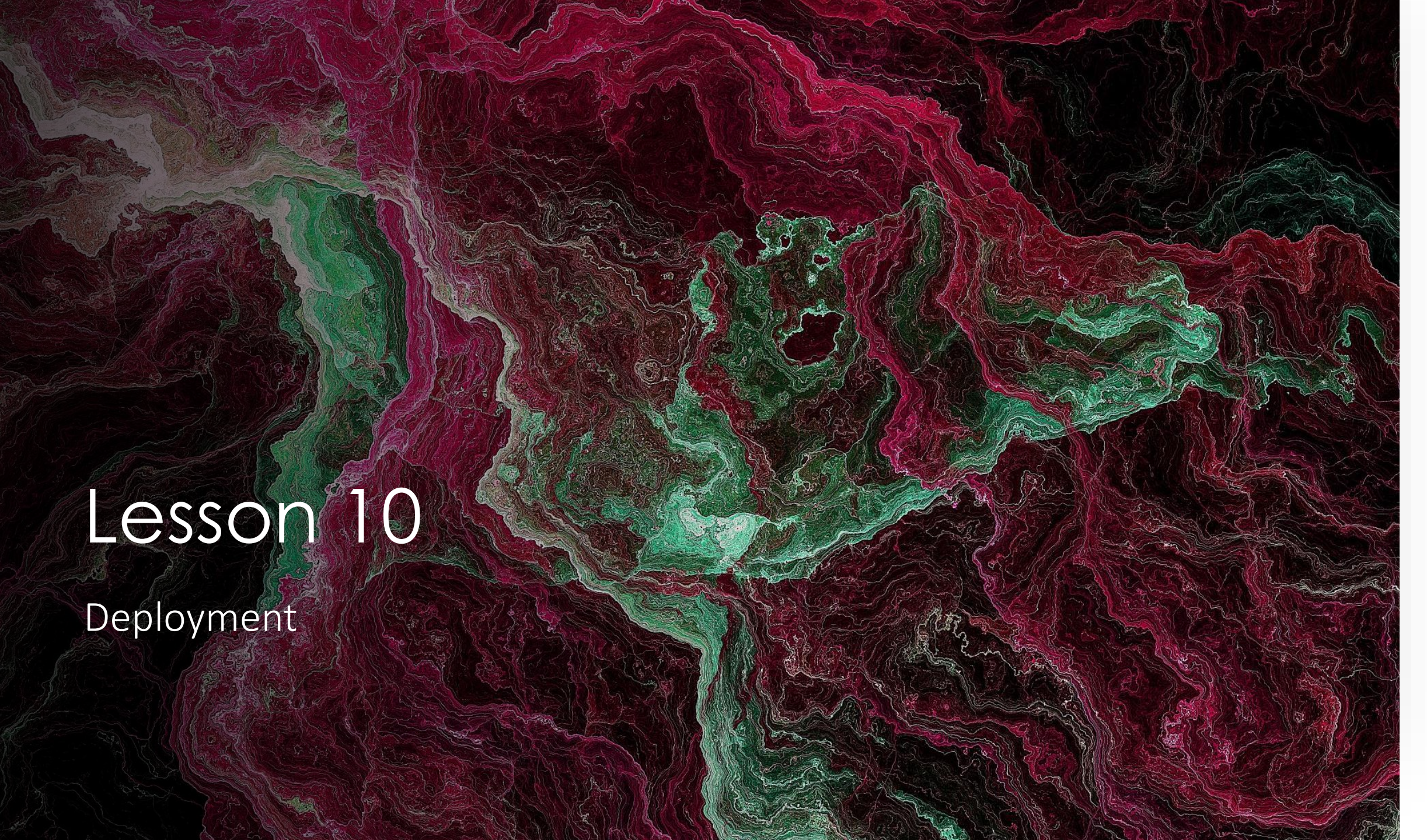
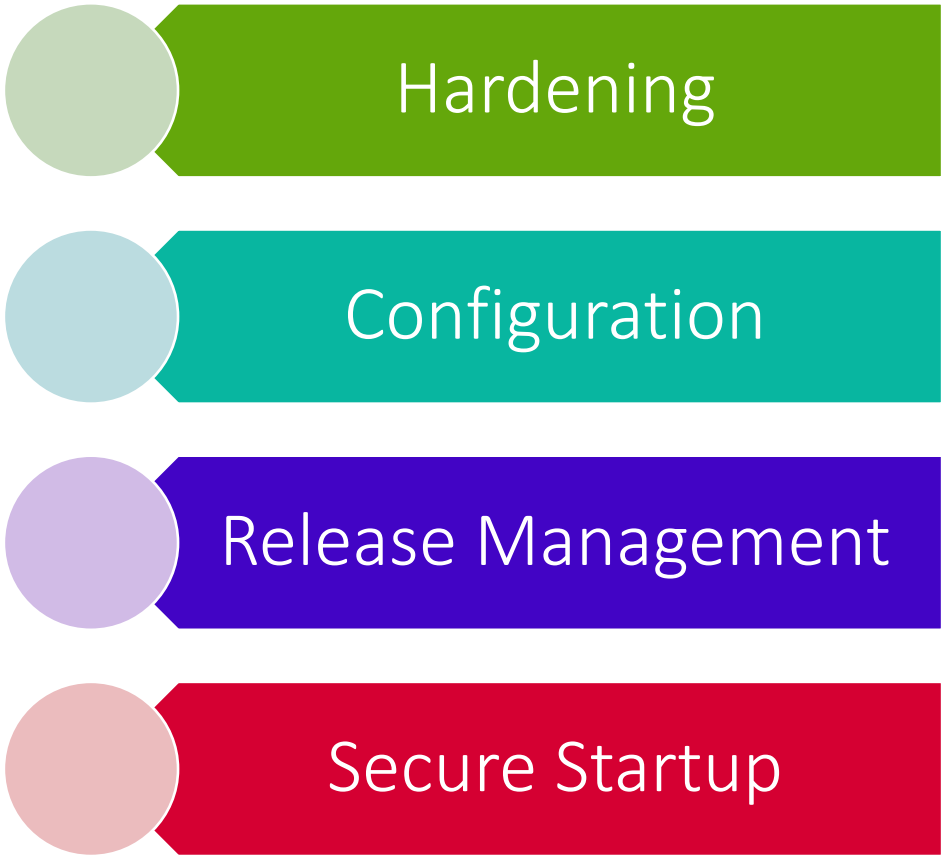


Lesson 10

Deployment

Basic concepts



Common misconfigurations

■Hard coding credentials and cryptographic keys inline code or in configuration files in cleartext.

■Not disabling the listing of directories and files in a web server.

■Installation of software with default accounts and settings.

■Installation of the administrative console with default configuration settings.

■Installation or configuration of unneeded services, ports and protocols, unused pages, and unprotected files and directories.

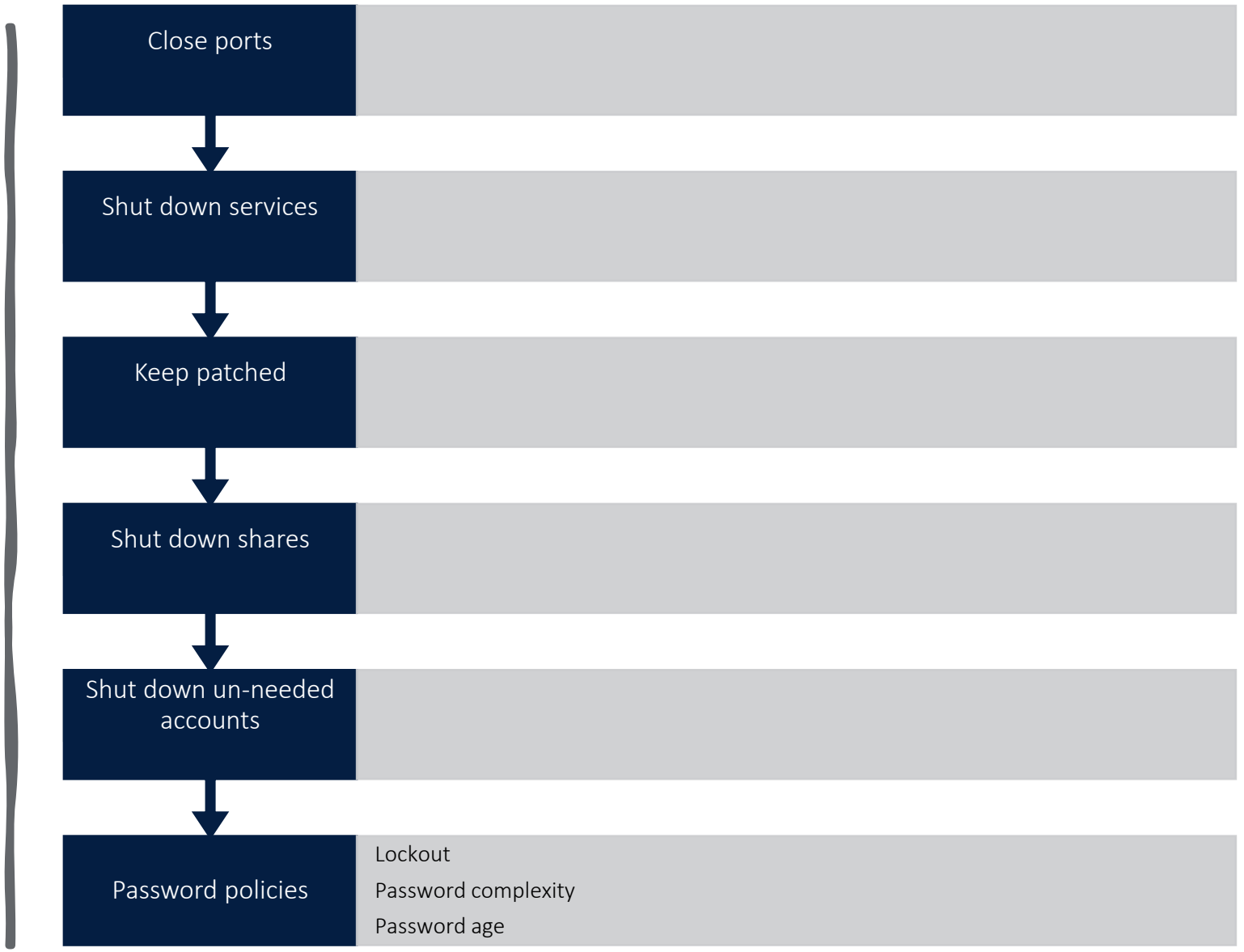
■Missing software patches.

■Lack of perimeter and host defensive controls such as firewalls, filters, etc.

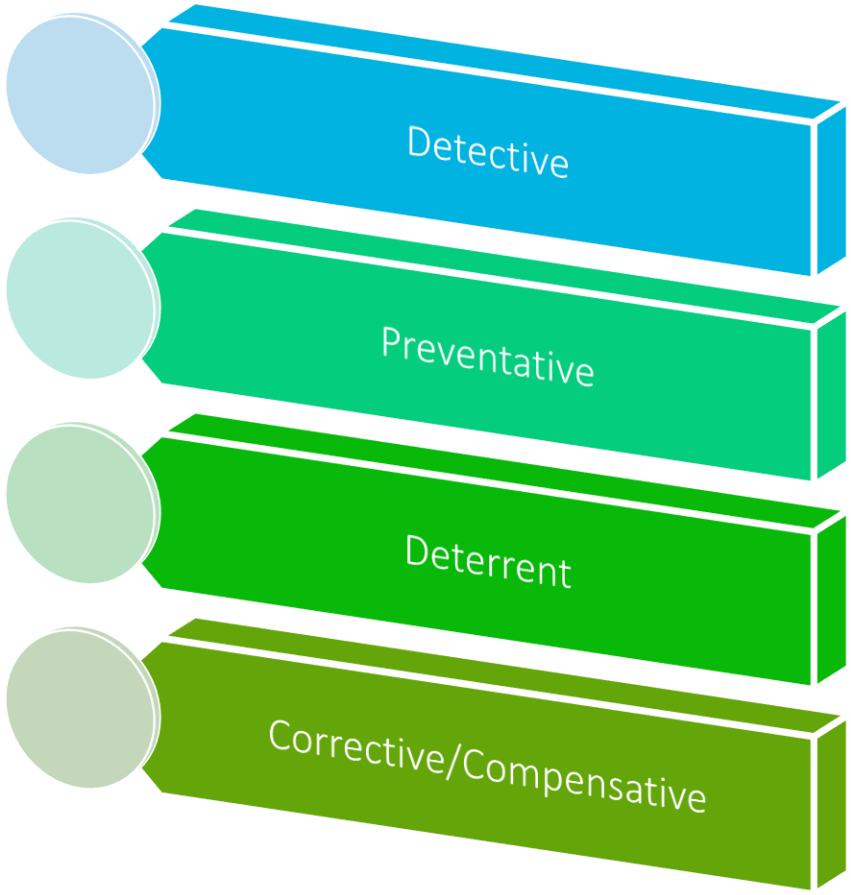
■Enabling tracing and debugging can lead to attacks on confidentiality assurance. Trace information can contain security sensitive data about the internal state of the server and workflow. When debugging is enabled, errors that occur on the server side can result in presenting the entire stack trace data to the client browser.

Paul, Mano (2013-09-03). Official (ISC)2 Guide to the CSSLP CBK, Second Edition ((ISC)2 Press) (Page 523)..

Operating System Hardening



Control types



monitoring

SCANNING

LOGGING

INTRUSION DETECTION

metrics

Characteristics of good metrics are:

- Consistent
- Quantitative
- Objective
- Relevant
- Inexpensive/Affordable

ISACA CISA Definition for Audit

"Systematic process by which a qualified, competent, independent team or person objectively obtains and evaluates evidence regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented."

Auditor Qualification

Independent:

•**Professional Independence**: Auditor acts independent of group being audited

- No friendships, dating, suggestive language parties, lunches

•**Organizational Independence**: Auditor and his/ organization has no special interest in the audited organization

Qualified, Competent:

Adhere to Professional Ethics Standard

•ISACA standard and professional care

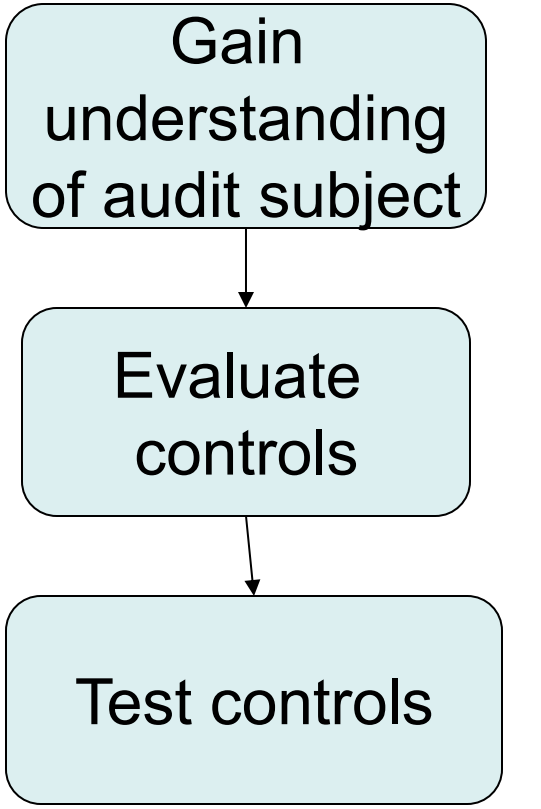
Professional Competence

•Has skills/knowledge to complete task

•Continued professional training/education

IS Audit Definition

IS Audit: Any audit that wholly or partially evaluates automated information processing system, related non-automated processes, & their interfaces



Simplified Audit Process

Definitions

- Control: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
- IT Control Objective A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.
- Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.
- Evidence: Evidence is any information used by the auditors whether the entity or data being audited follows the established audit criteria or objective.
- IT Governance: A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its process**s**

IT Framework

The Framework explains how IT processes deliver the information that the business needs to achieve its objectiv

This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains.

The Framework identifies which of the seven information criterion (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective

IS Control Objectives include

1. Safeguard Assets
2. Integrity of general operations
3. Integrity of sensitive and critical application Systems through:
   - Authorization,
   - Accuracy
   - Reliability
   - Completeness and security of Output
   - Database Integrity
4. Efficiency & Effectiveness
5. Compliance
6. Continuity & Disaster Recovery Plan
7. Incident Response and Handling plan

Evidence gathering Techniques

- Reviewing IS organization structures
- Reviewing IS Policies
- Reviewing IS Standards
- Reviewing IS documentation
- Interviewing appropriate personnel
- Observing processes and employees performance.

Control Self-Assessment (CSA)

- Control Assessment can be defined as a “management technique that assures stakeholders, customers and other parties that internal control system of the organization is reliable.
- It also ensures that employees are aware of the risks to the business and they conduct periodic, proactive reviews of control.

Audit Planning

- **Short-Term**: What do we need to audit this year?
- **Long-Term**: What should we plan to audit in the future?
- What should we test first? Consider…
  - What parts of our business are the most susceptible to risk?
  - What business/IS systems are changing?
  - Are new evaluation tools available?
  - What regulations must we test for?
  - Are there new regulations to test for?

Audit Planning

- **Scheduling**: Cannot test everything this yea
- **Random sampling**: Test all/most types of components randomly
  - transactions, devices, stores
- **Priority**: Test high risk first
- **Automation**: Frequent testing is best

Audit Engagement Plan Vocabulary

Audit Subject: The area to be audited

- E.g., Information Systems related to Sales

Audit Objective: The purpose of the audit

- E.g., Determine whether Sales database is safe against data breaches, due to inappropriate authentication, access control, or hacking

Audit Scope: Constrains the audit to a specific system, function, or unit, or period of time

- E.g., Scope is constrained to Headquarters for the last year.

Perform Risk Assessment

Inherent Risk: Susceptibility to a problem
•E.g., a bank's inherent risk is a robber
Control Risk: A problem exists that will not be detected by an internal control system
•For bank: A thief accesses another's account at Money Machine but is not detected
Detection Risk: An auditor does not detect a problem that does exist
•For bank: Fraud occurs but is not detected
Overall Audit Risk: Combination of audit risks

What Inherent, Control & Detection Risks exist on the IT side.

Prepare Audit Engagement Plan

- Develop risk-based approach
- Include audit objectives, scope, timing, required resources
- Comply with applicable law
- Develop audit program and procedures

Add Detail to Plan

Tools for the Auditor

ISACA has Standards and Guidelines related to Audit (

- Section 2200 General Standards
- Section 2400 Performance Standards
- Section 2600 Reporting Standards
- Section 3000 IT Assurance Guidelines
- Section 3200 Enterprise Topics
- Section 3400 IT Management Processes
- Section 3600 IT Audit and Assurance Processes
- Section 3800 IT Audit and Assurance Management

Perform Tests

Evidence: Audit findings must be based on sufficient and reliable evidence and appropriate interpretation of the evidence

Documentation: The audit work and audit evidence to support conclusions must be fully documented

Supervision: Audit staff is supervised to ensure that audit is professionally completed

Professional Skepticism: The auditor must keep an eye open for irregularities and/or illegal acts, unusual relationships, material misstatements

•When irregularities are encountered, the auditor should:

- Investigate fully
- document all communications, tests, evidence, findings
- report the irregularity to governance body in a timely manner

Substantive v Compliance Testing

Compliance Testing:

- Are controls in place and consistently applied?
- Access control
- Program change control
- Procedure documentation
- Program documentation
- Software license audits
- System log reviews
- Exception follow-ups

Substantive Testing:

- Are transactions processed accurately?
- Are data correct and accurate?
- Double check processing
- Calculation validation
- Error checking
- Operational documentation
- If Compliance results are poor, Substantive testing should increase in type and sample number

Compliance Testing

- Control: Is production software controlled?
- Test: Are production executable files built from prod source files?
- Test: Were proper procedures followed in their release

- Control: Is Sales DB access constrained to Least Privilege?
- Test: Are permissions allocated according to documentation?
- Test: When sample persons access DB, can they access only what is allowed?

Substantive Testing

- Audit: Is financial statement section related to sales accurate?
- Test: Track processing of a sample transactions through the system, performing calculations manually
- Test: Test error conditions

- Audit: Is tape inventory correct?
- Test: Search for sample days and verify complete documentation and tape completeness

Sampling

Statistical Sampling:

•N% of all items randomly tested

•Should represent population distribution

•**Variable Sampling**: How accurate is the sample population in matching the full population?

•Determine appropriateness of sampling: (e.g., $, weight, amount): Sample average $24.50, Real average: $26.99

No statistical (or Judgment) Sampling:

•Auditor justifies another distribution for sample selection

•Which items are most risky?

Sampling

Tolerable Error Rate: The maximum allowable error rate (e.g., inappropriately documented changes)

Non-Statistical Sampling includes**:**

Discovery Sampling: A minimal testing model used when the expected occurrence rate is extremely low (e.g., find fraud, break laws)

Stop-or-Go Sampling: If the first 20 have zero errors, then stop. Else if the first 100 have < 10 errors, stop. Else…

Attribute Sampling: How many of X have Y attribute?

•E.g. How many changes are appropriately documented?

Generalized Audit Software (GAS)

- File Access: Read records & file structures
- File reorganization: Allow sorting, indexing, merging/linking with other files
- Data Selection: Select a set of records
- Statistical functions: Perform sampling, stratification, frequency analysis
- Arithmetic Functions: Perform arithmetic operations on data sets

Prepare Audit Report

Identify & Include:

- Organization, recipients, restriction on circulation
- Scope, objectives, period of coverage, nature, timing a extent
- Findings, conclusions, recommendations/follow up, and reservations or qualifications
  - Grouped by materiality or intended recipient
  - Mention faults and constructive corrections
- Evidence to support results (may be separate)
- Overall findings, conclusion, & opinion
- Signed & dated

Perform Tests

Review IS Organization: Separation of duties

Review IS Policies, Standards, Procedures: Defined, periodically updated

Review IS Documentation: Policy, Procedures, Design, Test, Operations, Contract/SLAs, Security

Interview personnel: Segregation of duties, security awareness, competency

Observe personnel: Document everything in sufficient detail

Taguchi Methods

- Taguchi Methods are a set of statistical and experimental design techniques developed by Japanese engineer Genichi Taguchi to improve product and process quality by making them more robust—that is, less sensitive to variations (or “noise”) that are hard or impossible to control.
- They are especially valued in engineering design, manufacturing, and quality control because they emphasize building quality into the design stage, rather than relying solely on inspection and rework.

Taguchi Methods

- Taguchi Experiment Steps
- Define Objective
- State the performance characteristic to optimize.
- Identify Factors & Levels
  - Control factors (design parameters) and noise factors (environmental or manufacturing variability).
- Select an Orthogonal Array
  - Choose based on number of factors and levels (e.g., L8, L9, L16 arrays).
- Conduct Experiments
  - Run trials according to the array, systematically varying factors.
- Analyze Results
  - Calculate S/N ratios, determine optimal settings, and predict performance.
- Confirm
  - Validate the chosen settings through confirmation experiments.