Information Security for Managers

Workman, Phelps, Gathegi

Corporate Roles

Corporations are legal entities with Rights and Duties

Recall Citizens United v. Federal Election Commission, 2010

Corporate Roles

CEO *Chief Executive Officer*

Responsible for entire corporation (SOX)

Corporate Roles

CEO *Chief Executive Officer*
Responsible for entire corporation (SOX)

CFO *Chief Financial Officer*
Responsible for financial transactions (SOX)

Corporate Roles

CEO *Chief Executive Officer*
Responsible for entire corporation (SOX)

CFO *Chief Financial Officer*
Responsible for financial transactions (SOX)

CIO *Chief Information Officer*
Entire information infrastructure (IT, operations, support, strategy)

Corporate Roles

CEO *Chief Executive Officer*
Responsible for entire corporation (SOX)

CFO *Chief Financial Officer*
Responsible for financial transactions (SOX)

CIO *Chief Information Officer*
Entire information infrastructure (IT, operations, support, strategy)

CTO *Chief Technology Officer*
≈ CIO but in an IT provider company

Corporate Roles

COS *Chief Security Officer*

Policies, procedures, practices related to information security

Corporate Roles

COS *Chief Security Officer*
Policies, procedures, practices related to information security

CISO *Chief Information Security Officer*
Another name used for COS

Projects Should Use Standards

CMMI Capability Maturity Model Integration
A process and behavioral model that helps organizations streamline process improvement

Projects Should Use Standards

CMMI Capability Maturity Model Integration

A process and behavioral model that helps organizations streamline process improvement

Six Sigma

A method that provides organizations tools to improve the capability of their business processes.

Projects Should Use Standards

CMMI Capability Maturity Model Integration
A process and behavioral model that helps organizations streamline process improvement

Six Sigma
A method that provides organizations tools to improve the capability of their business processes.

COBIT Control Objectives for Info. and Related Technologies
A framework created by ISACA for IT management and governance

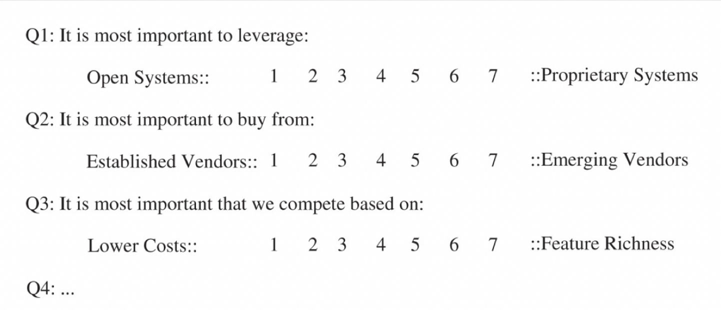
ISACA Information Systems Audit and Control Association

Project Considerations

Projects must consider

- Unfamiliarity
- Uncertainty
- Complexity
- Stakeholder identification and buy-in
- Custom vs. COTS
- In-house vs. Vendor

Prioritizing Competing Stakes



Q1: It is most important to leverage:

Open Systems:: 1 2 3 4 5 6 7 ::Proprietary Systems

Q2: It is most important to buy from:

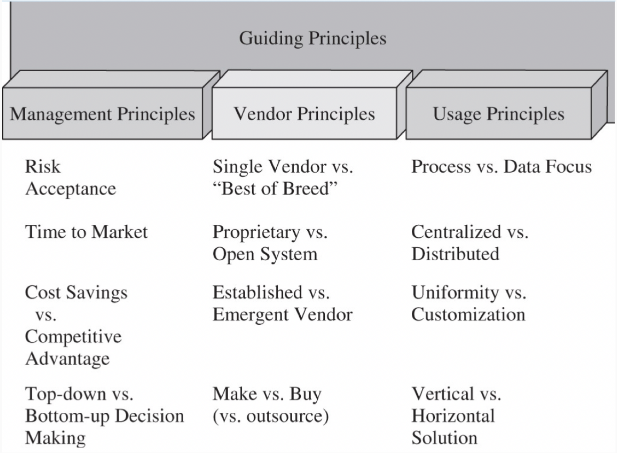
Established Vendors:: 1 2 3 4 5 6 7 ::Emerging Vendors

Q3: It is most important that we compete based on:

Lower Costs:: 1 2 3 4 5 6 7 ::Feature Richness

Q4: ...

Prioritizing Competing Stakes



Guiding Principles

Management Principles	Vendor Principles	Usage Principles
Risk Acceptance	Single Vendor vs. “Best of Breed”	Process vs. Data Focus
Time to Market	Proprietary vs. Open System	Centralized vs. Distributed
Cost Savings vs. Competitive Advantage	Established vs. Emergent Vendor	Uniformity vs. Customization
Top-down vs. Bottom-up Decision Making	Make vs. Buy (vs. outsource)	Vertical vs. Horizontal Solution

Effect of Organizational Structure

Identify who has *power*

- Positional power
- Expert power
- Referent power (charisma)

The project needs a *Champion* to navigate the power structure

Policies

Policies . . .

- Must be enforceable and enforced
- Not too specific yet not too general
- Should no devolve into procedures (no step-by-step)
- Can be codified as policies
- can be codified in software (timed password changes)
- Should cover automated systems
- Should cover behaviors (people are the “weakest link”)