BEAR
STEARNS

How to survive an IS audit

Jennifer L. Bayuk
jbayuk@bear.com

BEAR STEARNS

Survival Strategies Overview

1. Understand the point
2. Know the rules
3. Participate in the process
4. Welcome the opportunity

BEAR STEARNS

Survival Strategy One:

Accept the validity of the audit as a management exercise.

(exercise is almost a sport!)

BEAR STEARNS

The point of the game:

To determine the adequacy of

management controls

over

information services.

BEAR STEARNS

The playing field:

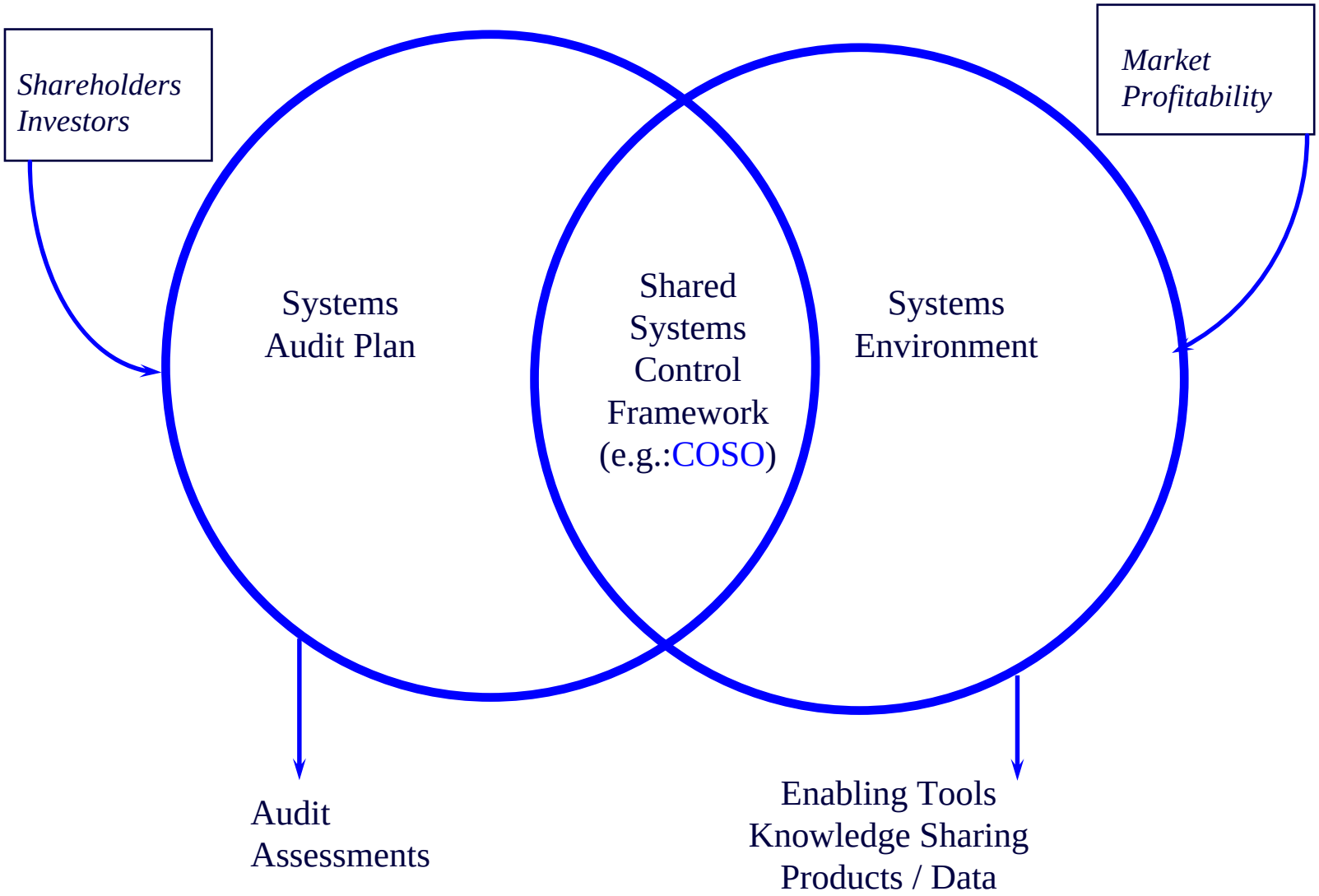
- **Management uses controls to ensure:**
  1. integrity in preparation of financial statements; and
  2. access to assets occurs only with their authorization.

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

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

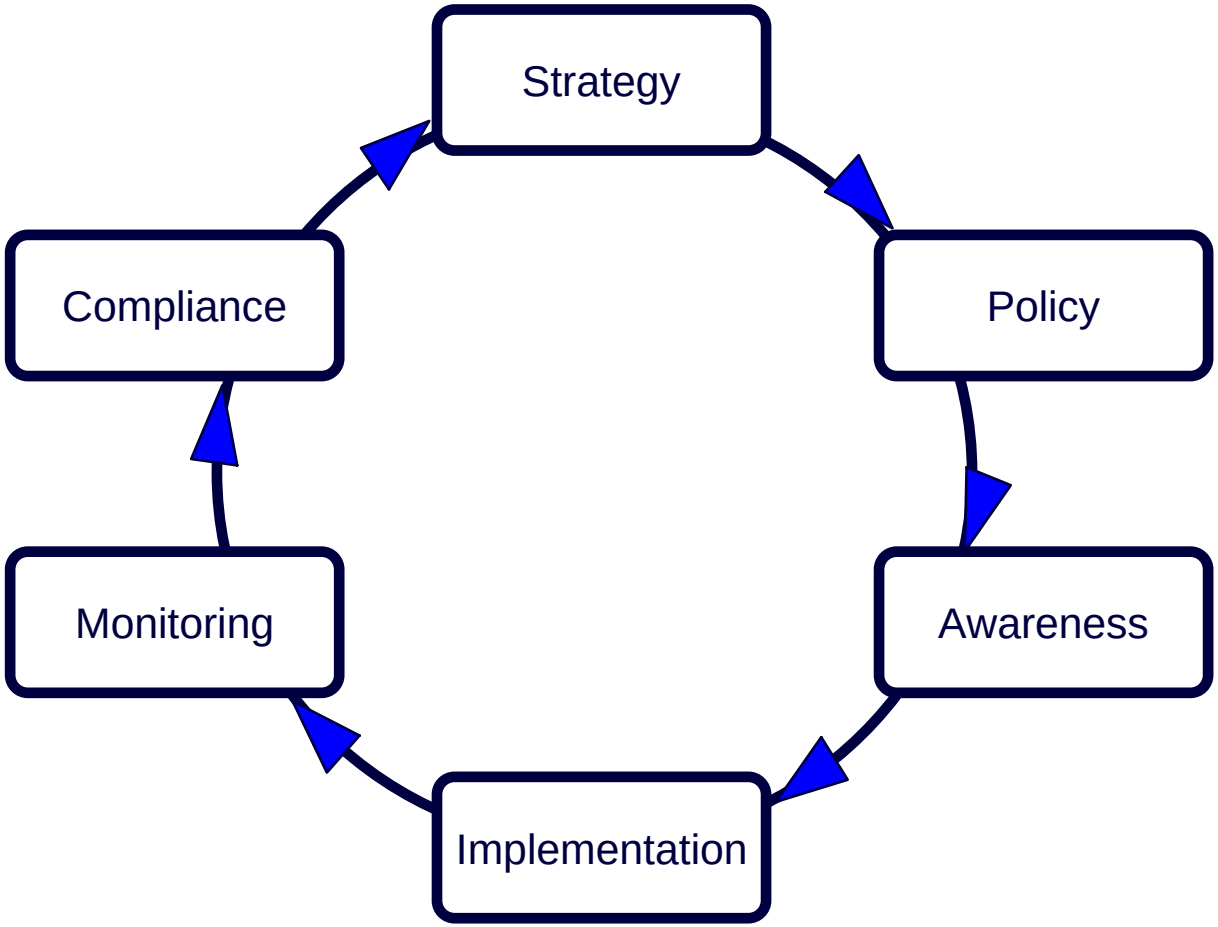
BEAR STEARNS

Example IS Controls Methodology



BEAR STEARNS

Example Shared Control Framework



BEAR STEARNS

Survival Strategy Two:

Identify the audit plan and the auditor's strategy.

(don't compete, just understand the rules of the game)

BEAR STEARNS

The Rules

1. **Review Areas**
2. **Control Objectives**
3. **Audit Steps**

BEAR STEARNS

1. Review Areas

- An information systems audit may include any combination of several specific review areas.
- Different control objectives are generally accepted to apply to each review area.
- Operating system security is generally one review area, however, aspects of information security appear in almost all review areas *(which is why the security personnel usually are the ones charged with escorting the auditors....)*.

1a. Review Area Examples:

Business Recovery
Database Management
Environment and Safety
Expense Control Process
Information Protection
Internet/Intranet
Media Library
Operating Integrity
Operating System Security
Organizational Structure
Physical Security
Policies and Standards
Remote Access
System Development Lifecycle
Telecommunications Controls
User Administration

1b. Review Area Examples (COBIT):

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

BEAR STEARNS

2. 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.**

BEAR STEARNS

2a. Control Objectives Examples:

The plan is to review:	which addresses the:	with respect to these industry standard processes (i.e.COBIT):	that demonstrate these control objectives (e.g.COBIT):
Business Recovery	business contingency	Ensure continuous service.	IT Continuity Framework
	and continuity plans in the		Plan Strategy
	event of a disaster.		Continuity Plan Contents
			Minimizing Requirements
			Maintaining Plan
			Testing Plan
			Plan Training
			Plan Distribution
			User Department Alternative Processing
			Back-up Procedures
			Critical Information Technology Resources
			Back-up Site and Hardware
			Wrap-up Procedures
		Monitor the process.	Collecting Monitoring Data
			Assessing Performance
			Management Reporting

BEAR STEARNS

2b. Control Objectives Examples:

The plan is to review:	which addresses the:	with respect to these industry standard processes (i.e.COBIT):	that demonstrate these control objectives (e.g .COBIT):
Expense Control	project cost accounting	Define a strategic plan.	Consistency with Organization
	systems and cost allocation		Plan Existence
	processes.		Approach and Structure
			IT Long-Range Plan Changes
			Short-Range Planning
			Assessment of Existing Systems
		Define organization/relationships.	Planning Function
			IS Organizational Placement
			Review of Achievements
			Roles and Responsibilities
			Responsibility for QA
			Responsibility for Security
			Ownership and Custodianship
			Data and System Ownership
			Supervision
			Segregation of Duties
			Staffing
			Job Descriptions
			Key IT Personnel
			Contracted Staff Procedures
		Define service levels.	Service Level Agreement Structure
			Performance Procedures
			Monitoring and Reporting
			Review SLAs & Contracts
			Chargeable Items
			Service Improvement Program
		Identify and attribute costs.	Identify Chargeable Items
			Define Costing Procedures
			User Billing and Chargeback
		Manage the investment.	Operating Budget
			Cost and Benefit Monitoring
			Cost and Benefit Justification
		Monitor the process.	Collecting Monitoring Data
			Assessing Performance
			Assessing Customer Satisfaction
			Management Reporting

BEAR STEARNS

2c. Control Objectives Examples:

The plan is to review:	which addresses the:	with respect to these industry standard processes (i.e.COBIT):	that demonstrate these control objectives (e.g. COBIT):
Operating System	security of the file systems	Ensure systems security.	Manage Security Measures
Security	and access privileges		Identification, Auth and Access
	granted by the operating		Security of Online Access to Data
	system.		User Account Management
			Management Account Review
			User Control of User Accounts
			Security Surveillance
			Data Classification
			Central Management
			Security Reporting
			Incident Handling
			Re-Accreditation
			Business Partner Trust
			Transaction Authorization
			Non-Repudiation
			Trusted Path
			Protection of Security Functions
			Cryptographic Key Management
			Malicious Software Controls
			Network Connections
		Manage third party services.	Supplier Interfaces
			Owner Relationships
			Third-Party Contracts
			Third-Party Qualifications
			Outsourcing Contracts
			Continuity of Services
			Security Relationships
			Monitoring
		Monitor the process.	Collecting Monitoring Data
			Assessing Performance
			Assessing Customer Satisfaction
			Management Reporting

BEAR STEARNS

3. 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.**

3a. Audit Step Example:

Control Objective:	Audit Step:	Pass/Fail
Manage Security Measures	Obtain a copy of information system security policy	
	Review how decisions are made with respect to security measures.	
	Review how requirements are formulated with respect to security measures.	
	Determine how security measures are kept up to date with system infrastructure changes.	
	Obtain a copy of information system procedures for user administration.	
	Obtain a copy of information system procedures for operating system security configuration.	
	Determine whether procedures are consistent with policy.	
Identification, Auth and Access	Determine whether user administration procedures are followed.	
	Determine whether users are identified before being granted access.	
	Ensure that password delivery procedures may not be tampered with.	
	Determie how users are classified into groups.	
	Identify each type of system access.	
	Identify authorization authority for each type of system access.	
	List users that have each type of access.	
	Compare user lists to documentation produced by authorization process, verify authorization.	
	Perform full and false inclusion testing on authorization documentation and system user lists.	
	Identify dormant users and review process to eliminate them.	
	Identify…… *you get the idea*	

BEAR STEARNS

Survival Strategy Three:

Coordinate your organization's response the audit process.

(an excellent opportunity for internal team-building :-))

BEAR STEARNS

IS Audit Process

1. **Preliminary Data Gathering**
2. **Opening Meeting**
3. **Fieldwork**
4. **Closing meeting(s)**

BEAR STEARNS

1. 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.

BEAR STEARNS

2. Opening Meeting

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

BEAR STEARNS

3. 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.

BEAR STEARNS

Survival tips for Compensating Controls:

- ⇒ **It is best to prevent undesired events from happening.**
- ⇒ **If you can't prevent, show that you can at least detect.**
- ⇒ **If you can't prevent or detect, show how you will be able to recover.**
- ⇒ **Note: Never identify an independent audit as a monitoring control. The information systems audit itself is not your monitoring or compliance process.**

BEAR STEARNS

4. 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

BEAR STEARNS

Survival Strategy Four:

Use the reporting process to demonstrate your organizational strengths.

(shine! shine! shine!)

BEAR STEARNS

The Final Report

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

BEAR STEARNS

1. 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

BEAR STEARNS

2. 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.

BEAR STEARNS

3. 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.

BEAR STEARNS

Summary of 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.**

BEAR STEARNS