Stepping Through the Information Security Audit

BEAR STEARNS

Jennifer Bayuk

CSI
COMPUTER SECURITY INSTITUTE

IS Audit Overview

1. **Understand the purpose**
2. **Know the process**
3. **Participate**
4. **Respond**

Purpose:

To determine the adequacy of

management controls

over

information services.

Working Definition:

- IS Audit is a process by which something is verified
  - In response to a management concern
    - With respect to computers as assets, operational integrity, data confidentiality, assets controlled by software, or any combination of the above
- Auditee is the IT manager delegated the responsibility for addressing concerns with respect to the technology

IS Audit Focus:

- **Management uses controls to ensure:**
  1. integrity in preparation of data; and
  2. access to assets occurs only with authorization.

- **Information services managers are responsible for technology controls.**

- **The objective of a technology control is to prevent, detect, or correct undesired events.**

Chronology of Concerns

- Feynman through Hopper through the mythical man-month – Focus on correct results

"data in" correlating to "data out"

- Fraud and Hacking – Focus on User Administration

data integrity, authorization, segregation of duties

- The Morris Worm – Focus on IT Heroes

exits, back doors, vulnerabilities

- COSO - Focus on Internal Control Structures

Strategic plans, defined policies, documented procedures, segregated job functions, change schedules, performance measures, cost control, quality management, and disaster recovery plans in support of an Internal Control Structure.

The tone is set at the top.

CSI COMPUTER SECURITY INSTITUTE

ISACA Serving IT Governance Professionals

Chronology of IT Audit

1960s: Recognition of new field: Automation Training Institute introduces CACS

Early 1970s: Influential Publications: EDPACS, IIA *Systems Auditability Control Report* (SAC).

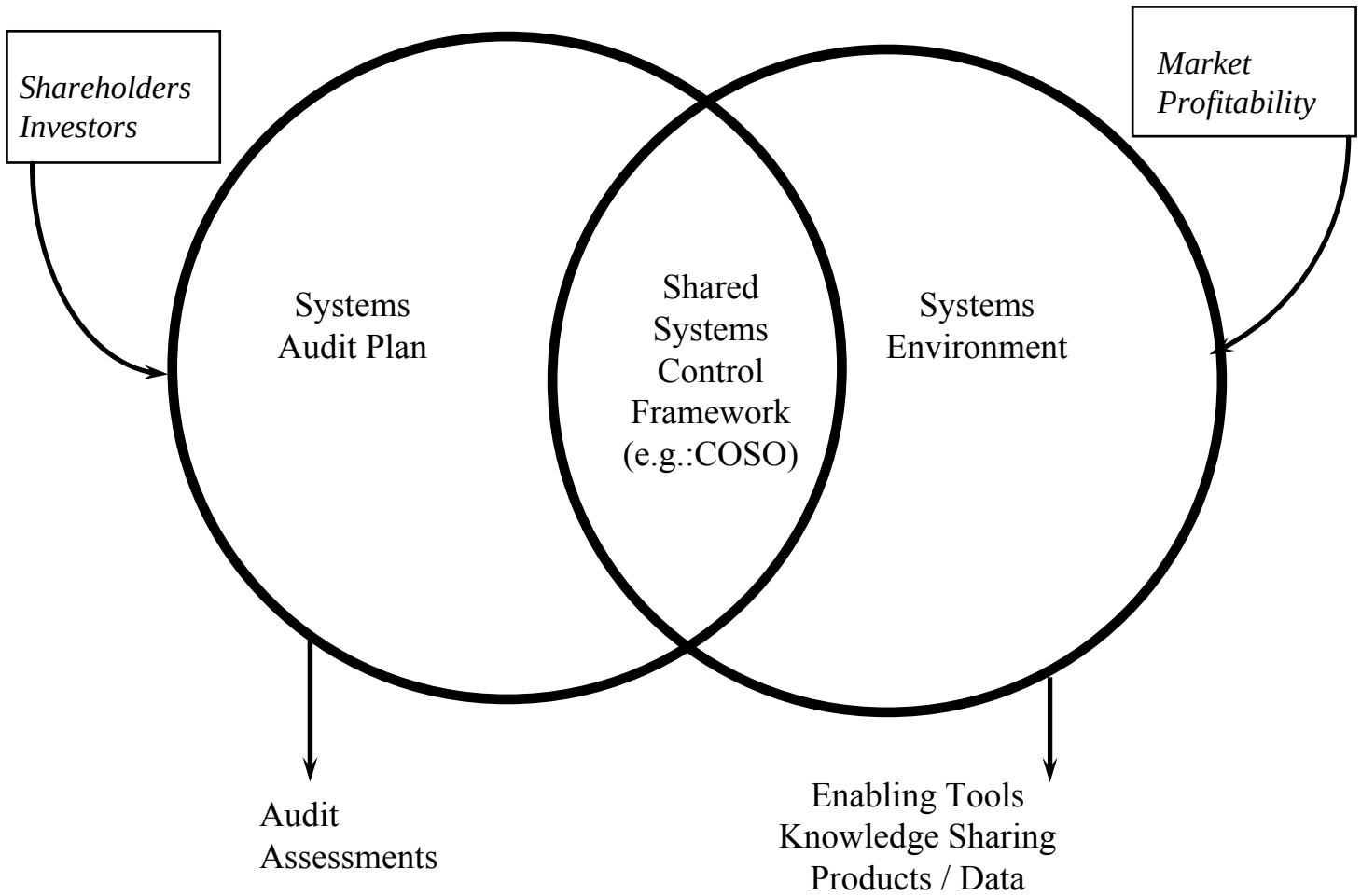
Late 1970s: EDPAA published *Control Objectives* and introduces CISA

1980s: EDPAA purchases CACS and publishes COBIT

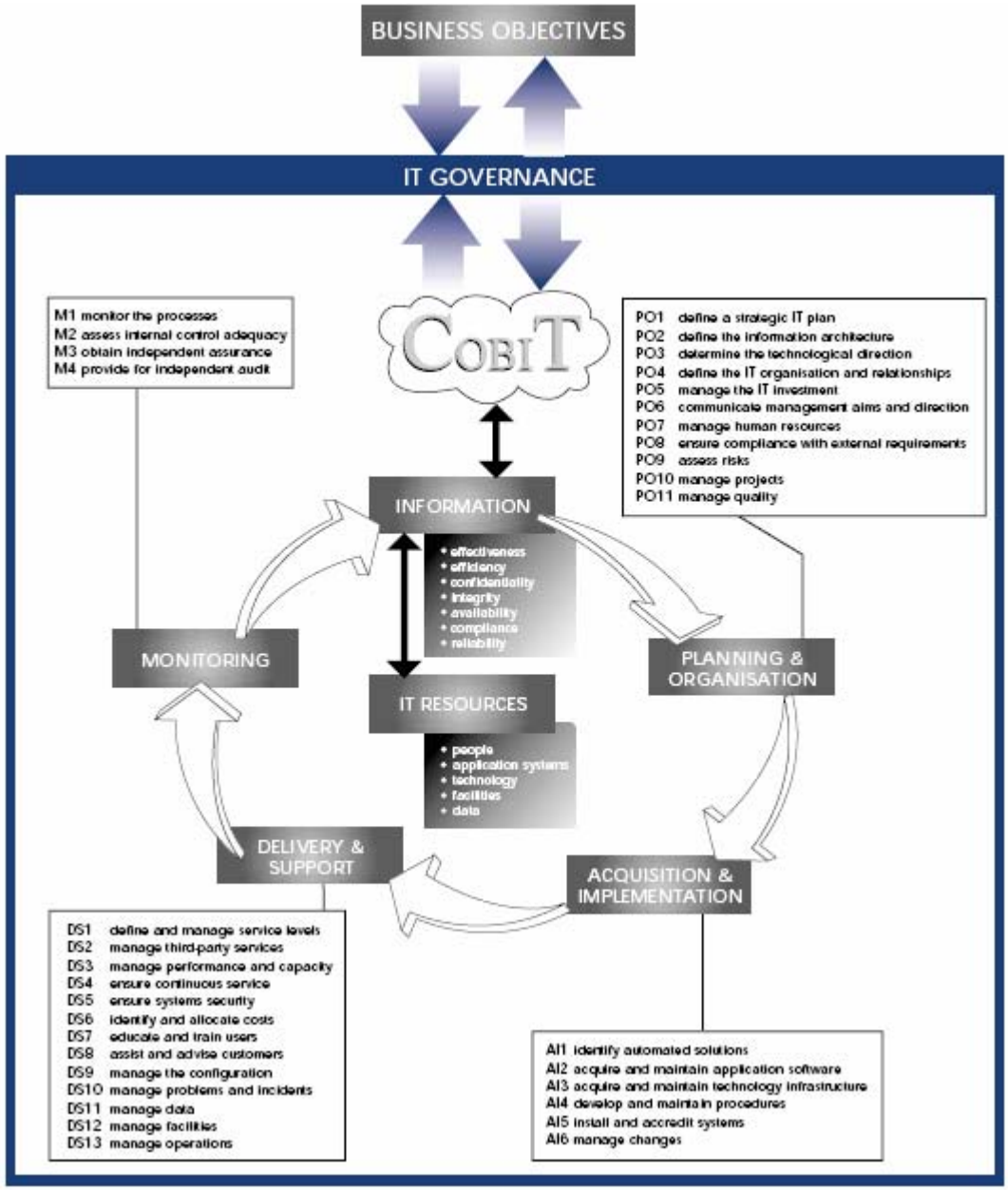
1990s: EDPAA becomes ISACA, global expansion to >40 countries and ~20,000 members

Today: ISACA has 48,000 CISAs, over 90 countries, introduced CISM

Example IS Controls Methodology



Shared Control Framework

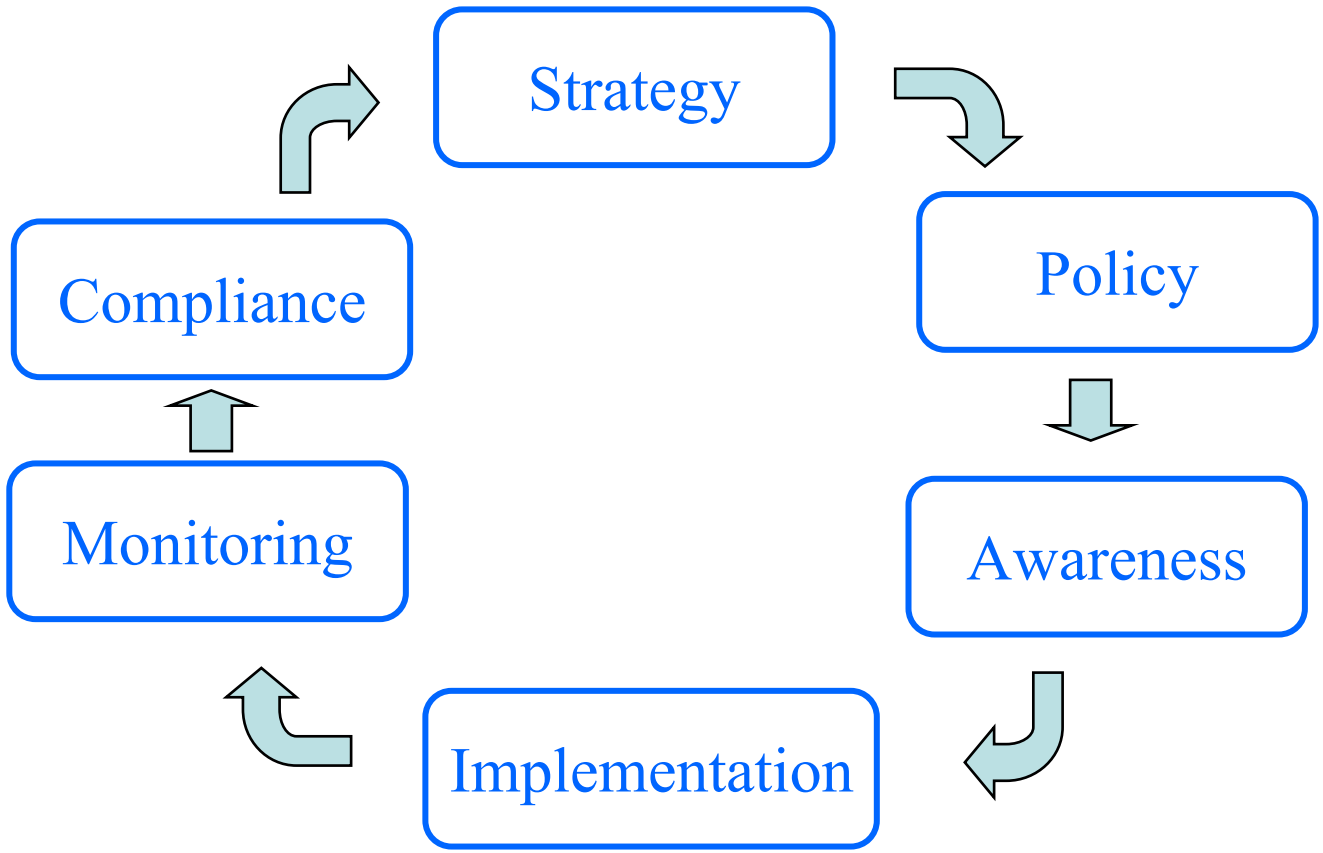


Source: COBIT

COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Example Shared Control Framework



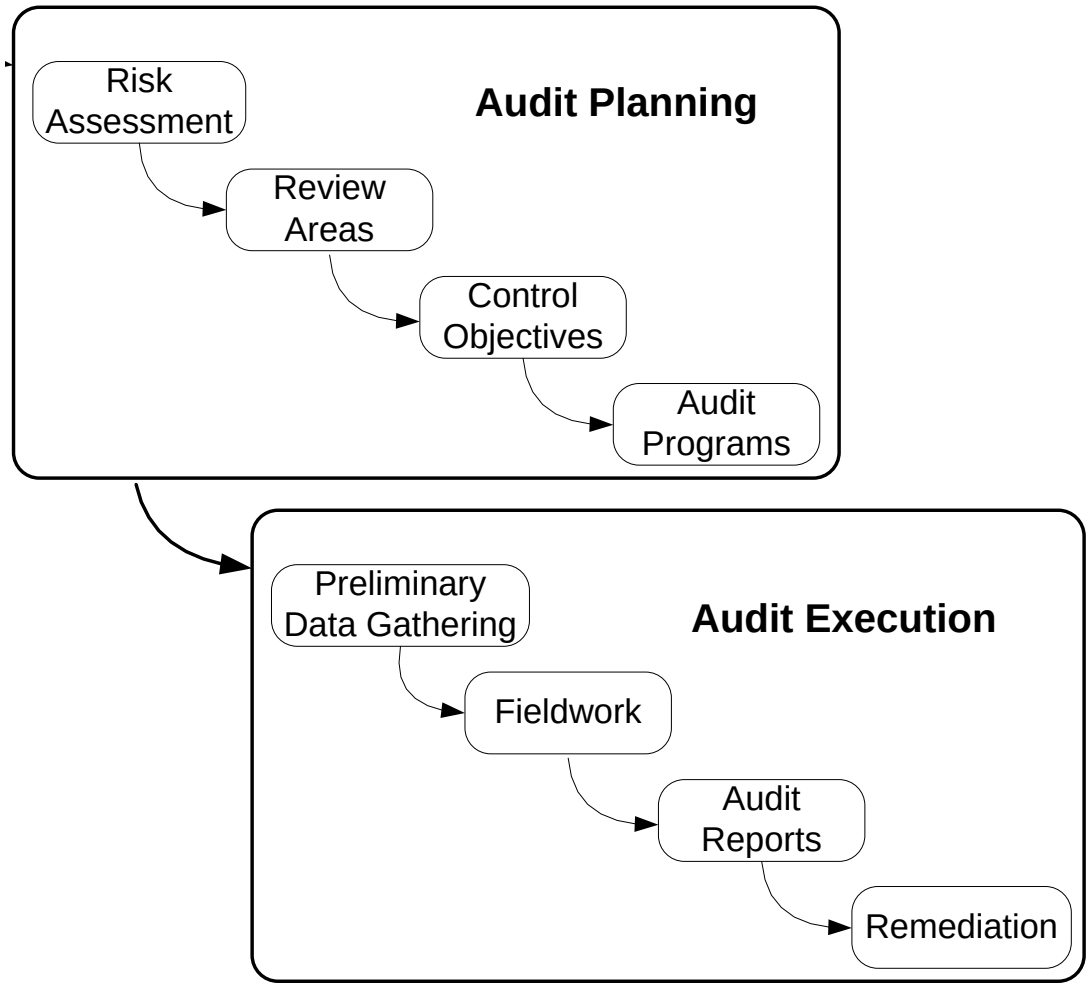
Audit versus Assessment

- Audit
  - Management control testing where passing implies underlying security
    - Internal and External Audit in the COSO Model
    - Regulator Review of Compliance
  - Process audits, where passing does not imply underlying security (e.g. ISO7799)
- Assessments - passing cannot be assumed to prove underlying security, some common examples:
  - Control self-assessments
  - Design/Architecture reviews
  - Due diligence reviews
  - Penetration studies

Types of Audits

- Regulatory Environment
  - Anti-Terror
  - Data Protection
  - Internal Control
- Best Practices
- Compliance versus Substantive

The Audit Process



Audit Planning

Risk Assessment

- Financial Analysis, Interviews with executives, analysis of critical operations, in search of:
  - Inherent risk
  - Control risk
  - Detection risk

\+ Control Frameworks

- Interviews with executives and review of organizations structure, policies, and procedures established in support of control objectives

≈ Audit Plan

Risk Assessment Example

Technology Risk Model – draft							
3 = High Risk - required for business continuity, few manual compensating controls							
2 = Medium Risk - required for business continuity, considerable manual compensating controls							
1 = Low Risk – not required for business continuity							
0 = No systems of that type required to run business							
Last Audit = years since system was audited AND found well controlled, weight = years, if never, weight =3							
Reputational Risk = percentage of interviewees that consider the system of media interest							
Perception = percentage of interviewees that expresse concern over system control environment							
Overall Risk Ranking - multiply reputational risk by perception and by sum of risk and audit weights							
Risk Affecting Factors:	Risk to Outsource	Risk to Deploy	Risk to Consult	Prior Audit	Reputational Risk	Perception	RISK RANKING
Corporate Internet Systems	3	3	3	1 year	100%	80%	8.00
Client-Owned Systems on-site	3	2	0	1 year	100%	60%	3.60
Office automation systems	1	1	1	2 years	5%	10%	0.03
Billing Systems	2	2	3	1 year	80%	30%	1.92
Backoffice Systems	2	2	2	2 years	40%	10%	0.32
Scheduling, Time & Expense	1	2	3	never	50%	30%	1.35
Voice Telecommunications	2	2	3	5 years	80%	0%	0.00
Data Telecommunications	3	2	2	3 years	100%	30%	3.00
Change control systems	2	2	1	2 years	50%	40%	1.40
Call Center /Help Desk	1	1	1	never	80%	20%	0.96

Review Areas

A review that is:	**Process-oriented**
will focus on:	*a given IT process*
so its scope will include:	*the systems used to create input for, to execute, or to control the process.*
A review that is:	**Business-oriented**
will focus on:	*a given business process*
so its scope will include:	*the systems necessary to support the business process*
A review that is:	**Control-oriented**
will focus on:	*how a technology controls are enforced*
so its scope will include:	*all, or a representative sample, of the systems for which the control is expected to be in place.*

CSI COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Review Area Examples

Planning & Organization
Define a strategic IT plan
Define the information architecture
Determine the technological direction
Define the IT organization and relationships
Manage the IT investment
Communicate management aims and direction
Manage human resources
Ensure compliance with external requirements
Assess risks
Manage projects
Manage quality

Acquisition & Implementation
Identify solutions
Acquire and maintain application software
Acquire and maintain technology architecture
Develop and maintain IT procedures
Install and accredit systems
Manage changes

Delivery & Support
Identify solutions
Acquire and maintain application software
Acquire and maintain technology architecture
Develop and maintain IT procedures
Install and accredit systems
Manage changes
Define service levels
Manage third-party services
Manage performance and capacity
Ensure continuous service
Ensure systems security
Identify and attribute costs
Educate and train users
Assist and advise IT customers
Manage the configuration
Manage problems and incidents
Manage data
Manage facilities
Manage operations

Monitoring
Monitor the processes
Assess internal control adequacy
Obtain independent assurance
Provide for independent audit

ource: COBIT

CSI COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Controls

- Control Objectives
- Control Activities
- Control Points

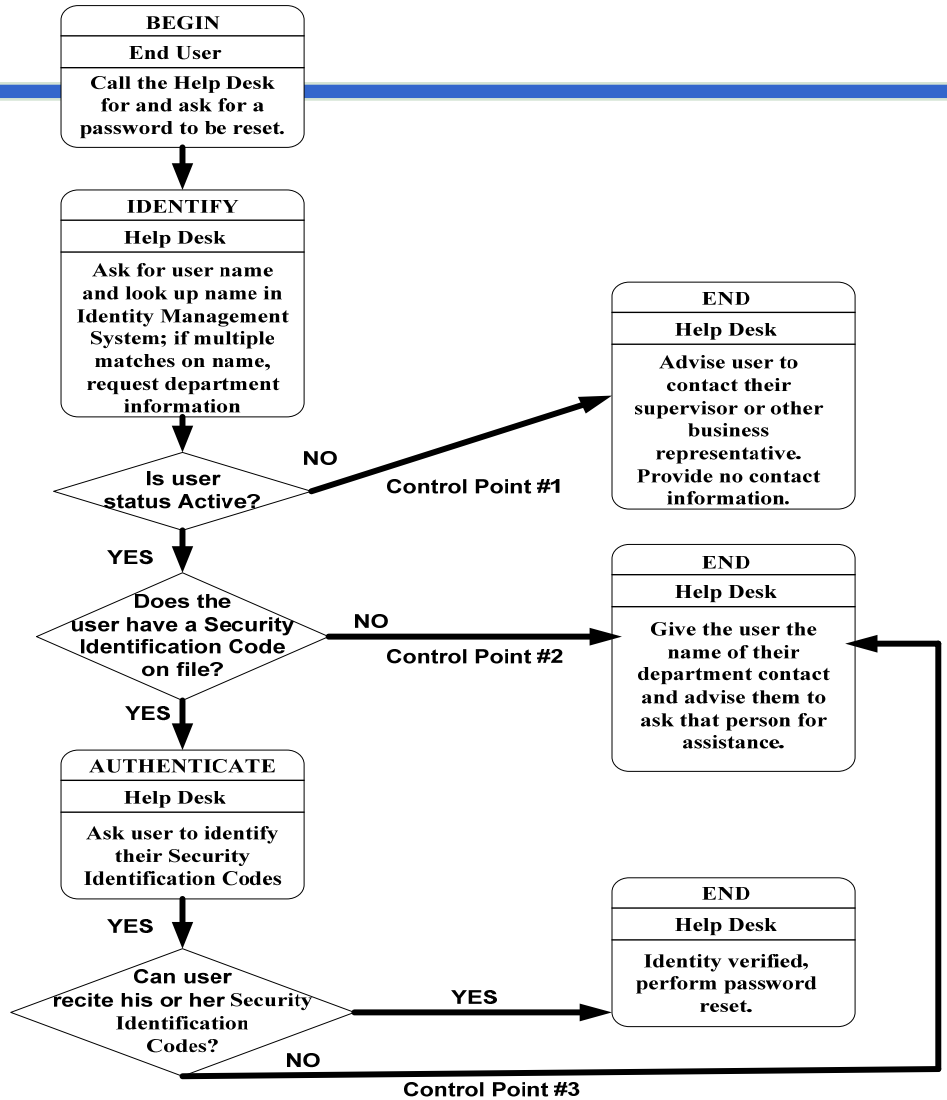
Control Objectives

- **Control objectives are specific, measurable goals that individual controls are designed to achieve.**
- **Auditors may set their own control objectives for an environment (except in a SAS70 audit).**
- **However, auditors do take into account management's control objectives.**

Scope

- Technical term that refers to the business purpose of the review.
- Maps to a set of control objectives

Control Activity Example



CSI COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Audit Programs

- Step by step process in performing an audit
- Guides to ensure that audits are on track
- Evidence that audits are complete
- Training materials to bring new auditors up to speed in a new technology

Audit Steps

- **Audit steps specify the actions that an auditor will take to independently gather evidence of activity established by management that contributes to control objectives.**
- **Steps in the IS audit plan should be identified by review area, control objective, and expected activity.**
- **If the expected activity is missing from a given IS environment, steps may be replaced by management demonstrations of compensating controls.**

Compensating Controls

Prevention, detection, and correct hierarchy:

It is best to prevent undesired events from happening.

- If undesired events cannot be prevented from happening, they should at least be detected.
  - If undesired events cannot be prevented and are not detected in time for incident response activities prevent harm from occurring, the situation must be correctable.

Audit Program Example

The plan is to review Information Protection, which addresses the security of the organisation's data and access privileges established in conformance with legal and regulatory requirements.

These high level control objectives:	are characterized as:	and will be evident through executing the audit steps:	Evidence	Pass /Fail
Ensure systems security, that is, safeguard information against unauthorised use, disclosure or modification, damage or loss.	IT security should be managed such that security measures are in line with business requirements. This includes: ▪ Translating risk assessment information to the IT security plans ▪ Implementing the IT security plan ▪ Updating the IT security plan to reflect changes in the IT configuration ▪ Assessing the impact of change requests on IT security ▪ Monitoring the implementation of the IT security plan ▪ Aligning IT security procedures to other policies and procedures	Obtain a copy of any IT and/or organisation-wide policies and procedures relating to information system security and access		
		Obtain a copy of relevant policies and procedures, and legal and regulatory body information systems security requirements (i.e., laws, regulations, guidelines, industry standards).		
		Interview IT senior and security management, data base administrator, security administrator and application development management.		
		...		
	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules.	Obtain an inventory of IT computing resources that contain information to be protected.		
		Verify that procedures for access control and user authorization on identified systems comply with policy.		
		Observe user authorization procedures.		
		...		
	...			
Manage Third Party Services, that is, ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements	Management should ensure that all third-party providers' services are properly identified and that the technical and organisational interfaces with suppliers are documented.	IT policies relating to third-party relationships exist, are consistent with other organisational policies and address need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required.		
		Interfaces are defined to independent agents involved in the conduct of the project and any other parties, such as subcontractors.		
		...		
	...	Contract contents include at least the following: ...		

CSI COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Evidence Evaluation

- Evidence obtained from outside sources is more reliable than evidence provided by the organization being audited.
- The qualifications of the person providing the evidence should be considered.
- Objective evidence is more reliable than that which requires evaluation or interpretation.

Audit Execution

- Preliminary Data Gathering
- Fieldwork
  - Opening Meeting
  - Onsite testing
  - Closing Meeting(s)
- Reporting

Preliminary Data Gathering

When auditor calls to schedule opening meeting, ask for :

- List of review areas and control objectives per review area
- Copy of audit steps - advance look at software packages if applicable
- Expected duration of fieldwork

Clear calendars of key personnel - ensure those most knowledgeable of your control structure are available to be interviewed at some point during fieldwork.

Opening Meeting

- Finalize scope (list review areas)
- Agree on control objectives
- Assign primary contacts for each review area
- Schedule pre-closing meeting

Fieldwork

- Ensure availability of resources required for auditor to complete audit steps (i.e. not your staff).
- Ensure supervision of all auditor access to systems. Encourage staff to discuss with the auditor what conclusions they are drawing from their observations.
- Ask auditor periodically:
  1. "Are you waiting on anyone or anything?"
  2. "Have you identified any concerns?"
- Be quick in pointing out compensating controls.

Audit Points

Condition:	a factual description of audit evidence
Criterion:	some objective standard as to why the audit point is valid
Cause:	the root cause of the situation that introduced the control weakness
Effect:	the risk that the condition presents to the audited organization
Recommendation:	Auditor's opinion on what control activity should be established to mitigate the risk of the bad effects due to condition.
And/Or	
Management Response:	IT Manager's action plan that will change the condition.

CSI COMPUTER SECURITY INSTITUTE

ISACA® Serving IT Governance Professionals

Closing Meeting(s)

- Pre-closing meeting
  - list all identified control weaknesses
  - review evidence gathered by auditor of any identified a control weakness
  - provide evidence of compensating controls; obtain agreement as to adequacy of controls
  - if necessary, schedule another pre-closing

- Closing meeting
  - No surprises

The Final Report

1. **Executive Summary**
2. **Audit Points**
2. **Management Responses**
3. **The CC list**

Executive Summary

Short summary of audit results, usually containing:

- approximately one sentence to each audit point
- a one-line indication of whether the auditor is satisfied that IT Management adequately addresses business risk

Example 1:

> Policies and procedures in place reflect best practices in most of the areas reviewed. Our overall assessment for the environment is satisfactory.

Example 2:

> We applaud the efforts of IT management to improve controls, but the recognition of the job still to be done renders the overall assessment for the environment unsatisfactory.

Audit Points

- You should have access to a draft of the final report that includes all audit points and at least a week to request revisions. If you don't like the wording or tone, ask the auditor to change it.
- Negotiate agreement with the auditor on:
  - Condition - make sure the condition factually describes audit evidence and makes no judgement (just the facts)
  - Criteria - ensure that there is some objective standard as to why the audit point is valid
  - Cause - make sure that the root cause is identified rather than some proximate cause
  - Effect - agree with the auditor on the risk that the condition present to the business, not only to the computing environment
- It is nice if you can agree on the Recommendation too, but not necessary

Management Responses

- You should have the opportunity to answer every audit point in the report with a Management Response. Make it an action plan.
- Where possible, correct things before the response is due, so the response can read: "Management agrees. Action completed."
- Where action plans to close any identified vulnerabilities need more time, show that the solution will be done as part of activities that are routinely performed by your organization.

The CC list

- Make sure the draft report includes a CC list; if not, ask the auditor for one.
- The CC list will usually include:
  - your boss
  - the head of your business unit
  - the chief financial officer of your organization
  - the chair of the board of director's audit committee
  - the external audit partner assigned to your company

  If anyone else is on it, find out why.
- If you think anyone on the list will be surprised or misunderstand the report, discuss it with them immediately.

Remediation

Until the condition described in all audit points has changed to reduce risk to an acceptable level, expect:

- Periodic Query
- Formal Tracking
- Board-level reporting

Survival Strategies

- **Accept the validity of the exercise as a management tool.**
- **Identify the audit plan and the auditor's strategy.**
- **Coordinate your organization's response the audit process.**
- **Use the reporting process to demonstrate your organizational strengths.**

Discussion