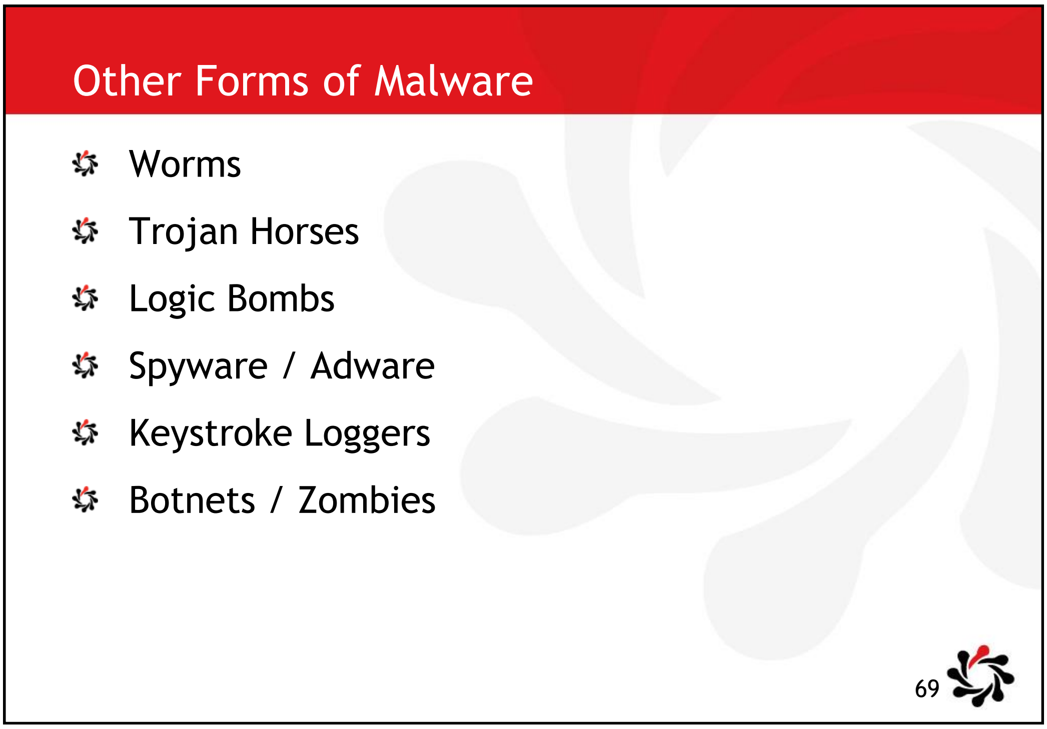
67



Viruses Protection

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

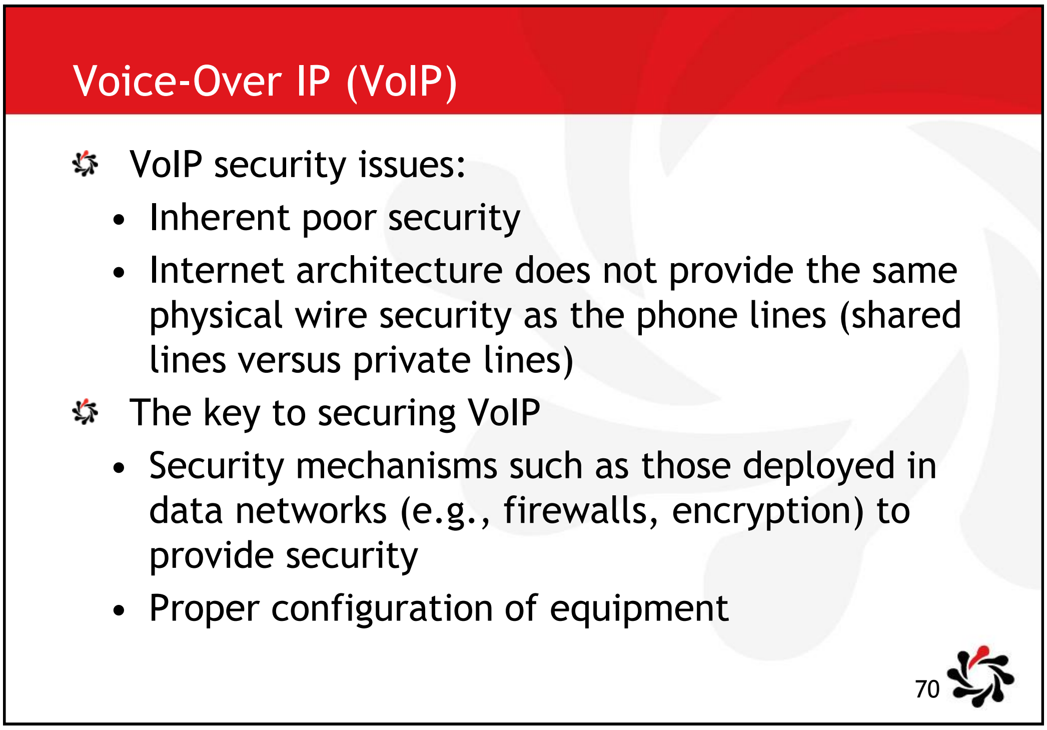
68



Other Forms of Malware

- Worms
- Trojan Horses
- Logic Bombs
- Spyware / Adware
- Keystroke Loggers
- Botnets / Zombies

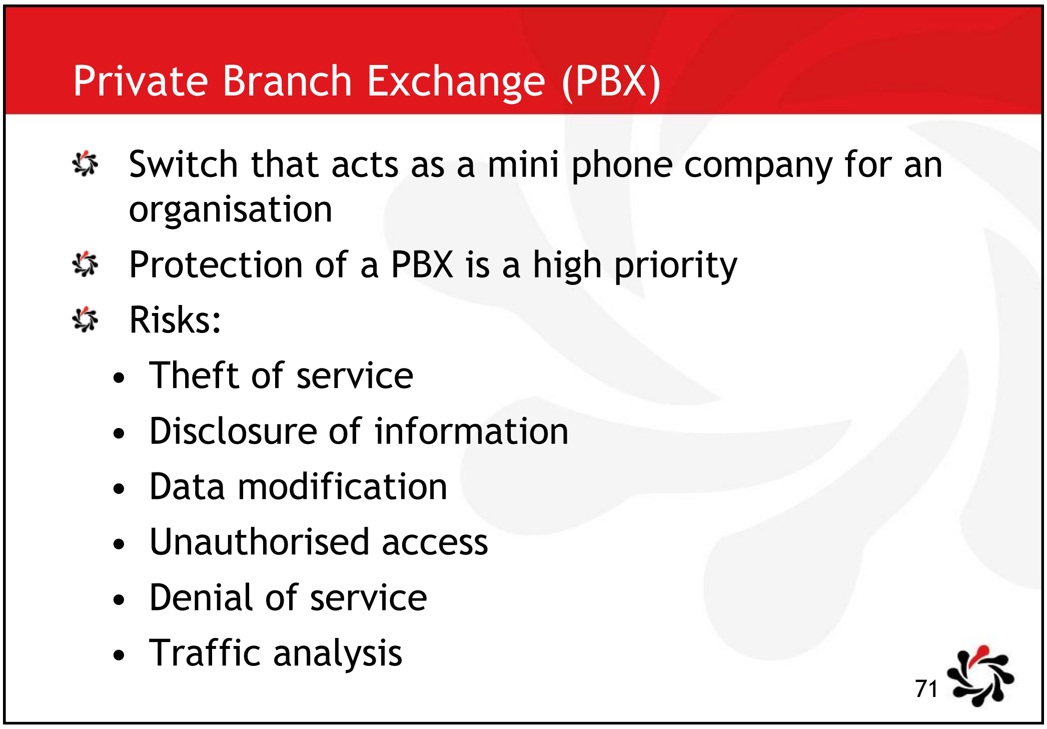
69



Voice-Over IP (VoIP)

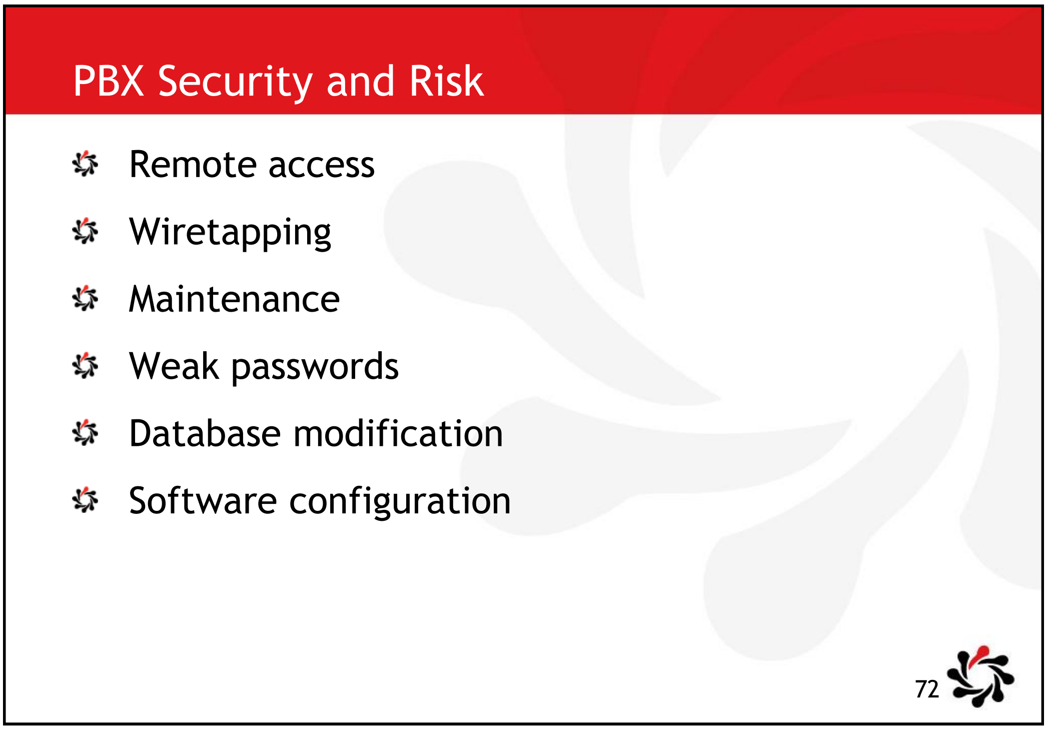
- VoIP security issues:
  - Inherent poor security
  - Internet architecture does not provide the same physical wire security as the phone lines (shared lines versus private lines)
- The key to securing VoIP
  - Security mechanisms such as those deployed in data networks (e.g., firewalls, encryption) to provide security
  - Proper configuration of equipment

70



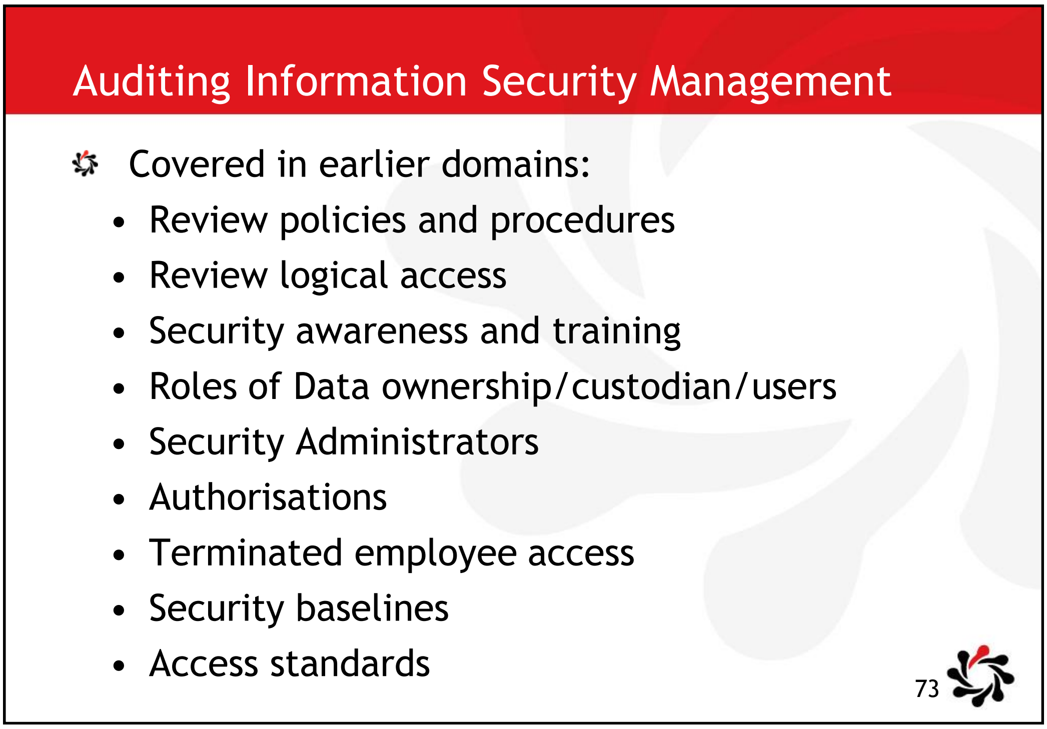
Private Branch Exchange (PBX)

- Switch that acts as a mini phone company for an organisation
- Protection of a PBX is a high priority
- Risks:
  - Theft of service
  - Disclosure of information
  - Data modification
  - Unauthorised access
  - Denial of service
  - Traffic analysis



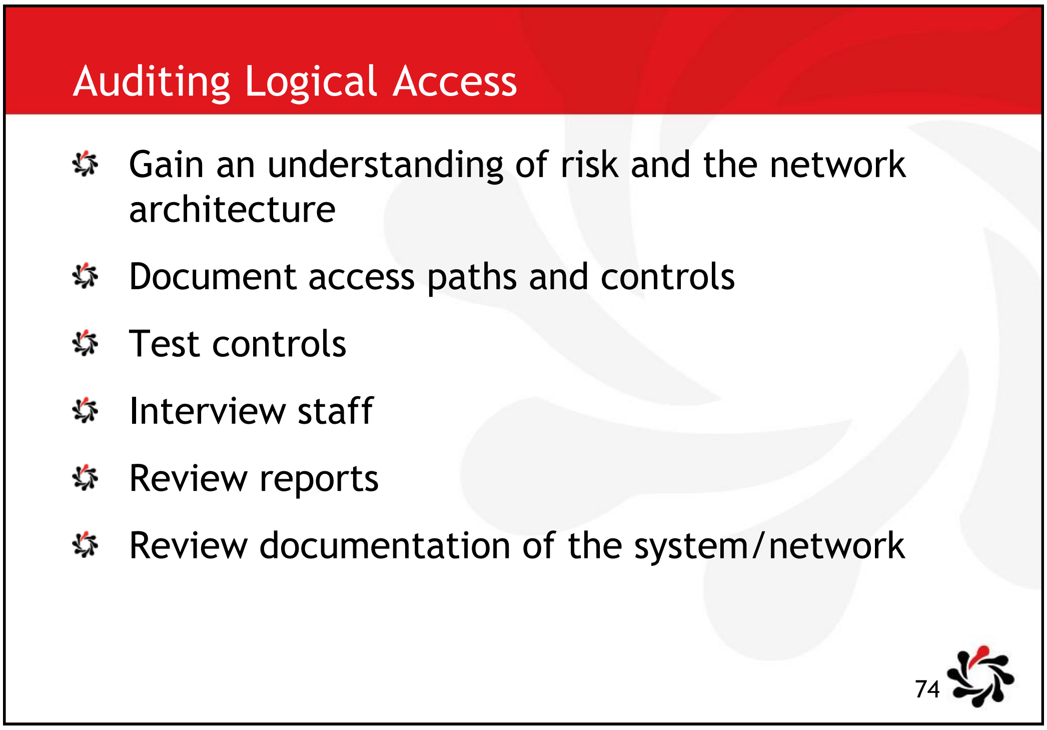
PBX Security and Risk

- Remote access
- Wiretapping
- Maintenance
- Weak passwords
- Database modification
- Software configuration



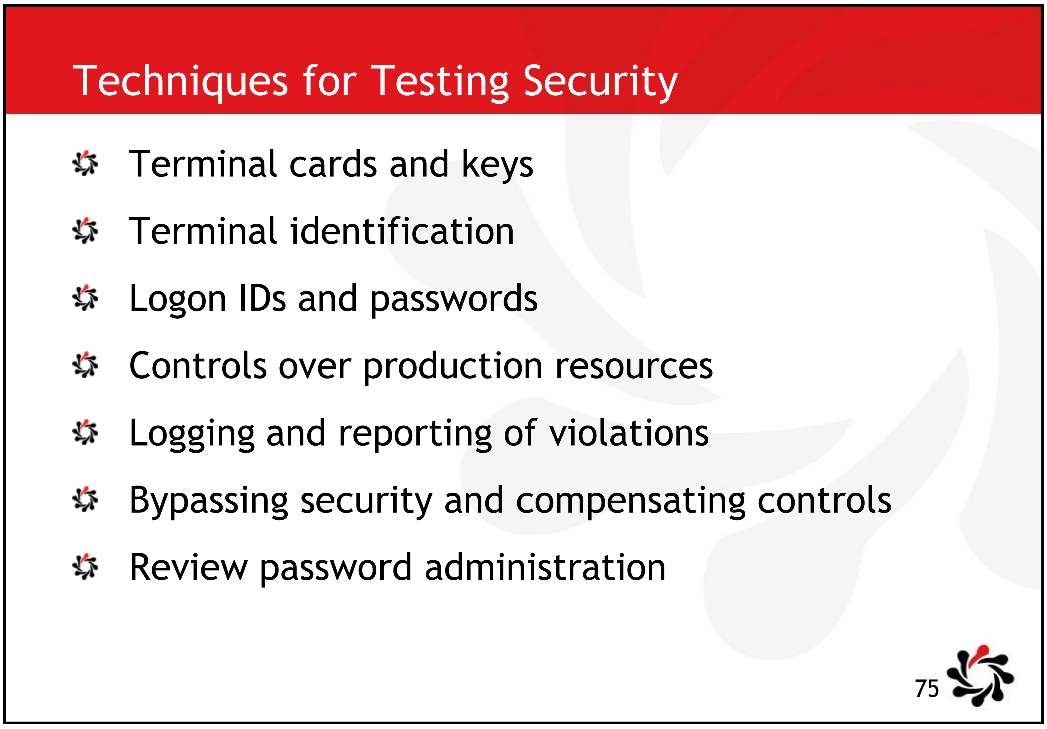
Auditing Information Security Management

- Covered in earlier domains:
  - Review policies and procedures
  - Review logical access
  - Security awareness and training
  - Roles of Data ownership/custodian/users
  - Security Administrators
  - Authorisations
  - Terminated employee access
  - Security baselines
  - Access standards



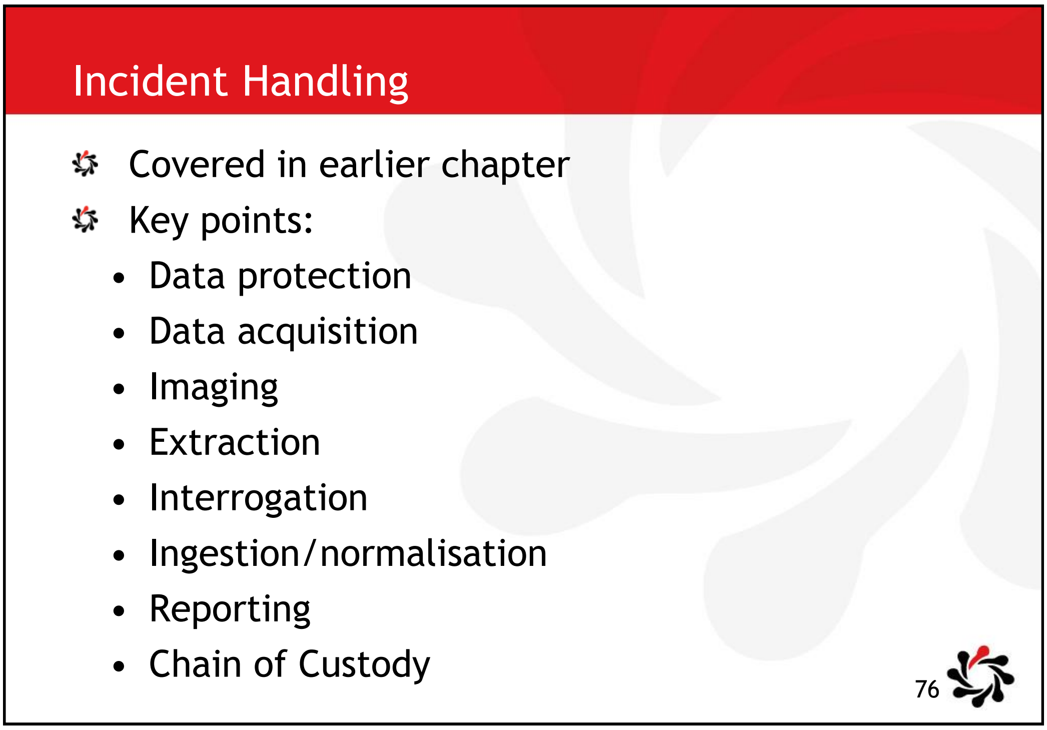
Auditing Logical Access

- Gain an understanding of risk and the network architecture
- Document access paths and controls
- Test controls
- Interview staff
- Review reports
- Review documentation of the system/network



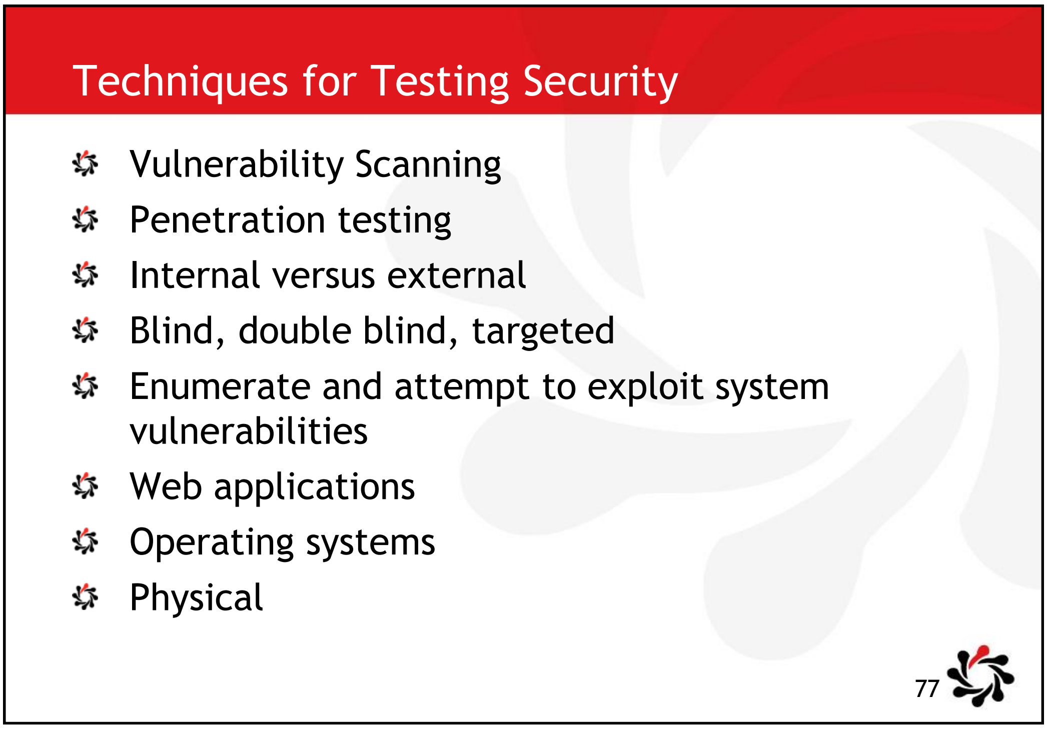
Techniques for Testing Security

- Terminal cards and keys
- Terminal identification
- Logon IDs and passwords
- Controls over production resources
- Logging and reporting of violations
- Bypassing security and compensating controls
- Review password administration



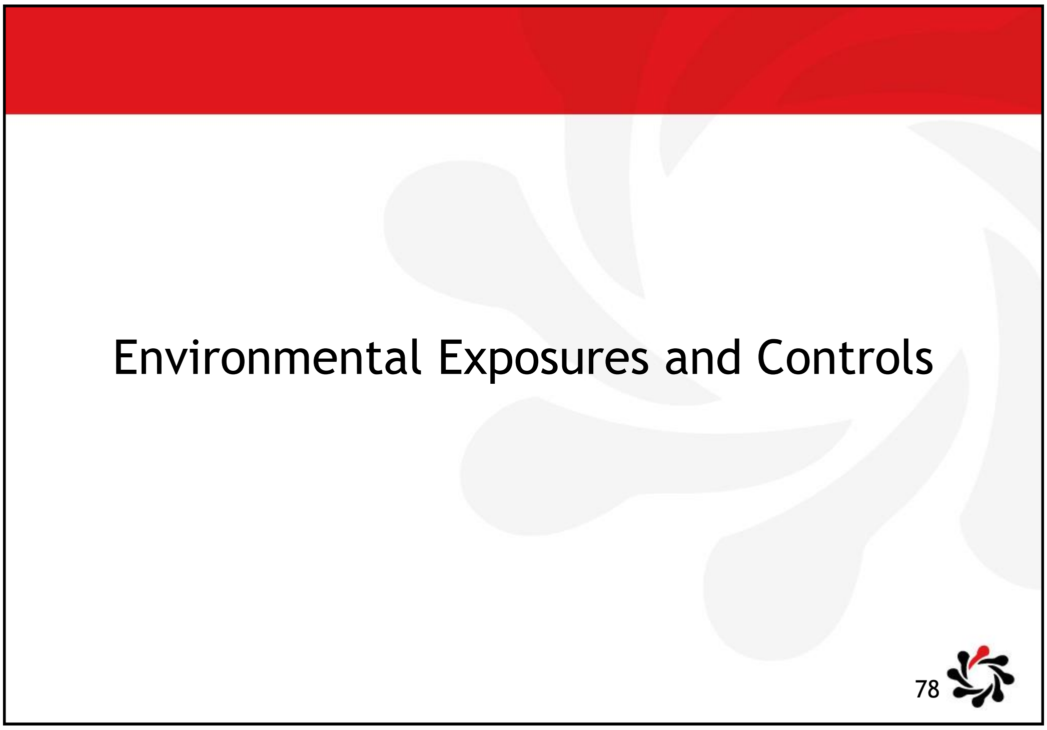
Incident Handling

- Covered in earlier chapter
- Key points:
  - Data protection
  - Data acquisition
  - Imaging
  - Extraction
  - Interrogation
  - Ingestion/normalisation
  - Reporting
  - Chain of Custody

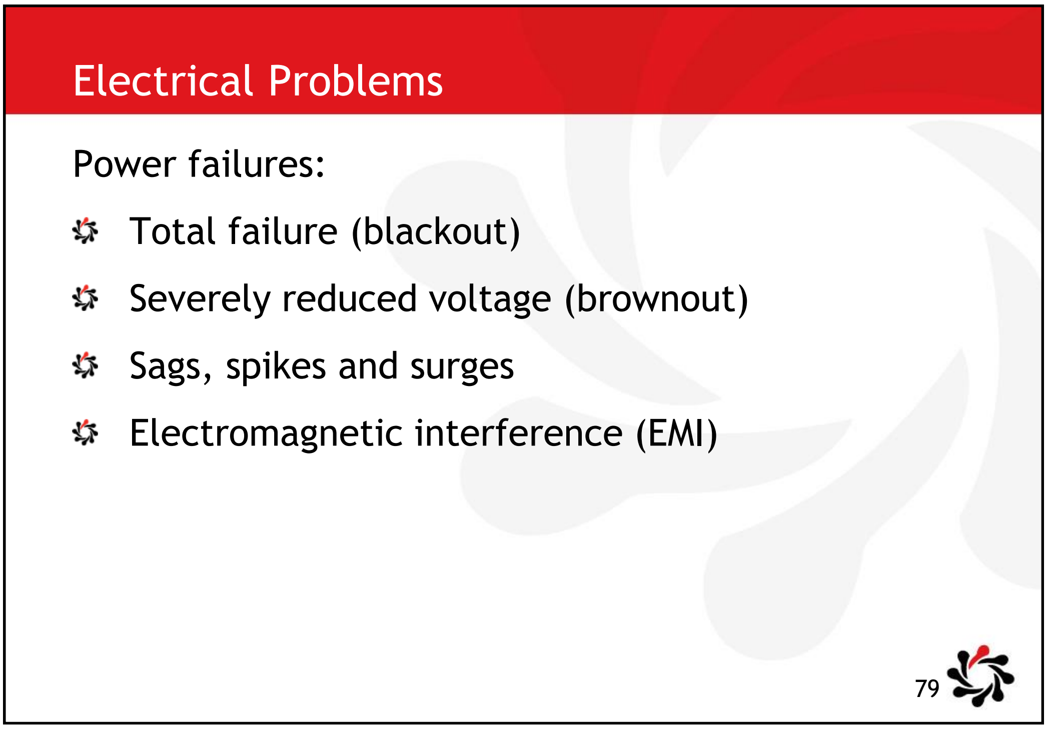


Techniques for Testing Security

- Vulnerability Scanning
- Penetration testing
- Internal versus external
- Blind, double blind, targeted
- Enumerate and attempt to exploit system vulnerabilities
- Web applications
- Operating systems
- Physical



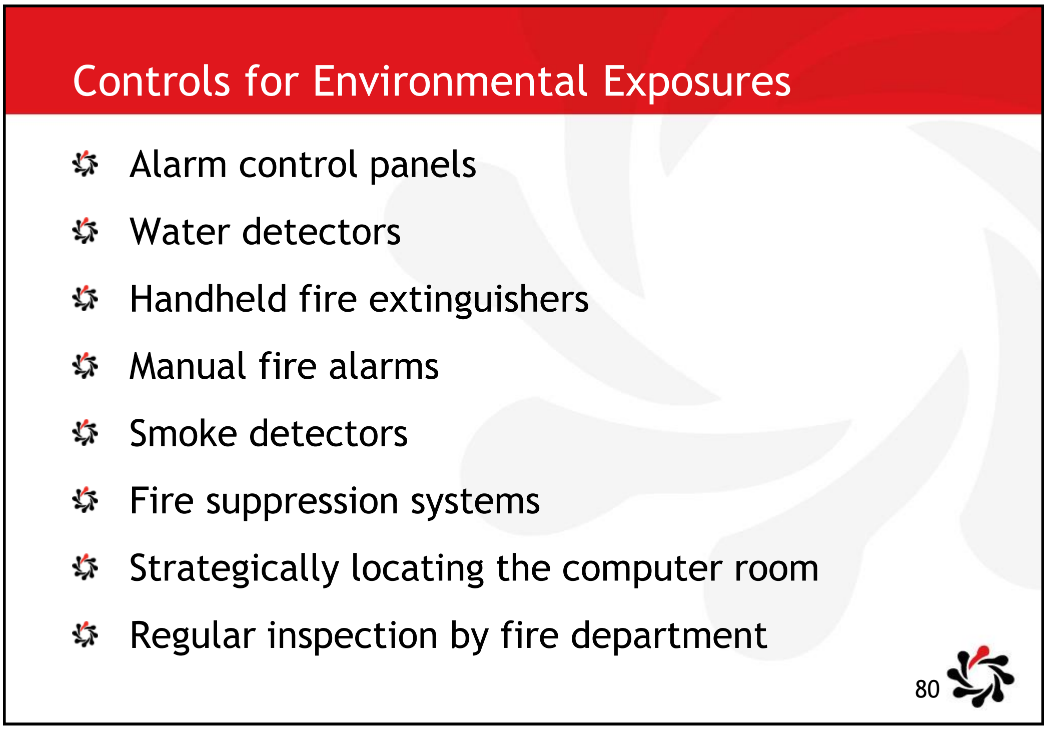
Environmental Exposures and Controls



Electrical Problems

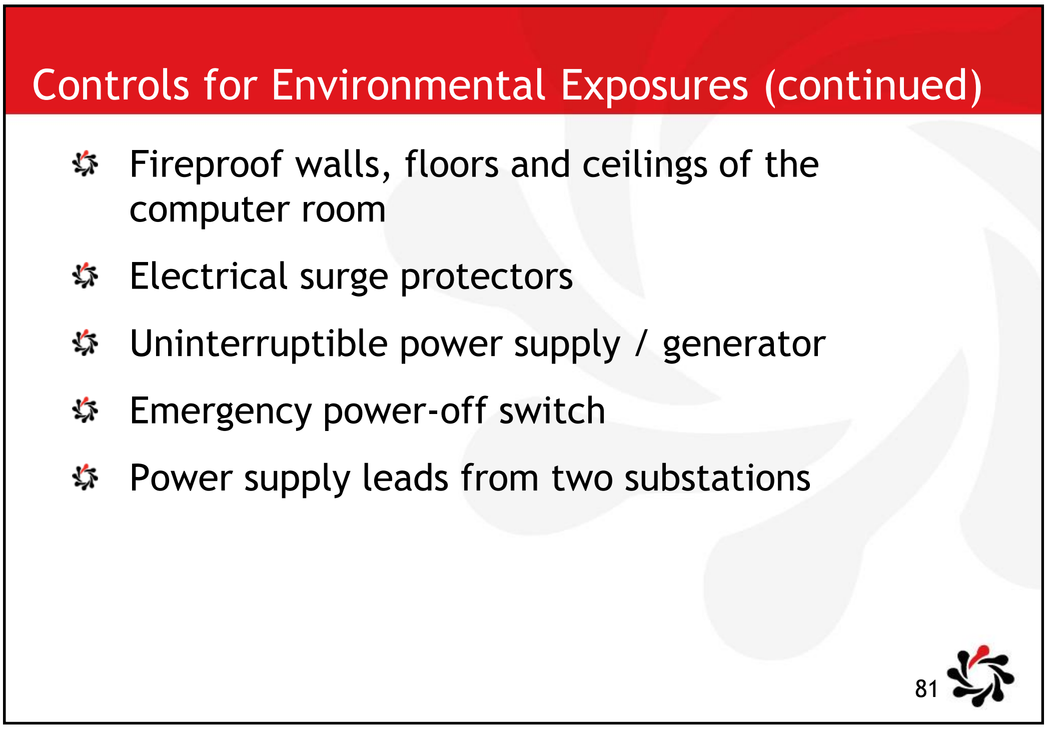
Power failures:

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



Controls for Environmental Exposures

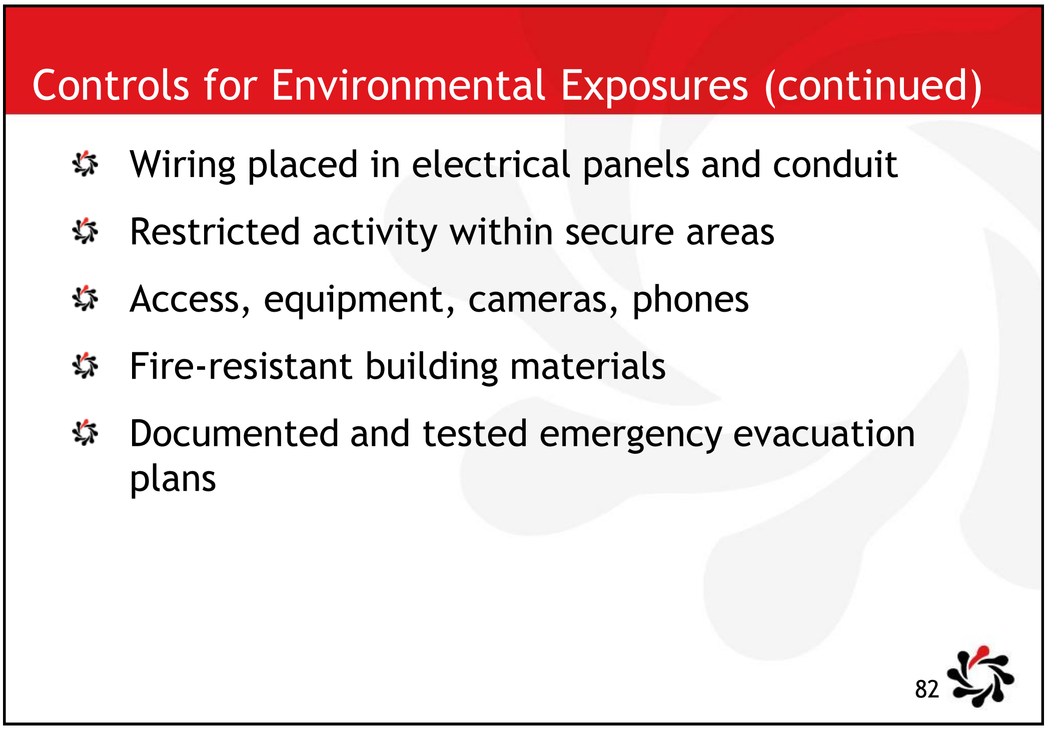
- Alarm control panels
- Water detectors
- Handheld fire extinguishers
- Manual fire alarms
- Smoke detectors
- Fire suppression systems
- Strategically locating the computer room
- Regular inspection by fire department



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

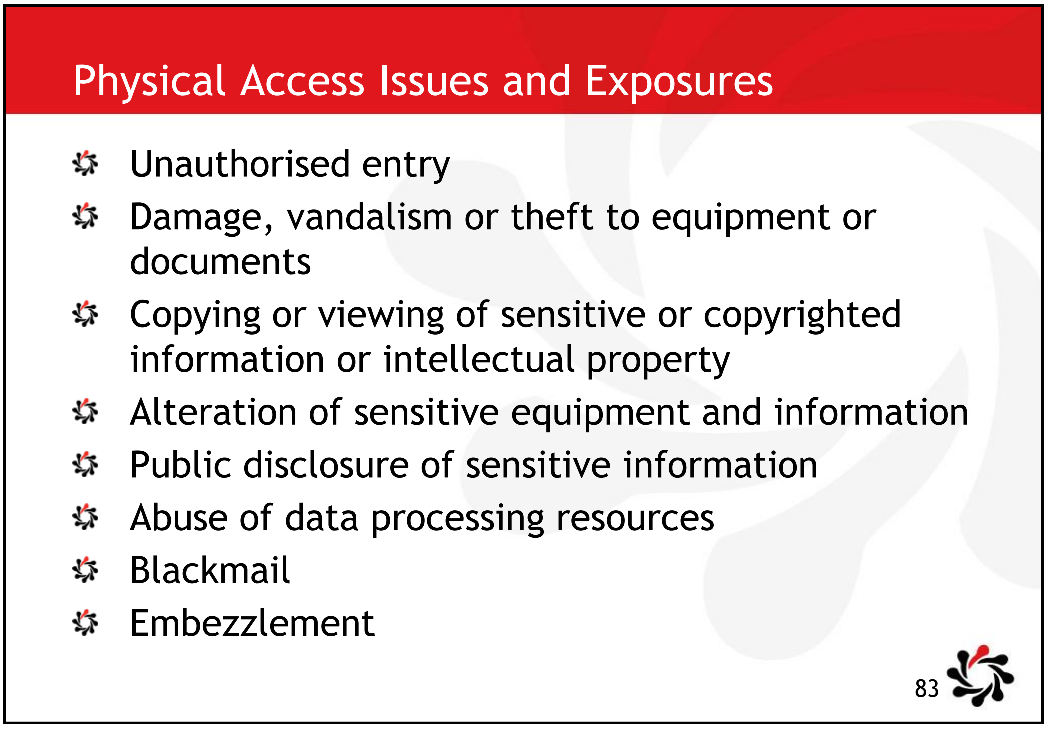
81



Controls for Environmental Exposures (continued)

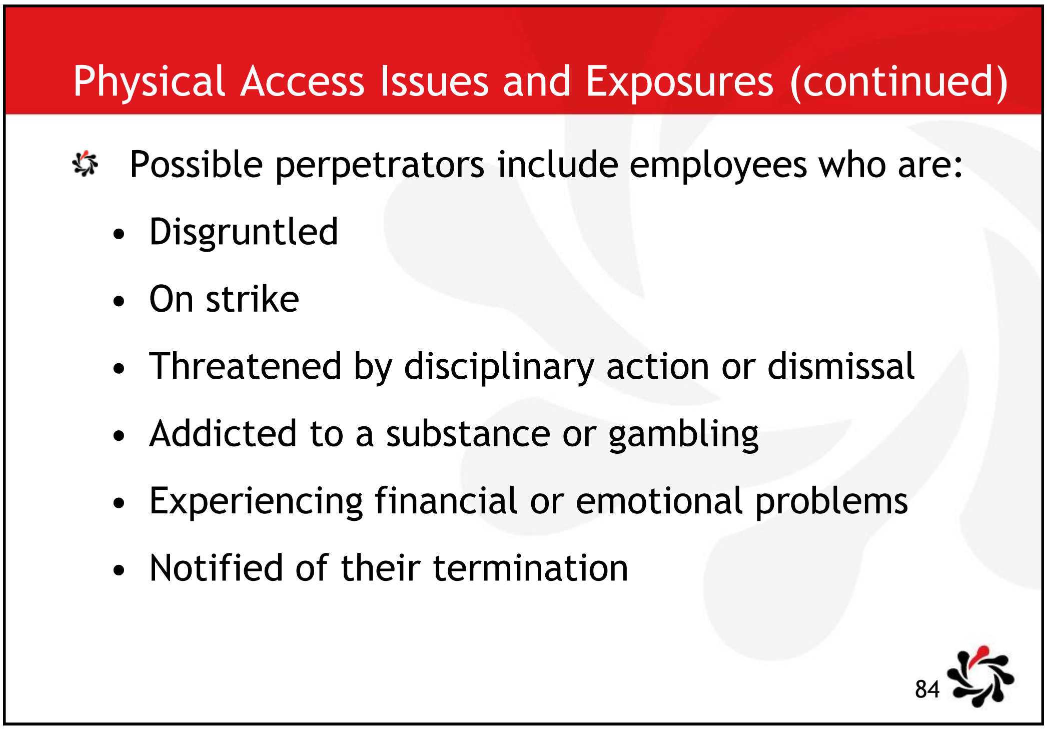
- Wiring placed in electrical panels and conduit
- Restricted activity within secure areas
- Access, equipment, cameras, phones
- Fire-resistant building materials
- Documented and tested emergency evacuation plans

82



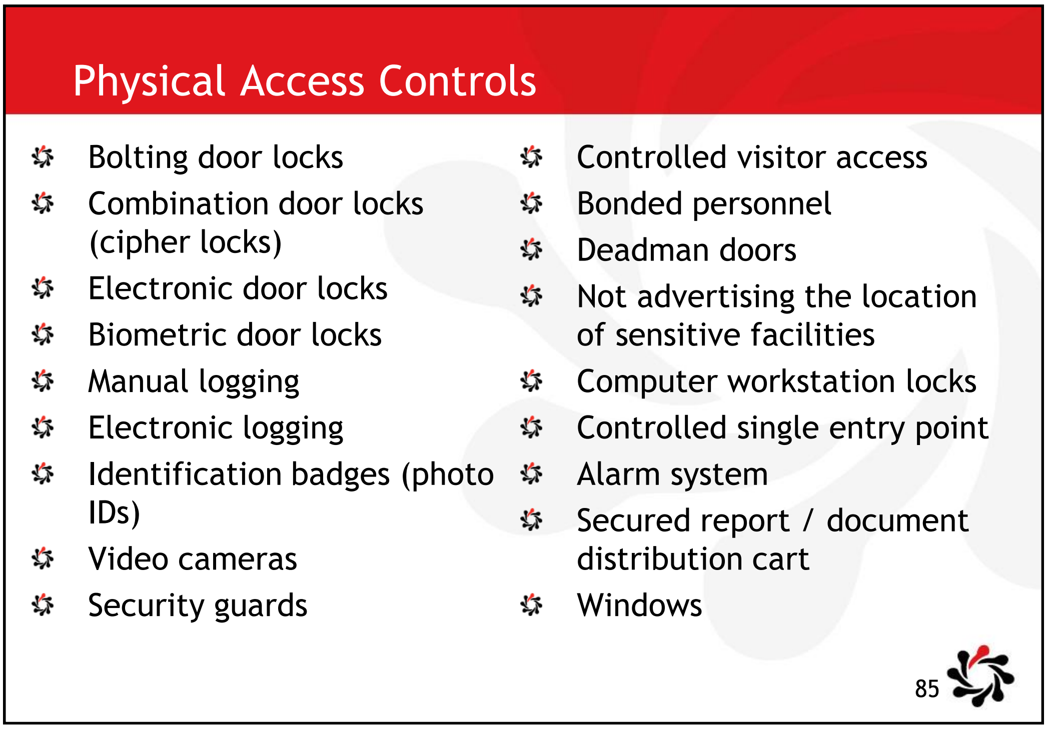
Physical Access Issues and Exposures

- 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



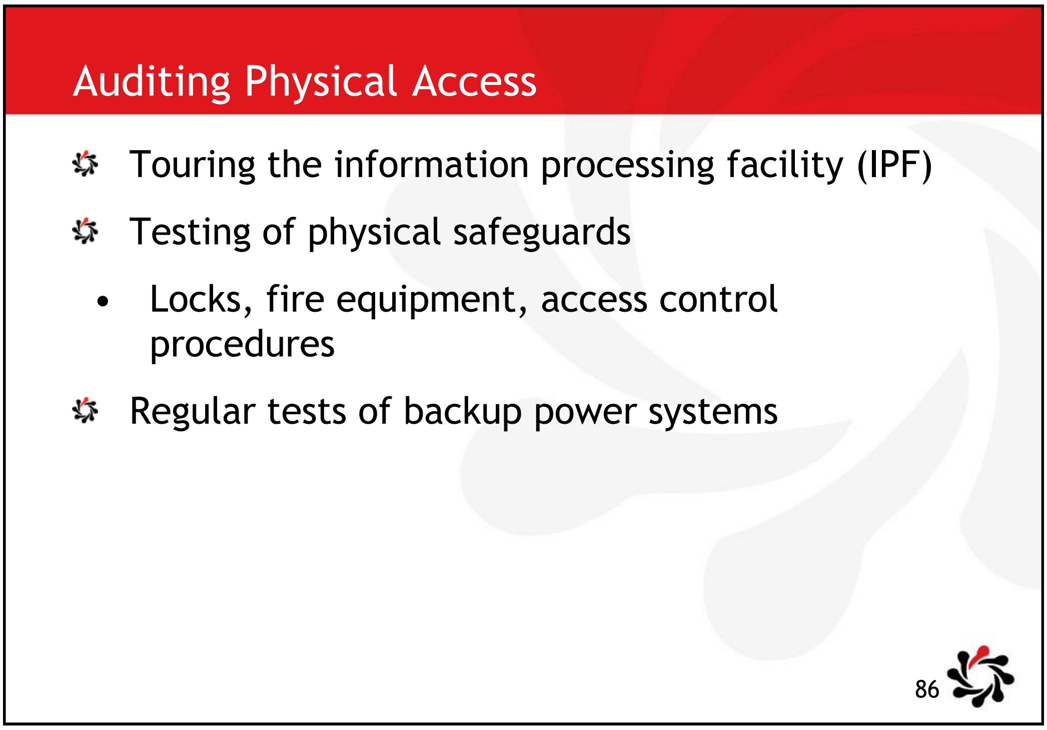
Physical Access Issues and Exposures (continued)

- 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



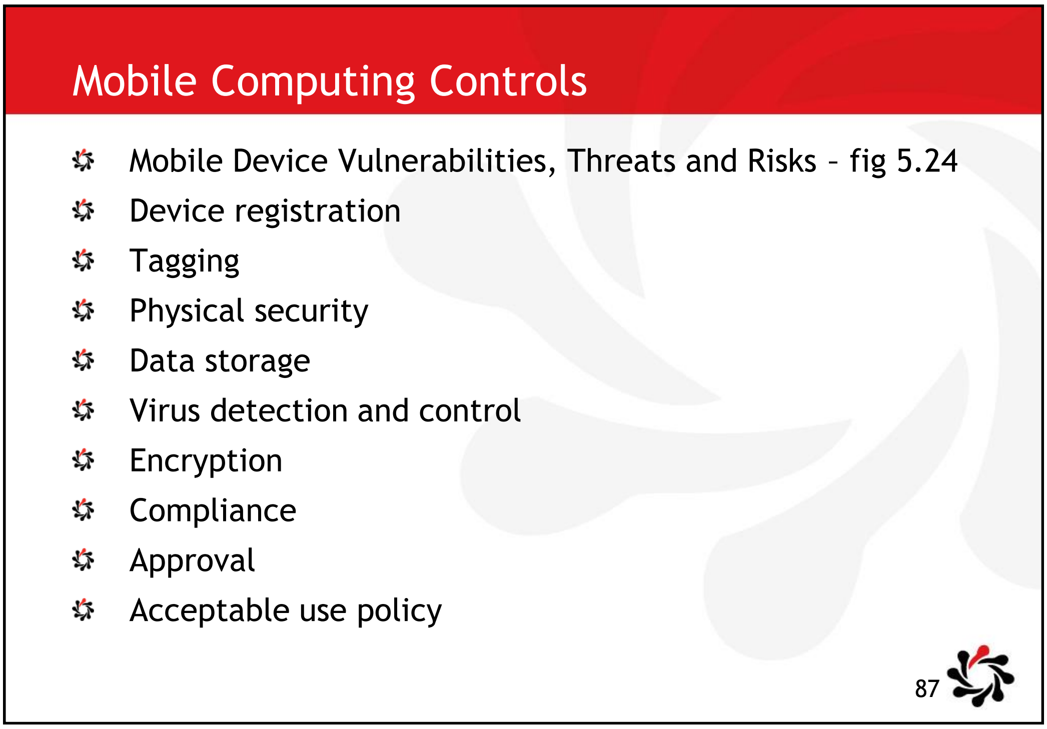
Physical Access Controls

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



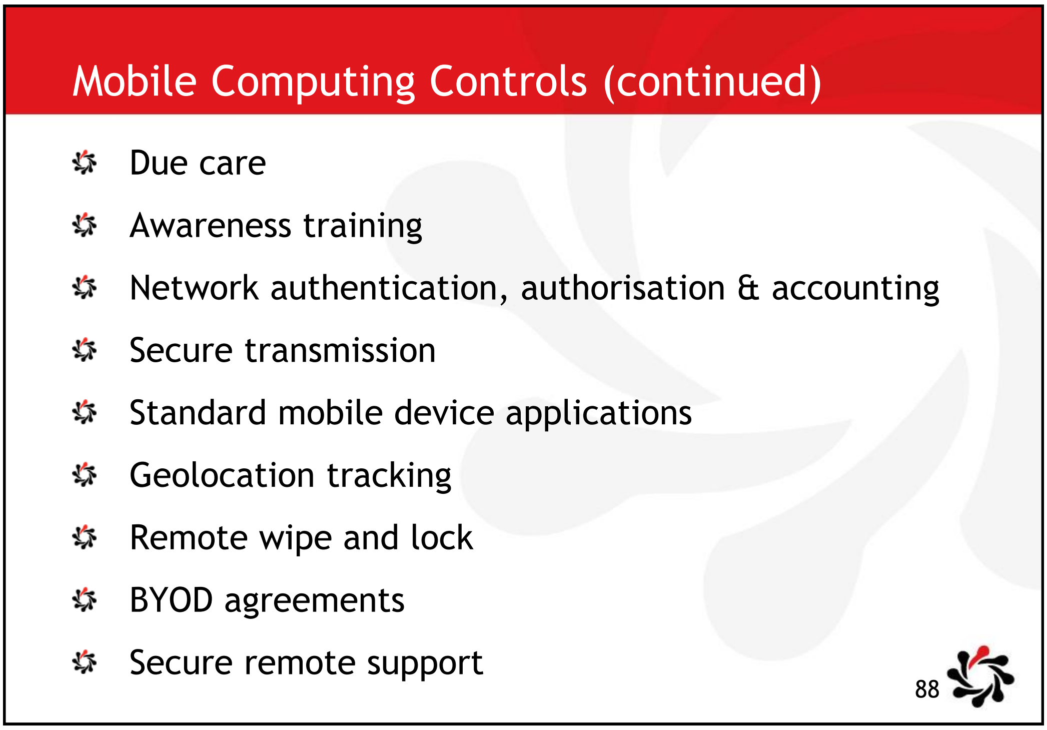
Auditing Physical Access

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



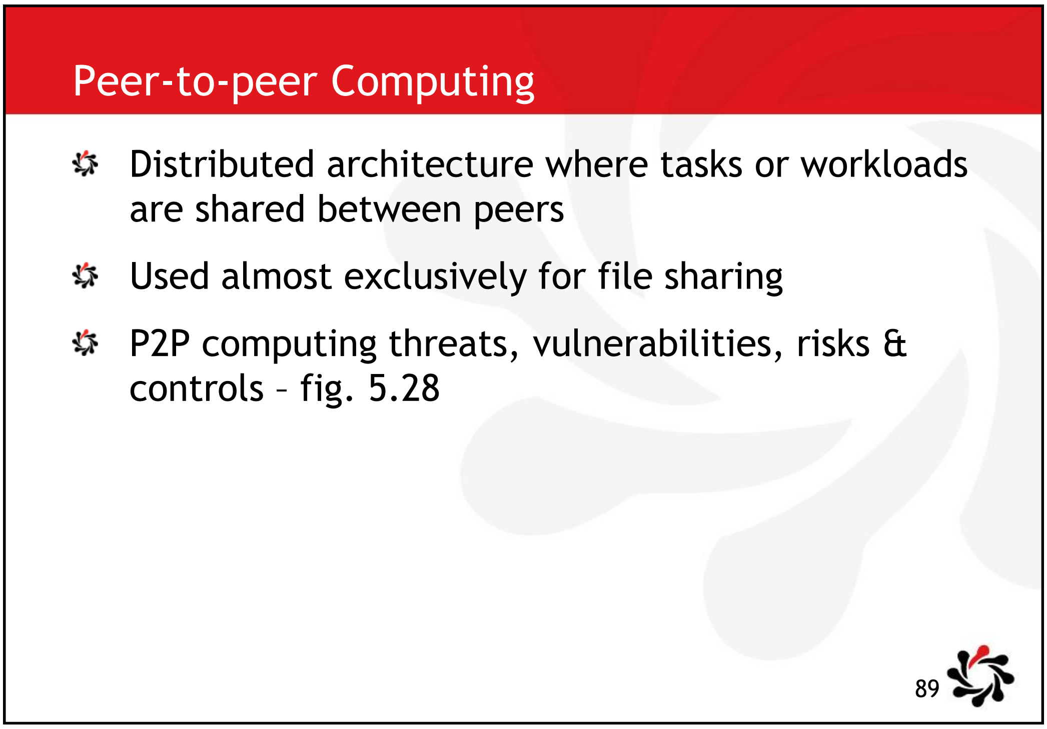
Mobile Computing Controls

- 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



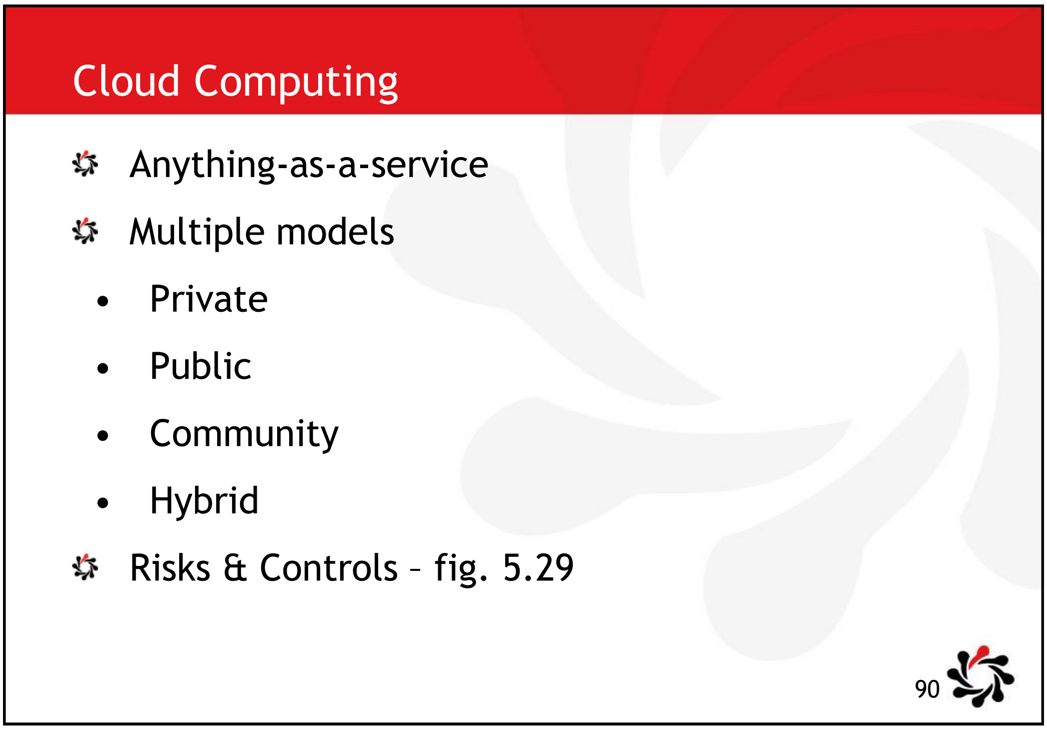
Mobile Computing Controls (continued)

- 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



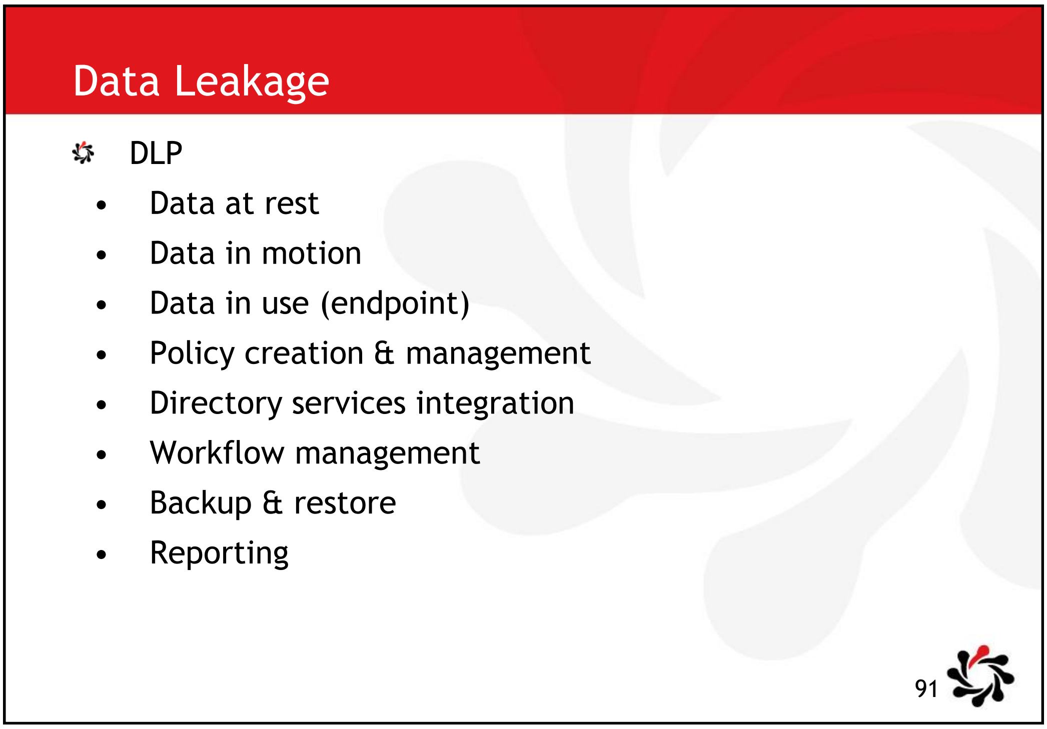
Peer-to-peer Computing

- 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



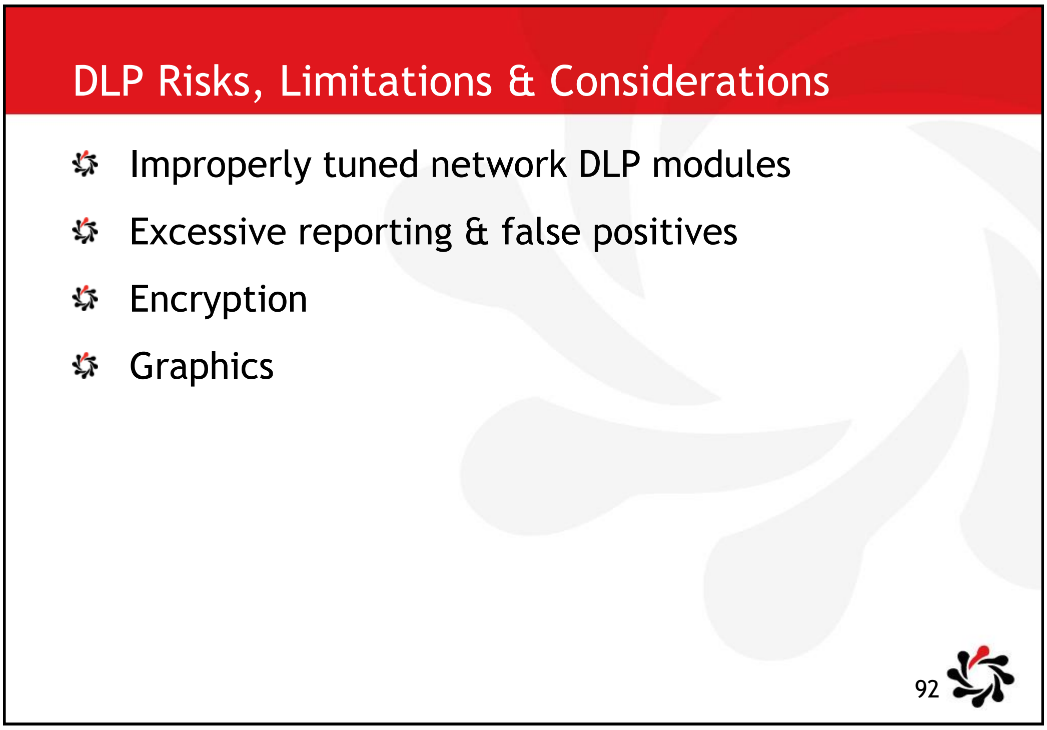
Cloud Computing

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



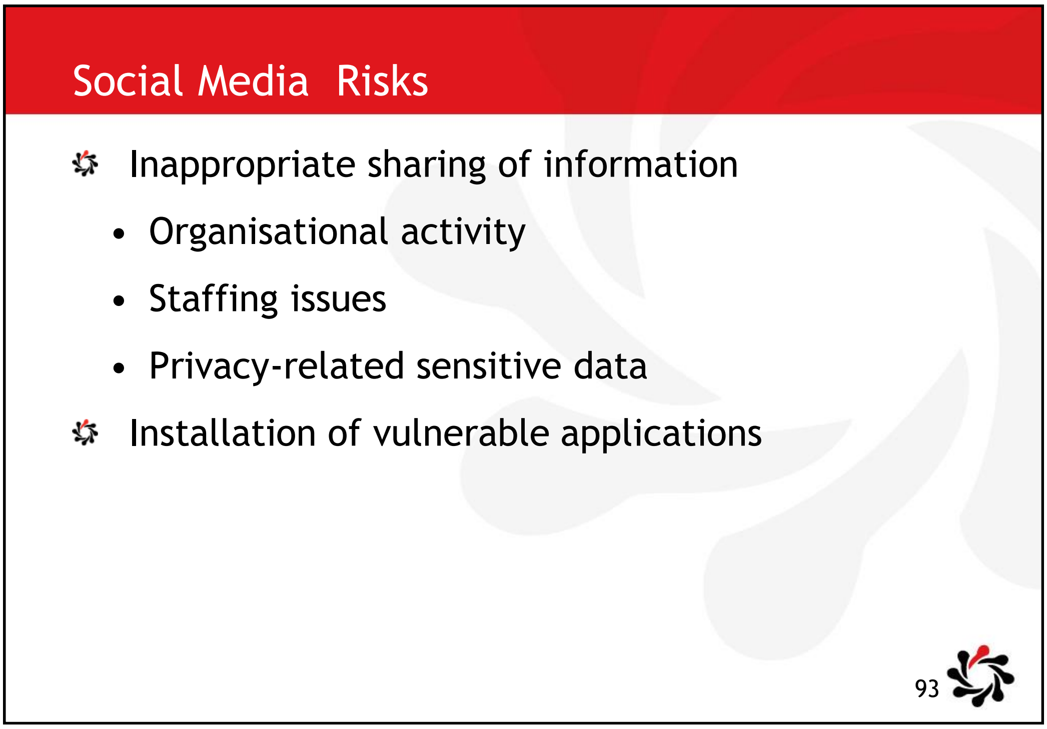
Data Leakage

- 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

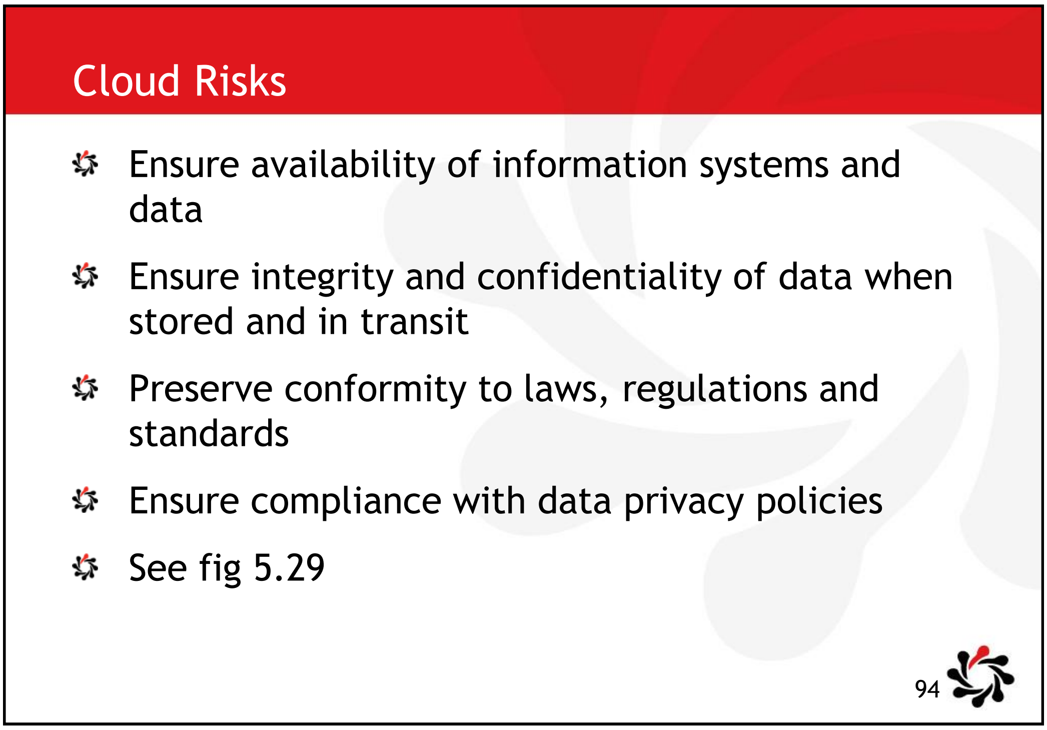
- Improperly tuned network DLP modules
- Excessive reporting & false positives
- Encryption
- Graphics



Social Media Risks

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

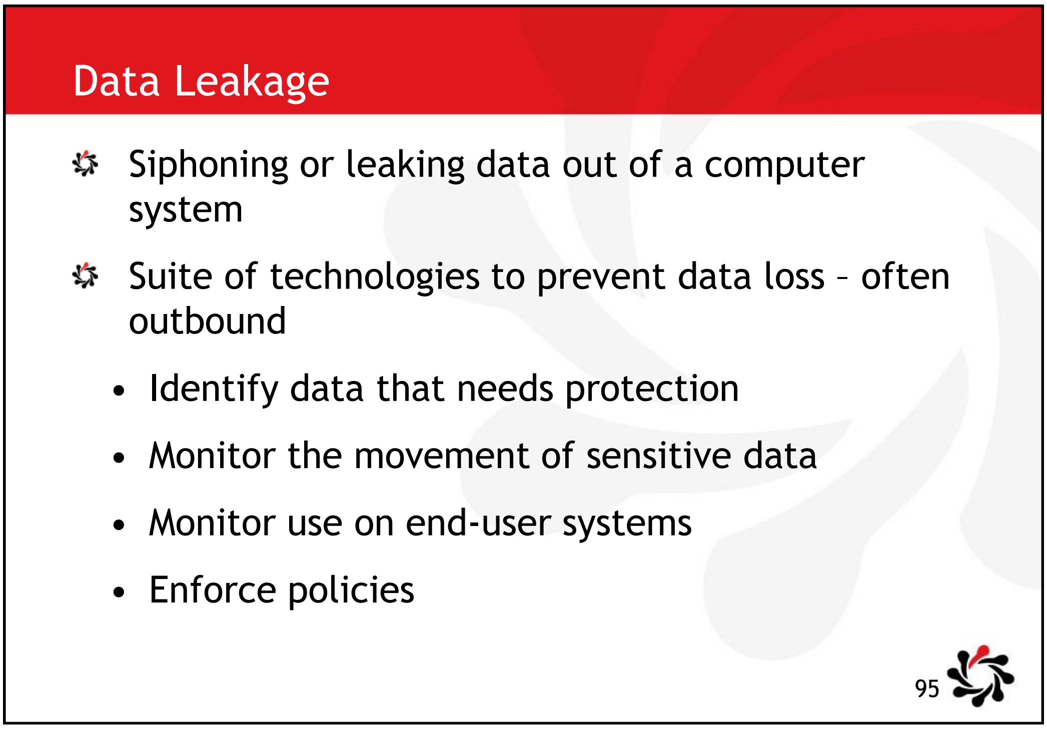
93



Cloud Risks

- Ensure availability of information systems and data
- Ensure integrity and confidentiality of data when stored and in transit
- Preserve conformity to laws, regulations and standards
- Ensure compliance with data privacy policies
- See fig 5.29

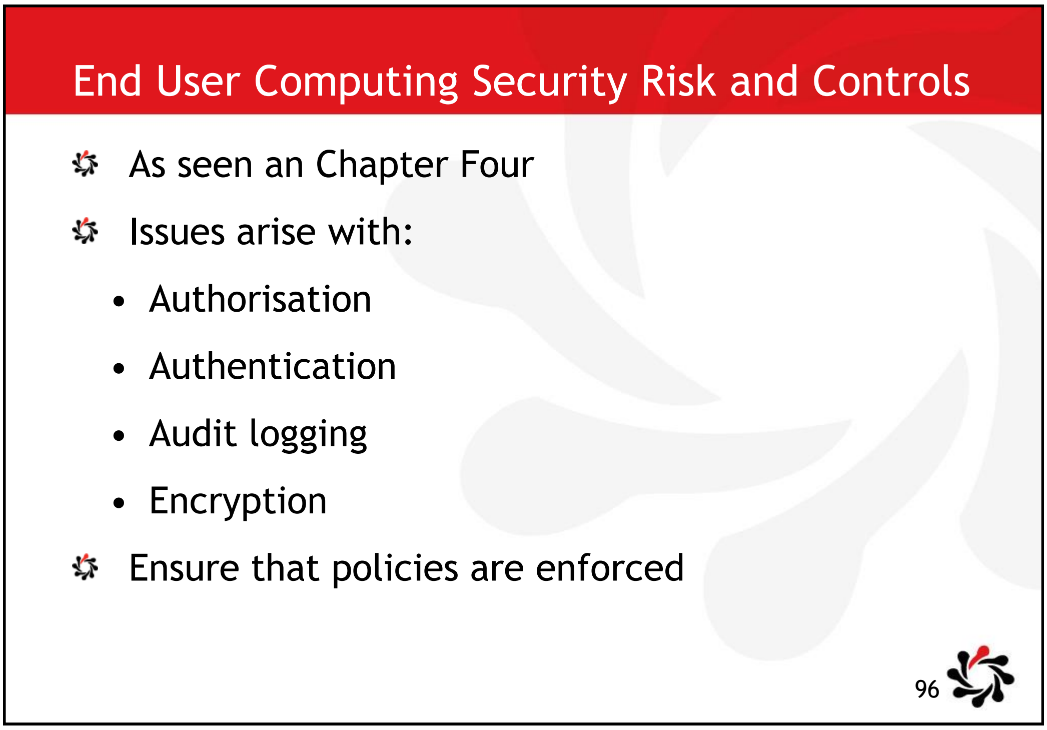
94



Data Leakage

- Siphoning or leaking data out of a computer system
- Suite of technologies to prevent data loss – often outbound
  - Identify data that needs protection
  - Monitor the movement of sensitive data
  - Monitor use on end-user systems
  - Enforce policies

95



End User Computing Security Risk and Controls

- As seen an Chapter Four
- Issues arise with:
  - Authorisation
  - Authentication
  - Audit logging
  - Encryption
- Ensure that policies are enforced

96

End of Chapter Five

97