Information Security Metrics

an audit-based approach

Jennifer L. Bayuk

BEAR STEARNS

Overview

- Concepts
- Approach
- Application

BEAR STEARNS

Concept 1

Key to measuring information systems security effectiveness is a clear statement of the objectives of information security controls.

Or, if security effectiveness is to be measured, we must first know what it means to be effective.

BEAR STEARNS

Concept 2

Adept information systems management organizations are able to demonstrate a systems control framework that corresponds to industry standard control objectives.

Or, although the definition of effectiveness must depend on the goals of the organization, IT professionals have clear guidelines in the form of industry standards.

BEAR STEARNS

Concept 3

Security is effective if management has achieved the control objectives that have been decided to be integral to its systems control framework.

Or, as with anything else, a process is effective if it meets its objectives.

BEAR STEARNS

Concept 4

System audit is the process of verifying that management has achieved a designated set of industry standard control objectives.

BEAR STEARNS

Conclusion

A systems control framework that is clearly stated and corresponds to industry standard control objectives is verifiable via system audit.

Or, security effectiveness is measurable.

BEAR STEARNS

Approach

- Industry Standard Control Objectives
- Locally Defined Systems Security Framework
- Audit Steps that cover both

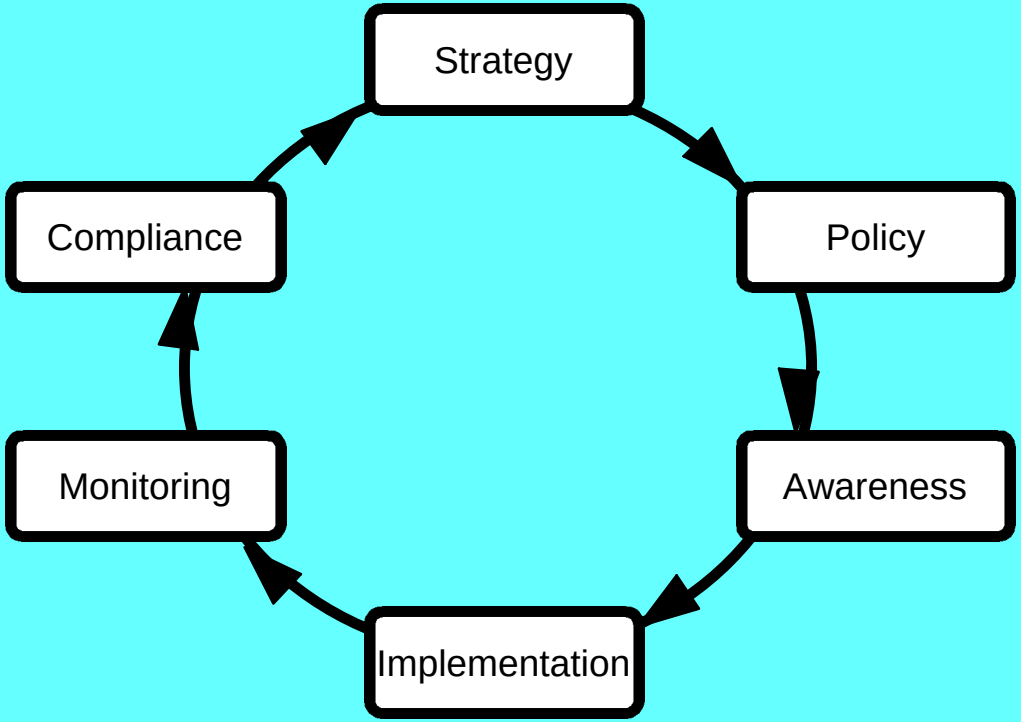
BEAR STEARNS

Industry Standard Control Objectives

- Manage Security Measures
- Identification, Authentication and Access
- Security of Online Access to Data
- User Account Management
- Management Review of User Accounts
- User Control of User Accounts
- Security Surveillance
- Data Classification
- Central Identification and Access Rights Management
- Violation and Security Activity Reports
- Incident Handling
- Firewall Architectures and Connections with Public Networks

BEAR STEARNS

Systems Control Framework



Policy - to dictate organizational standards with respect to information systems security.
Awareness - to provide accountability.
Implementation - to address how policy is to be enforced.
Monitoring - to detect policy violations.
Compliance - to ensure policy violations are corrected.
Strategy - to align information systems security efforts to organizational goals.

BEAR STEARNS

Audit steps - a basis for metrics

Audit steps specify the *actions* that an auditor will take to *independently* gather *evidence* of *activity established by management* that *contributes* to *control objectives*.

Multiple audit steps are usually required to completely cover a given control objective.

BEAR STEARNS

How to use audit steps as a basis for metrics:

- Create audit steps that verify that control objective is met.
- Classify each audit step by framework process.
- Calculate percent of audit steps passed for control objective.
- Calculate percent of audit steps passed for each framework process.
- To account for differences in control objectives across organizations, either:
  - exclude from overall percentages the audit steps that were not attempted.
  - or if the organization's control objectives themselves seem incomplete, then observations and/or recommendations for some new combination of control objectives and processes may replace audit steps not attempted.

BEAR STEARNS

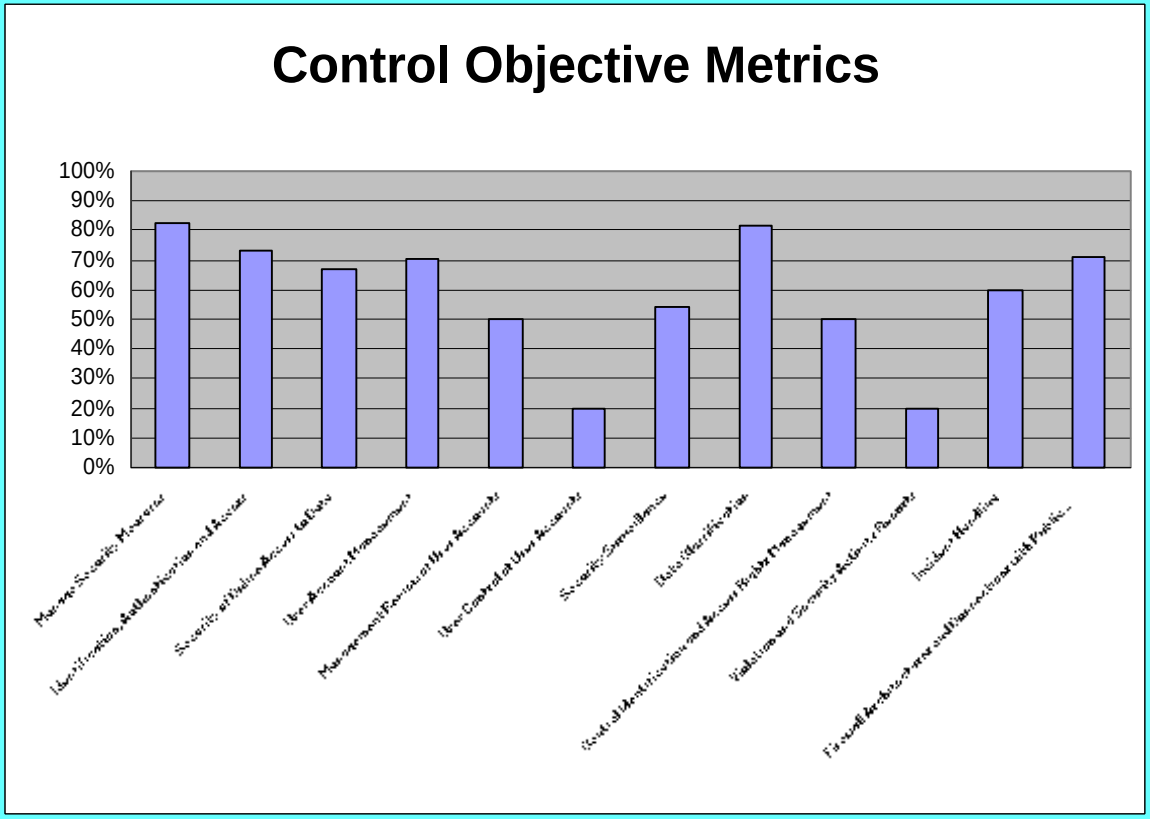
Audit Approach (see paper Appendix A)

	The plan is to test these control objectives:	which are characterized as:	and will be evident through executing the audit steps, which have been tailored to the environment under review:	Pass ? (Y/N)	Framework Component Pass=Y => existing Pass=N => suggested
1.1	Manage Security Measures	Information Technology security should be managed such that security measures are in line with business requirements. This includes: translating risk assessment information to information technology security plans; implementing of the information technology security plan; updating the information technology security plan to reflect changes in the information technology configuration; assessing the impact of change requests on information technology security; monitoring the implementation of the information technology security plan; and aligning information technology security procedures to other policies and procedures.	Obtain a copy of information security policy.	*Y*	*Policy*
1.2			Verify that the security policy production process identifies and addresses IT risks.	*Y*	*Policy*
1.3			Verify that the security policy production process identifies and addresses regulatory requirements.	*Y*	*Policy*
1.4			Verify that the security policy production process identifies and addresses management information needs.	*N*	*Policy*
1.5			Verify that IT requirements with respect to security measures follow policy.	*Y*	*Awareness*
1.6			Verify that security planning is integrated into the IT planning process.	*Y*	*Strategy*
1.7			Verify that the security implementation process identifies and addresses operational considerations.	*Y*	*Implementation*
1.8			Verify that decisions with respect to security mechanisms utilize accurate technology assessments.	*Y*	*Implementation*
1.9			Verify that procedures for access control and user authorization complies with policy.	*Y*	*Implementation*
1.10			Obtain evidence that procedures for access control and user authorization are followed.	*Y*	*Monitoring*
1.11			Verify that there is an IT security plan implemented for each system with the scope of the review.	*Y*	*Implementation*

BEAR STEARNS

Audit Results for Comparision

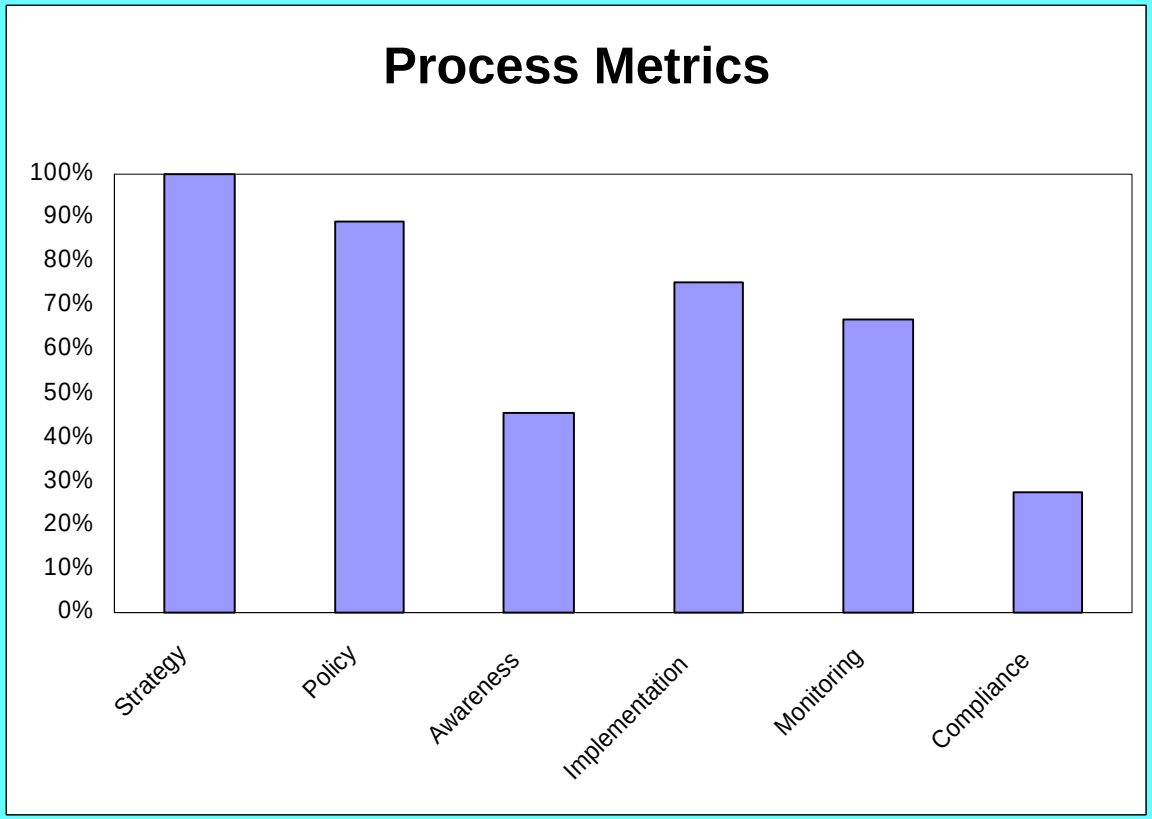
(see paper Appendix B)



BEAR STEARNS

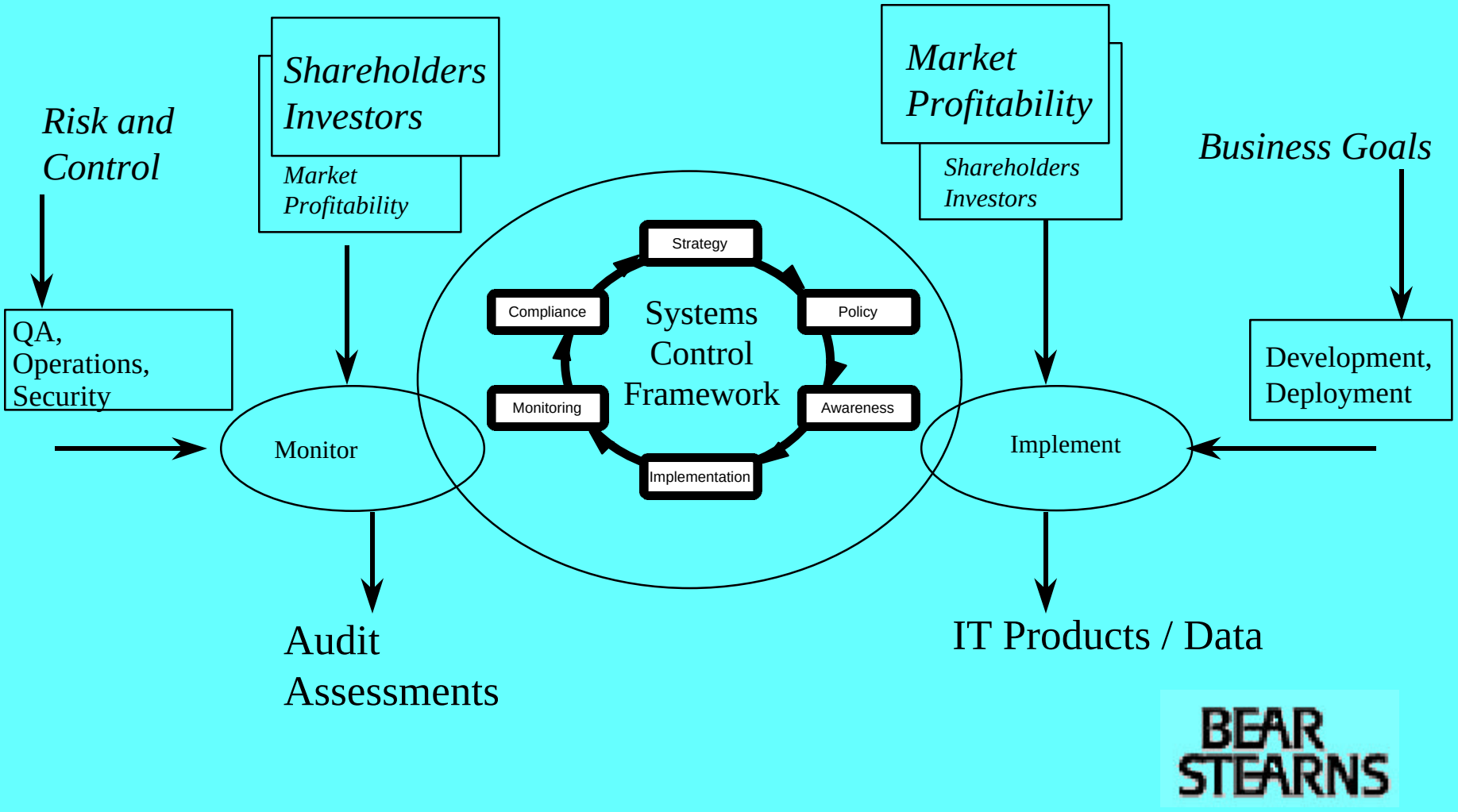
Audit Results for Process Effectiveness

(see paper Appendix C)



BEAR STEARNS

Application: Real World Example



BEAR STEARNS

Real World Review Areas:

Review Area	Business Unit Reviews					Central IS		
	BU1	BU2	BU3	BU4	BU5	US	Global	Systems Overview
Organizational Structure	X	X	X	X	X		X	X
Policies and Standards	X	X	X	X	X		X	X
User Administration	X	X	X	X	X	X	X	X
Operating System Security	X	X	X	X	X	X	X	X
Database Management	X	X	X	X	X			X
Information Protection	X	X	X	X	X	X	X	X
System Development Lifecycle			X		X	X	X	X
Business Recovery	X	X	X	X	X	X	X	X
Operating Integrity	X	X	X	X	X	X	X	X
Remote Access	X	X	X	X	X	X	X	X
Internet/Intranet	X					X		X
Telecommunications Controls	X			X			X	X
Expense Control Process						X	X	X
Environment and Safety	X	X			X		X	X
Physical Security	X	X			X	X	X	X
Media Library	X			X			X	X

BEAR STEARNS

Real World Control Objectives

Overall Objective:	Assess the technology 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
Source:	Committee of Sponsoring Organizations (COSO) Shared Control Framework Information Systems Audit and Control Association (ISACA) Control Objectives for Information Related Technology (COBIT)
Metrics:	30+ audit steps per control objective

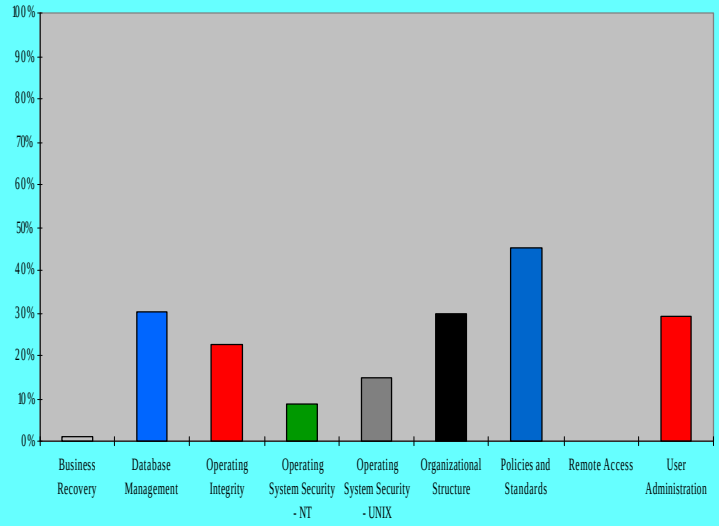
BEAR STEARNS

Real World Basis for Comparison:

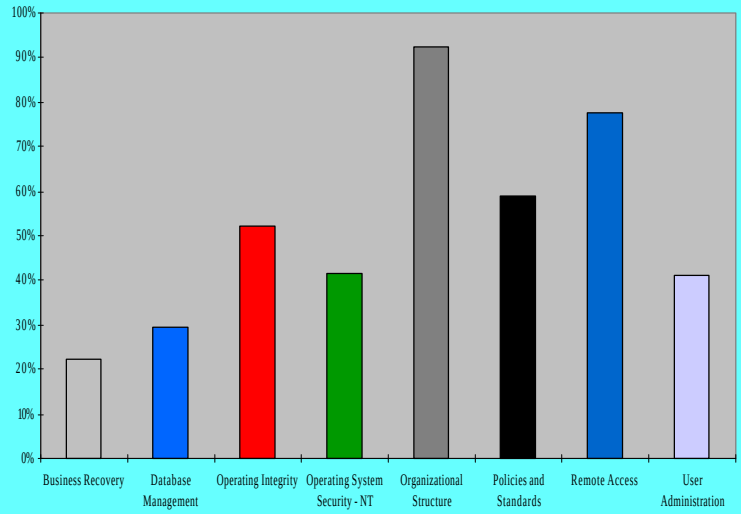
- **CRITICAL - Below 50% in all review areas**
- **SATISFACTORY - Over 75% in 50% of review areas**
- **WATCH - Neither critical nor satisfactory**

BEAR STEARNS

Real World Result Comparison



BUSINESS UNIT 1:
CRITICAL



BUSINESS UNIT 2:
WATCH

BEAR STEARNS

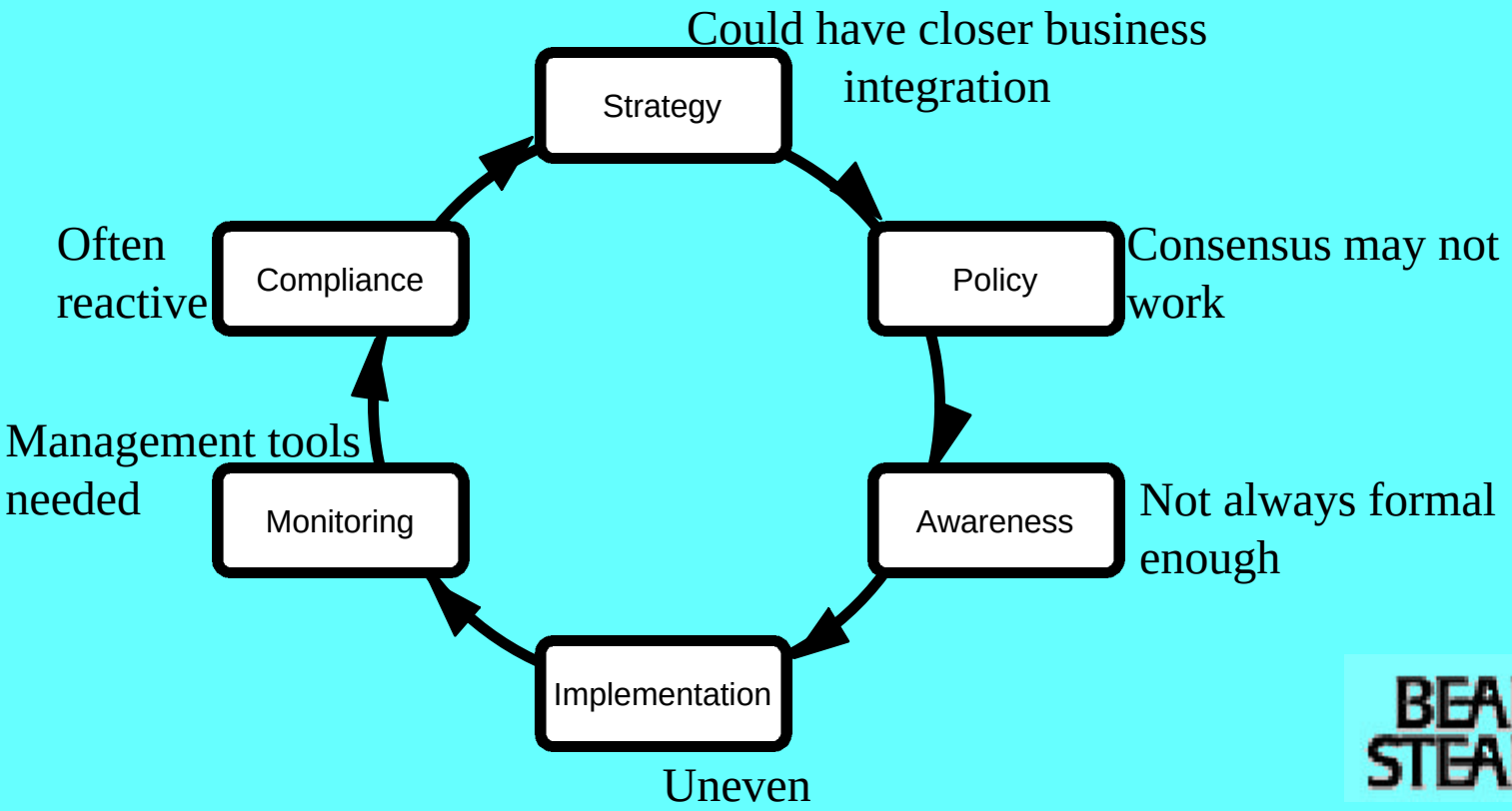
Real World Basis for Recommended Improvements:

Framework	Control Objective	% Pass
Awareness	1. Manage Security Measures	46.12%
	2. Identification, Authentication and Access	43.80%
	3. Security of Online Access to Data	35.50%
	4. User Account Management	47.40%
	5. Management Review of User Accounts	25.00%
	6. User Control of User Accounts	16.70%
	7. Security Surveillance	30.00%
	8. Data Classification	20.00%
	9. Central Identification and Access Rights Management	82.60%
	10. Violation and Security Activity Reports	50.00%
	11. Incident Handling	50.00%
	12. Firewall Architectures and Connections with Public Networks	42.90%
Overall Security Awareness Objectives Met:		**40.84%**

BEAR STEARNS

Potential process level recommendations

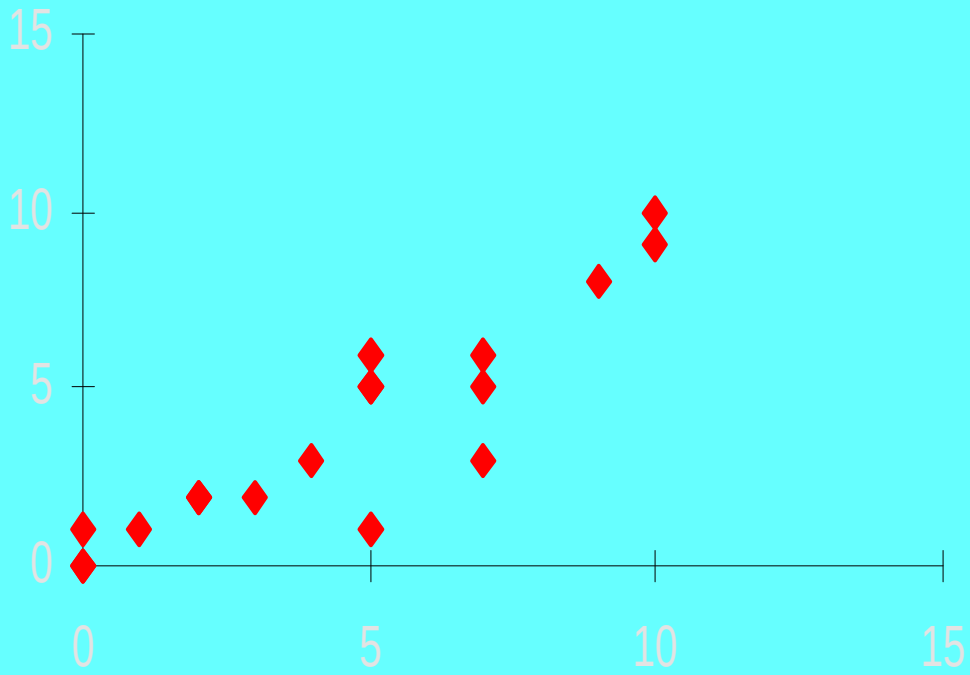
Note: Improvements in process metrics ipso facto improve industry standard metrics!



BEAR STEARNS

Real World Survey

Metrics
Audit Approach
Results



BEAR STEARNS

Real World Feedback

- **"I'm concerned that auditors don't understand technology involved in an audit and spend too much time getting training from my staff: MINIMIZE TAX BURDEN"**
- **"Given deadlines, deliverables on the deployment side, no auditing would bring complacency on the monitoring side"**
- **"It is excellent to see specific control requirements prior to an audit starting."**
- **"Audit is most needed in setting design criteria for new development."**
- **"Expense control should not be part of security audit process."**

BEAR STEARNS

Summary

- Concepts
- Approach
- Application

BEAR STEARNS

jbayuk@bear.com

www.bayuk.com

BEAR STEARNS