The San Francisco Chapter of ISACA proudly presents...
SF ISACA 2007 Fall Conference
IT Audit
Information Security
IT Governance
Risk Management
Compliance

Operationalizing Security and Compliance: Generating Maximum Compliance ROI

Mark Seward
Director of Marketing, QualysGuard

Qualys, Inc.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

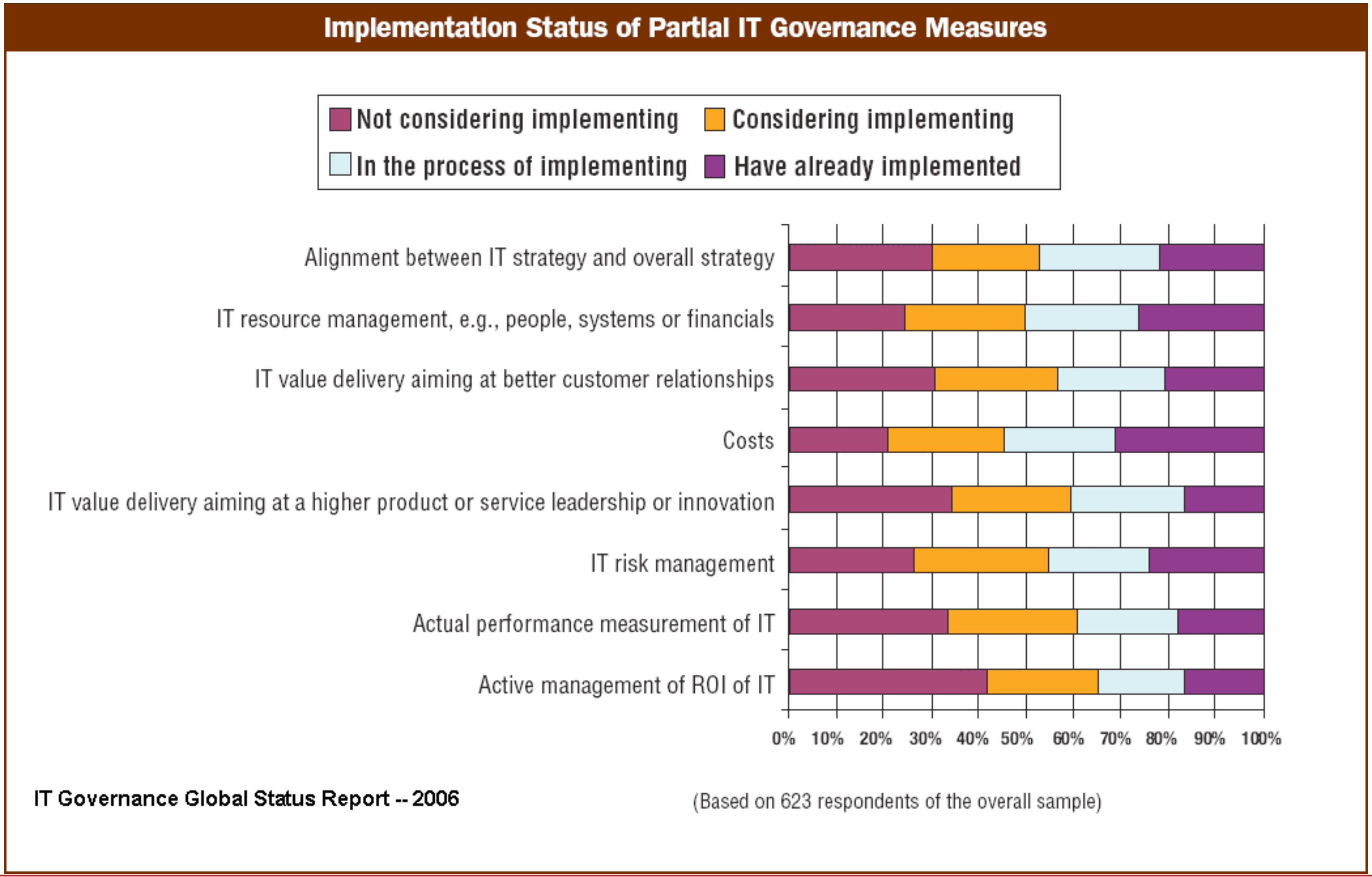
- Where is GRC today
- What drives the business and why do we care
- Review – “What’s a process”
- Primary business actors involved with compliance
- Team-function centric approach
- The needs assessment
- “Just-in-time” information
- Summary

Process approach to GRC

- "…many business experts believe that the concept of a **cross-functional** convergence of these activities (Governance, Risk and Compliance) represents a progressive approach in this area, and is quickly replacing the traditional fragmented or silo mentality.

- *January 23:Operational Risk - Part 1 - The Corporate Defense Continuum, Governance, Risk and Compliance, Sean Lyons, 1/23/2007 on-line at: http://www.garp.com/risknews/newsfeed.asp?Category=6&MyFile=2007-01-23-14131.html*

IT Governance and Business Alignment



Implementation Status of Partial IT Governance Measures

IT Governance Global Status Report -- 2006

(Based on 623 respondents of the overall sample)

A Reminder -- What drives the business?

- Revenue – Customer Attrition / Retention
- Profitability – Lower Costs
- Asset Protection – Security
- Workforce Performance -- Efficiency
- Reputation – Brand Protection
- Risk Reduction – Implied Goal

Can everyone in the IT organization name these?
Does everyone in IT know what they mean?
Can you say "corporate culture?"

Governance Risk and Compliance (GRC) “as-is” assessment

- Governance Risk and Compliance (GRC) as a response to regulation
  - Implementing a series of fragmented, tactical, one-off projects
  - usually manual efforts
  - duplicated activities
  - high costs
  - wasted time and resources
  - limited GRC effectiveness.
- Need to be able to document and monitor business processes that cross multiple enterprise divisions and regions, span entire process chains, and are supported by multiple, disconnected IT applications.

Business Process Defined

- By definition:
  - A business process is any sequence of structured or semi-structured tasks performed in series or in parallel by two or more individuals to reach a common goal.

Business Process Examples

- Departmental Processes (functional silo)
- Hiring is a process – mostly in HR
- Vulnerability Management is a process – assigned to IT
- Sales processes – acquiring new customers

- Business Objective Processes (aligns business drivers across department silos)
- ‘Quote to Cash’ – sales, finance, IT
- ‘Order to Ship’ – sales, finance, shipping, IT
- ‘Dock to factory floor’ – Ford Motor Company
- Governance Risk and Compliance (GRC) – IT, HR, finance, board of directors

Department actors on a cross-functional compliance process stage

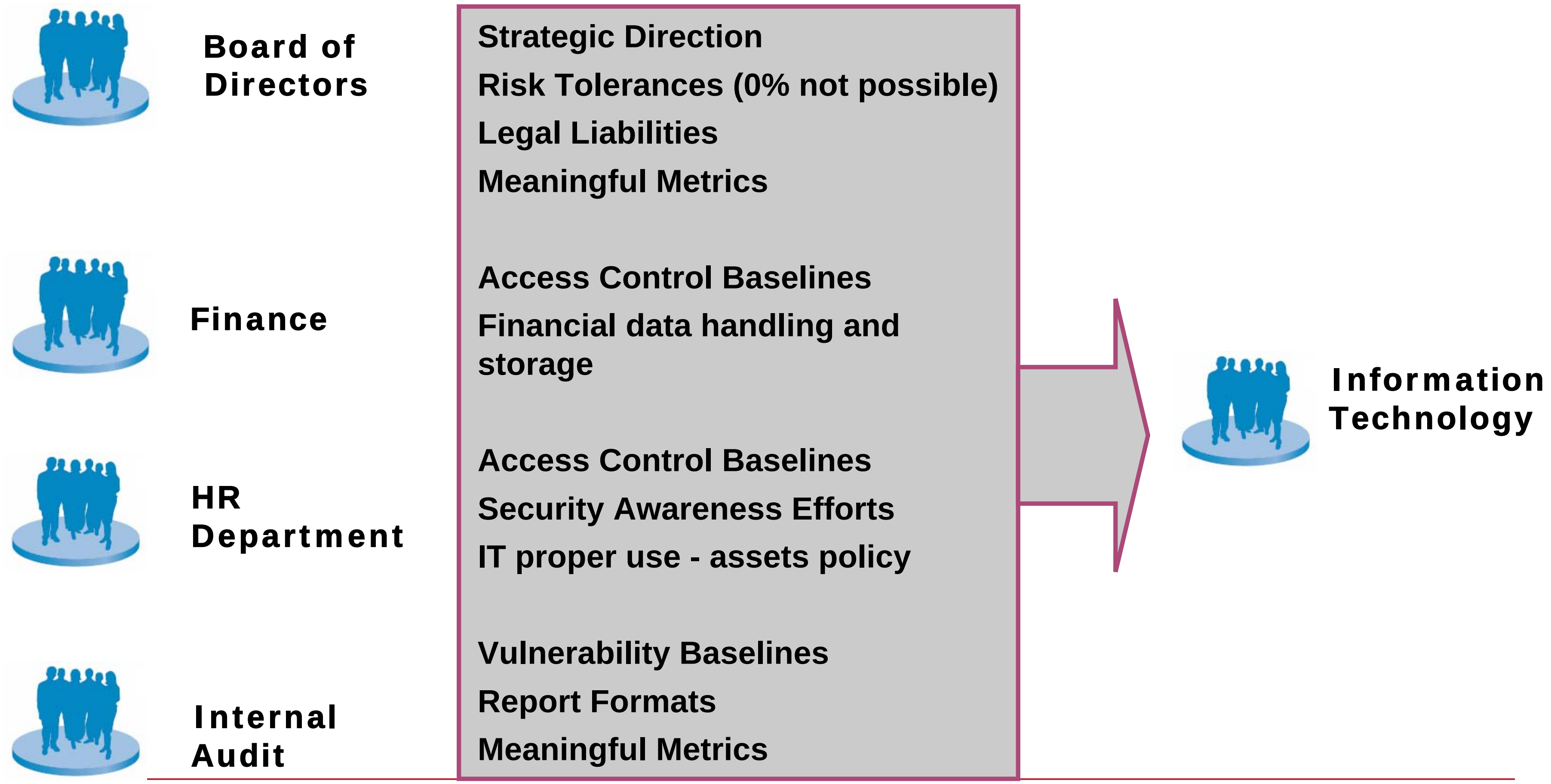
- HR
  - Issues desktop/laptop “proper use” documentation
  - Involved in termination processes
  - Employee record retention
  - May be involved in security awareness and/or privacy programs
- Finance
  - Asset tracking for the enterprise
  - Financial data handling and storage
- Board of Directors
  - Overall responsibilities for organizational risk, governmental compliance, and audit oversight

IT Department actors on the compliance process stage (cont.)

- IT Operations, Security, Audit
  - IT operations
    - Break fix activities
    - Deployment and system maintenance
    - Change management / approvals
    - Data retention and redundancy
    - May be involved in security awareness programs
  - IT security
    - Security incident management (reactive)
    - Determines systems vulnerabilities (proactive)
    - May maintain platform and application security baseline documentation
  - IT internal audit
    - Assesses systems for compliance with standards
    - Audits current processes for compliances

Needs Assessment – What Does IT Need?

Stakeholders **IT Information Requirements**



Board of Directors

- Strategic Direction
- Risk Tolerances (0% not possible)
- Legal Liabilities
- Meaningful Metrics

Finance

- Access Control Baselines
- Financial data handling and storage

HR Department

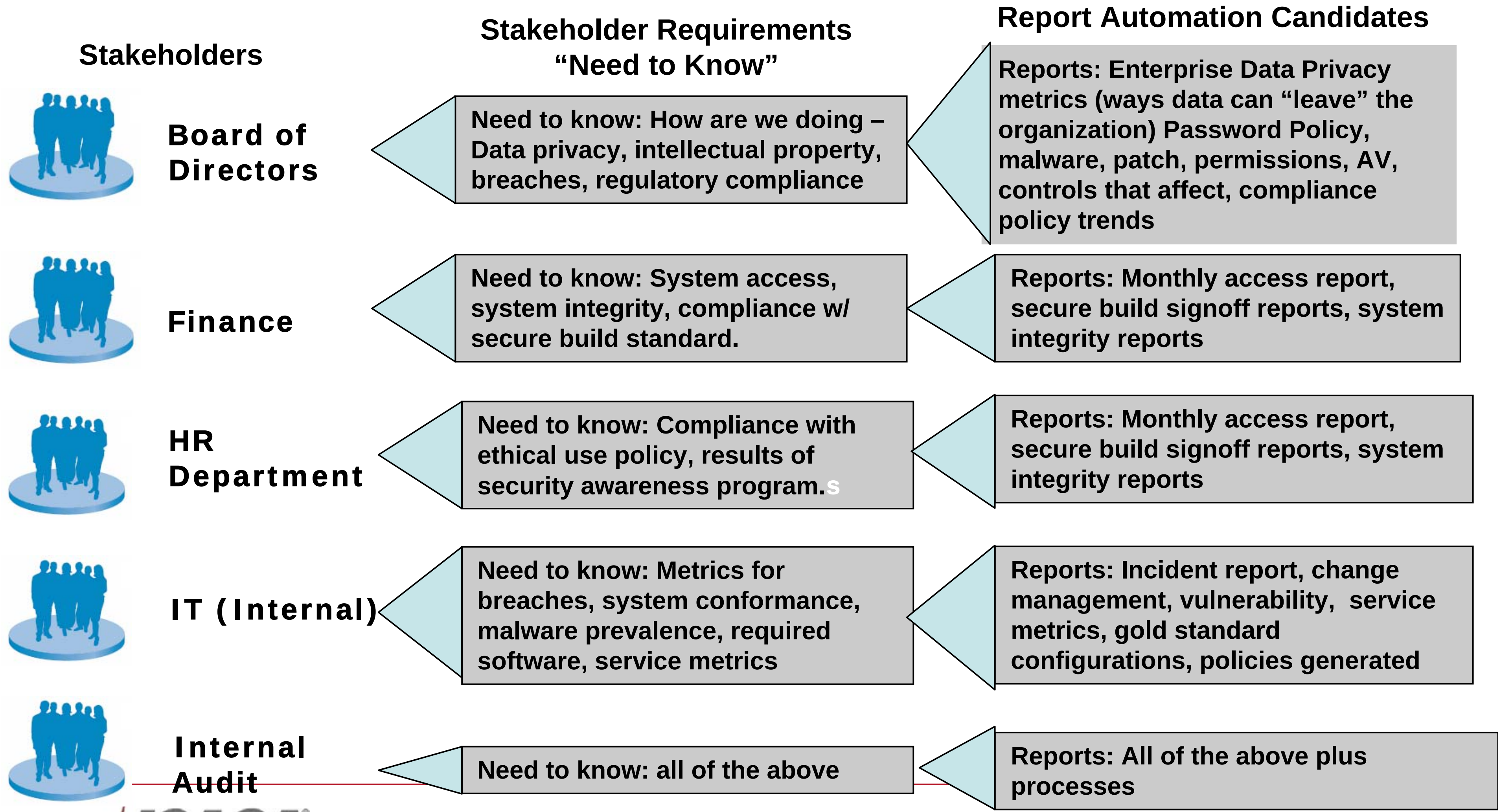
- Access Control Baselines
- Security Awareness Efforts
- IT proper use - assets policy

Internal Audit

- Vulnerability Baselines
- Report Formats
- Meaningful Metrics

Information Technology

Needs Assessment – What do Stakeholders Need?



Stakeholders	Stakeholder Requirements “Need to Know”	Report Automation Candidates
Board of Directors	Need to know: How are we doing – Data privacy, intellectual property, breaches, regulatory compliance	Reports: Enterprise Data Privacy metrics (ways data can “leave” the organization) Password Policy, malware, patch, permissions, AV, controls that affect, compliance policy trends
Finance	Need to know: System access, system integrity, compliance w/ secure build standard.	Reports: Monthly access report, secure build signoff reports, system integrity reports
HR Department	Need to know: Compliance with ethical use policy, results of security awareness program.s	Reports: Monthly access report, secure build signoff reports, system integrity reports
IT (Internal)	Need to know: Metrics for breaches, system conformance, malware prevalence, required software, service metrics	Reports: Incident report, change management, vulnerability, service metrics, gold standard configurations, policies generated
Internal Audit	Need to know: all of the above	Reports: All of the above plus processes

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

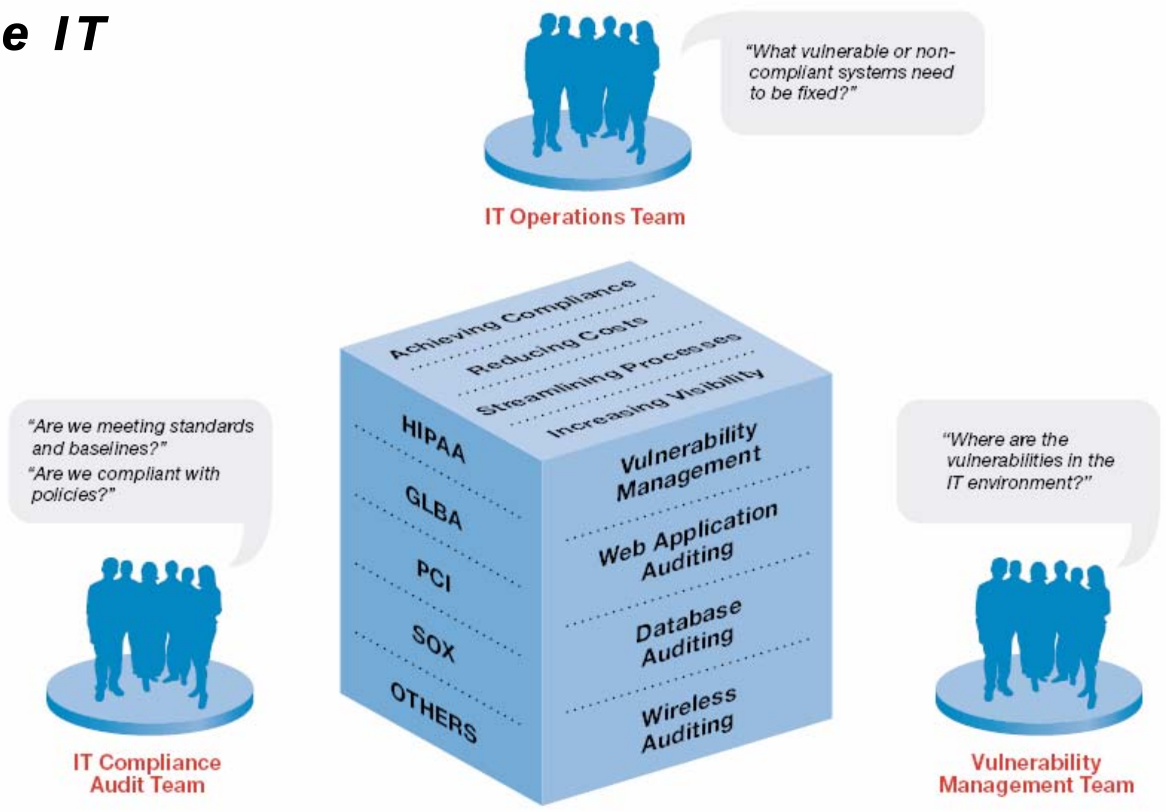
When do they need it?

- **Needs assessment complete**
  - What information needs to be delivered when?
  - Time your “hooks” into other business processes?
  - Does the information become “stale” if delivered too early?
  - What are the repercussions (risks to other parts of the business) of being “late?”
  - “Just-in-time” for information delivery
    - Automate where possible
      - Report Availability Notifications
      - Distribution of reports

A View of the IT Department

Pervasive IT Silos

Multiple IT Projects



The need for a single data set

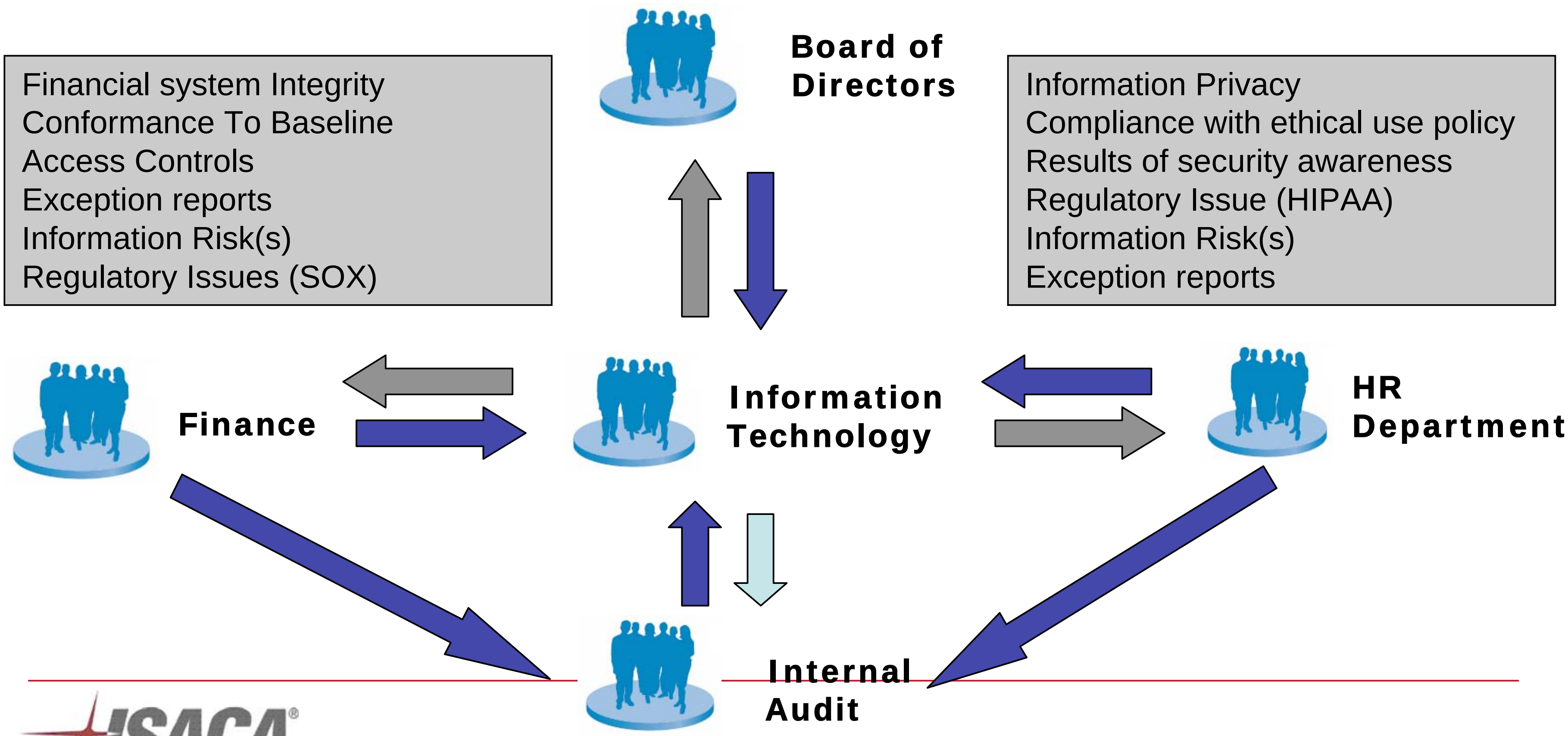
Examine internal requirements through the needs assessment process

Automation Brings Cost Savings for GRC

- Simplified business process design, workflow modeling, can cut the time spent by IT staff on deployment and administration.
- Automation allows individuals to work more efficiently and take on new tasks.
- Automating a task that requires five hours of manual intervention, reduces this time by half and will yield a significant cost savings
- Building and making changes to any business process, even minor ones, is extremely labor-intensive. A workflow designer that is icon-driven makes process building a simple drag-and-drop process. What's more, the ability to edit on the fly makes you much more efficient and effective.

Alignment with Business Drivers

Revenue / Customer Attrition & Retention
Profitability / Lower Costs
Asset and Data Protection and Security
Risk Tolerance and Reduction
Workforce Performance / Efficiency
Reputation and Brand Protection



Financial system Integrity
Conformance To Baseline
Access Controls
Exception reports
Information Risk(s)
Regulatory Issues (SOX)

Information Privacy
Compliance with ethical use policy
Results of security awareness
Regulatory Issue (HIPAA)
Information Risk(s)
Exception reports

Summary

- Moving to an integrated process for GRC requires
  - Knowing the Business Drivers
  - Understanding how other departments align with the key business drivers
  - Undertaking a needs assessment across departments
    - Two way – What are IT's needs and what are the departmental needs
  - Just-in-time delivery of required information
  - Where possible move to a single data set as the basis for reports
  - Standardized reporting formats across departments
  - Break down IT interdepartmental silos
  - GRC efforts should be subsumed into other departmental processes
- An aligned GRC process drives business objectives and provides ROI for compliance processes

Questions?