protiviti[SM]
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Sarbanes Oxley: Year Two and Beyond-

What it Means for Information Technology

ISACA Luncheon **Houston, TX**

January 20, 2005

John Harrison

protiviti
Independent Risk Consulting

We Begin with a Premise….

No one wants to remain in a "mindless project" mode after Year 1 of Section 404 compliance

Therefore, companies must transition to an ongoing process for Year 2 and beyond

The question is…How do they do that?

protiviti
Independent Risk Consulting

Agenda

Before we talk about moving beyond Year 1…

Set the stage with a few observations about the current landscape and lessons learned

Once we set the stage…

Discuss alternative strategies for complying with SOA in the future

We will then discuss some IT specific Issues…

What are the impacts on the IT department and its operations going forward with regulatory compliance as the drivers?

SOA and other regulatory compliance will impact all (or almost all) significant IT initiates from now on.

How do I continue to comply with Sarbanes-Oxley Act (SOA) in 2005 and beyond ……

and start to create value from all of this effort?

protiviti
Independent Risk Consulting

Two Realities After the Initial 404 Assessment is Complete…

REALITY #1

Process owners have a business (an IT process) to run and may be unable or may lack the skills to carry the entire compliance load

IMPLICATION: Certifying officers need an appropriate structure to provide them confidence that what is supposed to be done is being done and to demonstrate the appropriate level of due care

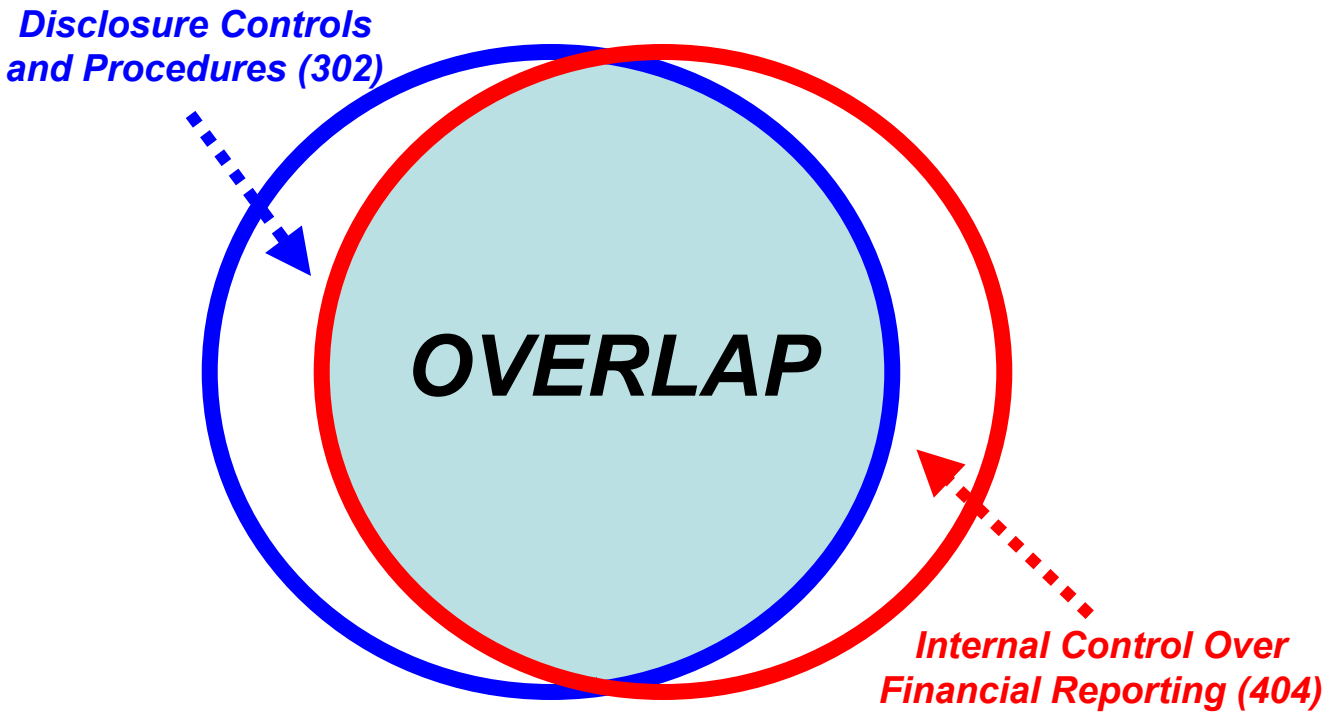
REALITY #2

The IT Department is integral to the overall internal controls evaluations for 404 and 302 and a plethora of other regulatory compliance requirements:

IMPLICATION: The IT processes will continue to come under scrutiny and that changes and improvements will continue to be critical to ongoing compliance

Going forward, think of 302 and 404 as a SINGLE requirement requiring continuous reporting

Your 302 executive certification is going to change after the first internal control report is issued



protiviti
Independent Risk Consulting

Year One Lessons Learned-IT Control Issues

Focus on these areas going forward and develop plans considering continued regulatory compliance:

The following processes are critical to the 404 compliance efforts- finally there's agreement:

- Change Management for applications, infrastructure and new systems (SDLC)
- Security Administration (access controls)
- Computer Operations- data management, back-up and recovery, problem management, job scheduling, etc.
- 3rd Party Outsourcing Issues and Challenges
- End User Computing- spreadsheets and other non-IT Department computing

protiviti
Independent Risk Consulting

Year One Lessons Learned-IT Control Issues(cont.)

Year 1 lessons should influence IT department planning and projects for the next several years, at least:

- Critical financial applications have been identified, documented and evaluated
- There are numerous IT processes which support these applications
  - But many were not standardized
  - And many had not retained evidence for control evaluation
- Fixes for this year have been “spot fixes” and “Band-Aids”
- Numerous IT initiatives have been put on hold for this year to get by SOA

What are the compliance alternatives for 2005 and beyond?????

protiviti
Independent Risk Consulting

In ALL Alternative Compliance Structures…

What are the implications related to how compliance should be addressed going forward?

- Process owners are ultimately responsible and should be held accountable
- Process owners:
  - Decide and design the controls
  - Supervise, monitor, test and assess, as well as sometimes execute, the controls
  - Document and self-assess controls
  - Remediate control deficiencies
- The continuing shift in ownership will require plenty of training, coaching, and monitoring
- The message – ***The issue is not whether to hold process owners accountable, but how***

protiviti
Independent Risk Consulting

In ALL Alternative Compliance Structures…

Going Forward Without Project Management Discipline is Not a Good Idea!

- A Project Management Office (or an equivalent function) should be considered to stay on top of the effort
- There will continue to be multiple tests by multiple people of multiple controls within multiple processes across multiple units and locations in multiple geographies
- There will also likely be changes requiring remediation that will need to get done
- As new IT applications and changes are implemented SOA considerations are integral to the project and need to be included in the SDLC process and steps
- The message – ***Monitoring "teeth" are needed, or else it's just "hope and pray" it gets done***

protiviti
Independent Risk Consulting

In ALL Alternative Compliance Structures…

Companies must evolve to a model that allows for Sustained Compliance!

- IT management should look for ways to standardize and consolidate processes to the extent possible
- Careful analysis and planning in the early stages can refine the number of primary/key/critical technology controls, as well as the extent of testing for each
- Time consuming manual controls should evolve to more preventive and automated controls
- Controls may be enhanced to go beyond compliance into actually improving business performance
- The message – ***Year 1 got you to the finish line; Year 2 is about investing in long-term efficiencies and quality so that… Year 3 can demonstrate cost-effective Sustained Compliance.***

protiviti
Independent Risk Consulting

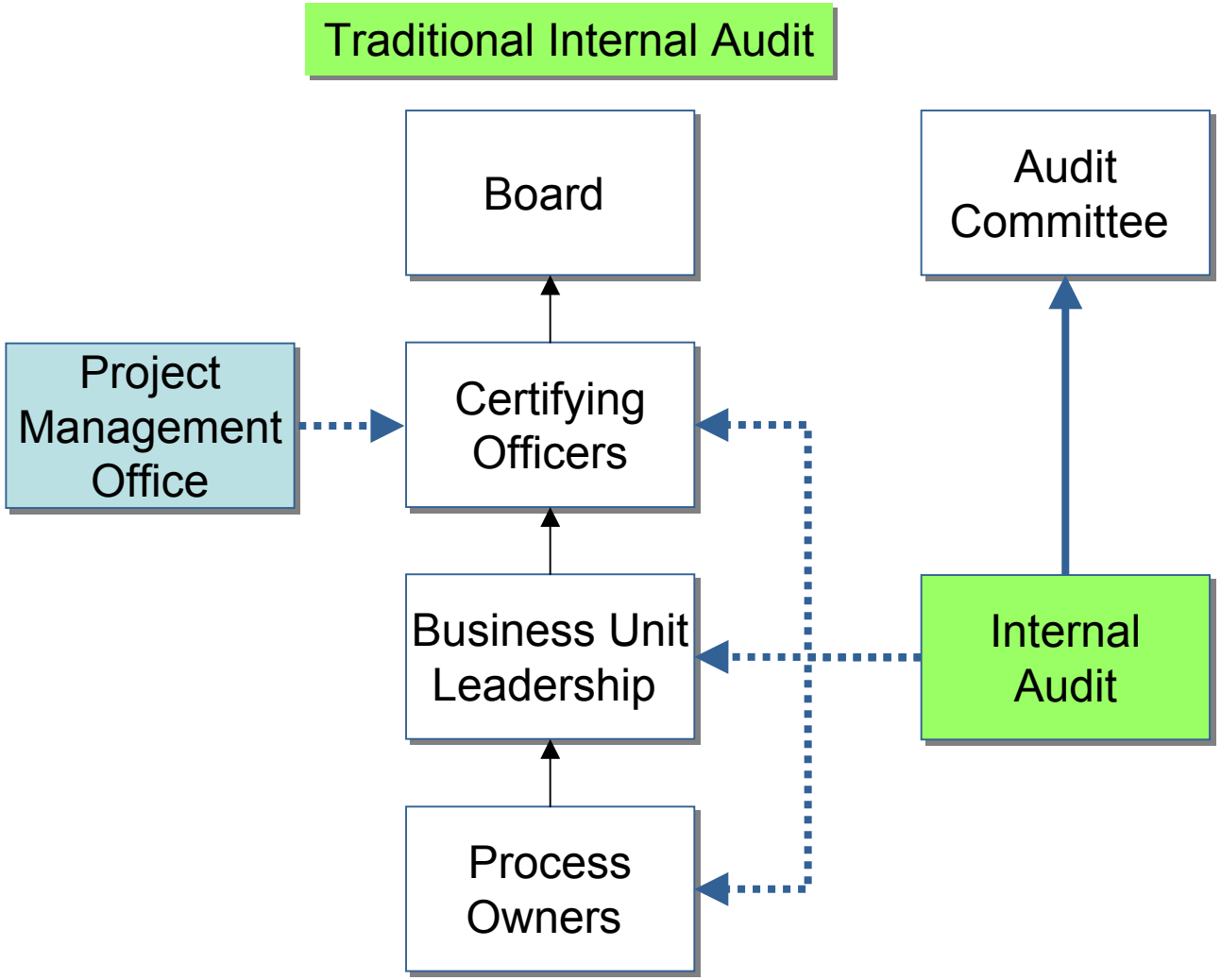
Alternative SOA Compliance Structures

What happens:

- IA tests controls
- IA consults on control environment whenever possible

Advantages:

- IA focuses on financial reporting controls
- Represents the least amount of internal change from a historical perspective (assuming a competent internal audit function)



protiviti
Independent Risk Consulting

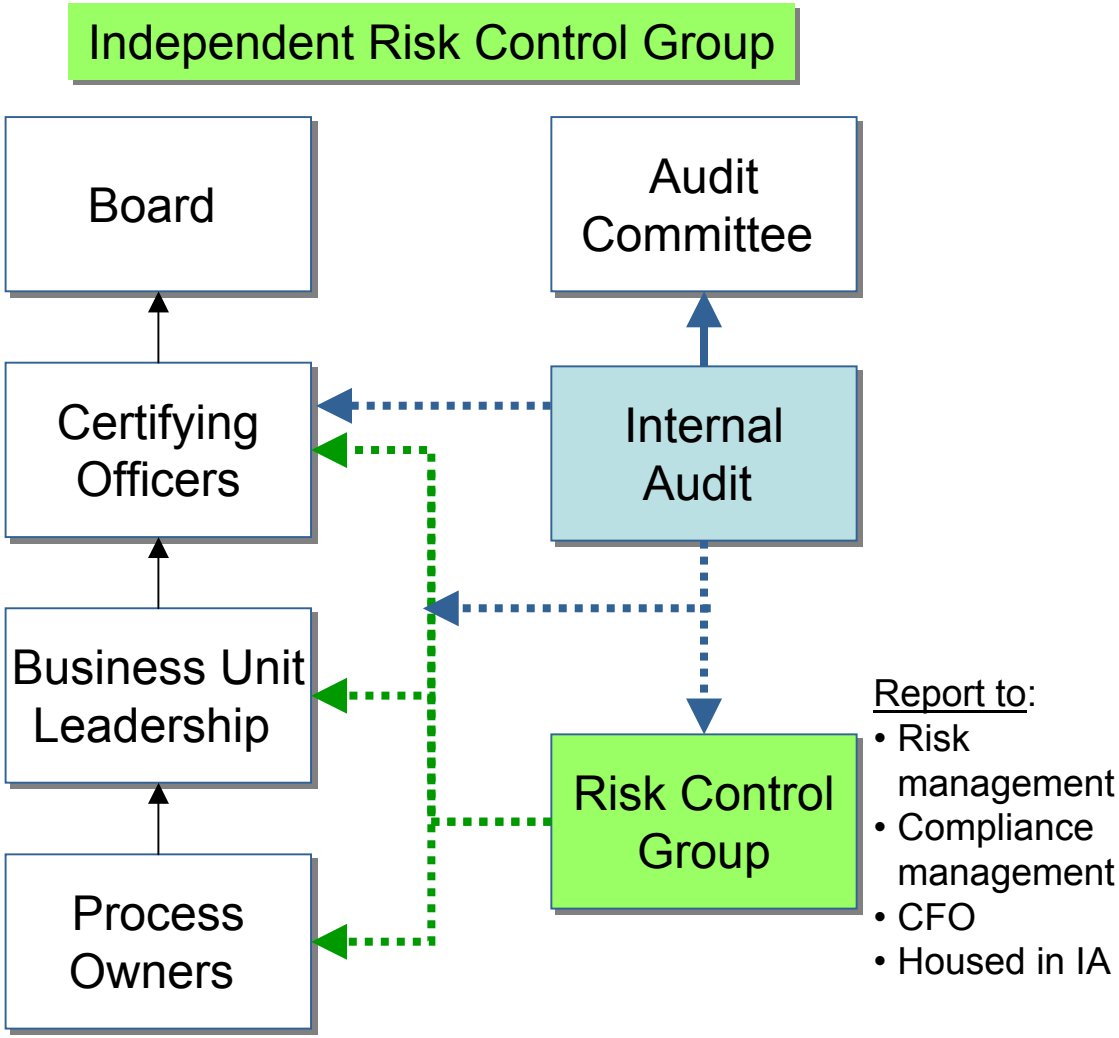
Alternative SOA Compliance Structures

What happens:

- Risk control group:
  - Coaches process owners
  - Assists with remediation
  - Tests controls
  - May exist with or without an IA function
- IA independently assesses management's compliance process

Advantages:

- Maximize appearance of IA objectivity to increase external auditor reliance
- Consolidated team of risk specialists promotes consistency of control structure



protiviti
Independent Risk Consulting

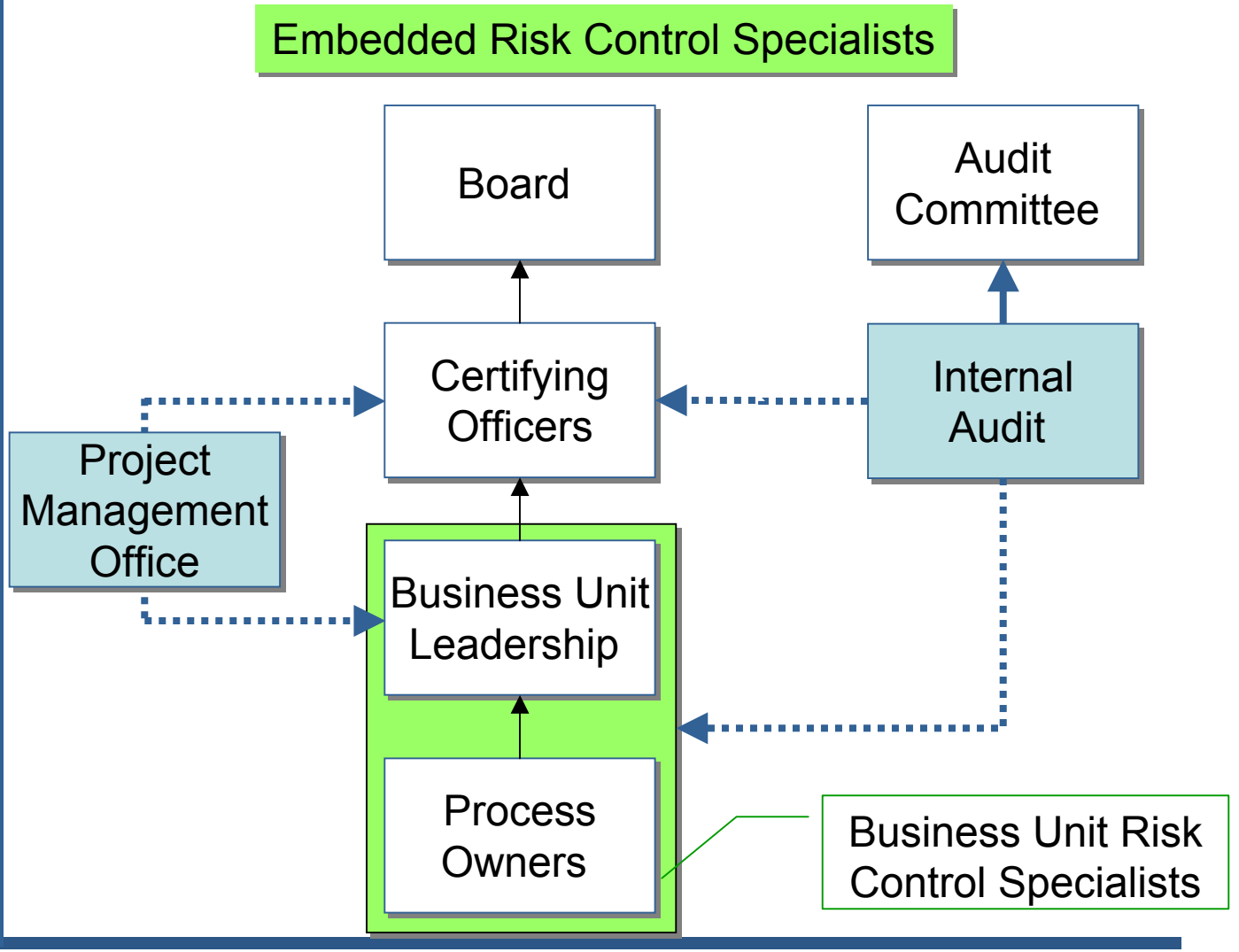
Alternative SOA Compliance Structures

What happens:

- Risk control specialists:
  - Are embedded within business units
  - Work directly with process owners on control environment
  - Perform testing
- IA independently assesses management's compliance process

Advantages:

- Process owners supported close to the source
- Maximize appearance of IA objectivity



Clarifying roles & responsibilities and reinforcing accountability

- Traditional Internal Audit
- Independent Risk Control Group
- Embedded Risk Control Specialists

What are the constraints in deploying process owners and / or internal audit?

What are their capabilities?

What is their capacity?

What infrastructure needs to be in place to support this effort?

What is the cost?

Some Questions to Think About

Clarifying roles & responsibilities and reinforcing accountability

- Traditional Internal Audit
- Independent Risk Control Group
- Embedded Risk Control Specialists

Are risk control specialists needed to assist process owners with testing and other activities?

If so, where should they be positioned within the organization?

How do you staff and measure performance?

What does Year 2 specifically mean for Information Technology?

protiviti
Independent Risk Consulting

Regulatory and Governmental Compliance Issues

Sarbanes Oxley is not the only regulation that IT departments need to understand, plan for and comply with

- Sarbanes Oxley Act
- Health Information Portability and Accountability Act (HIPAA)
- Patriot Act
- Anti-Money Laundering
- FFIEC, FERC, others
- New York and other Stock Exchange Listing Requirements
- Other industry related standards

protiviti
Independent Risk Consulting

Regulatory Compliance Drivers

The common denominators to Regulatory Compliance

- Key risks are mitigated-
- Said another way- key processes are well controlled

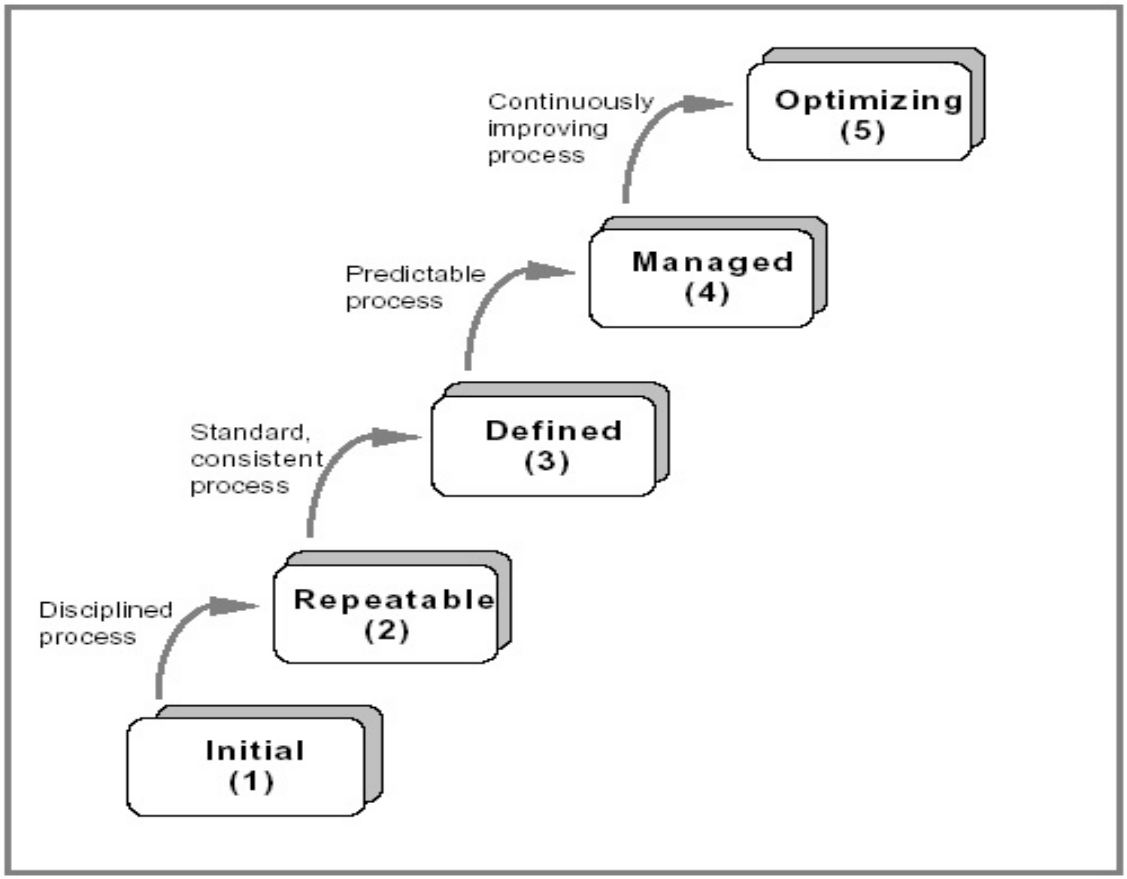
Best way to ensure compliance is through well controlled and documented processes that are understood and operated consistently on a day to day basis-

What is a workable approach to ensure this?

protiviti
Independent Risk Consulting

How to measure a process

The SEI Capability Maturity Model concept can be used to measure, manage and monitor your IT processes



Source: SEI Capability Maturity Model Integration (CMMI)

protiviti
Independent Risk Consulting

Characteristics of Maturity Levels

"To improve the level of maturity requires continuous improvement, based on small, ever-improving steps. As the organization gradually improves, they slowly improve their overall performance. It is not productive to skip a level because each level represents a foundation to the next."

Level 1 – Initial-

Characterized by an **ad-hoc, chaotic environment**. Few process are defined.

Level 2 – Repeatable-

Basic processes are in place, and discipline is in place to repeat earlier successes.

Level 3 – Defined-

Processes are **defined, documented and standardized** throughout the organization. All projects adhere to these standards.

Level 4 – Managed-

Detailed **measures** of processes are **collected**.

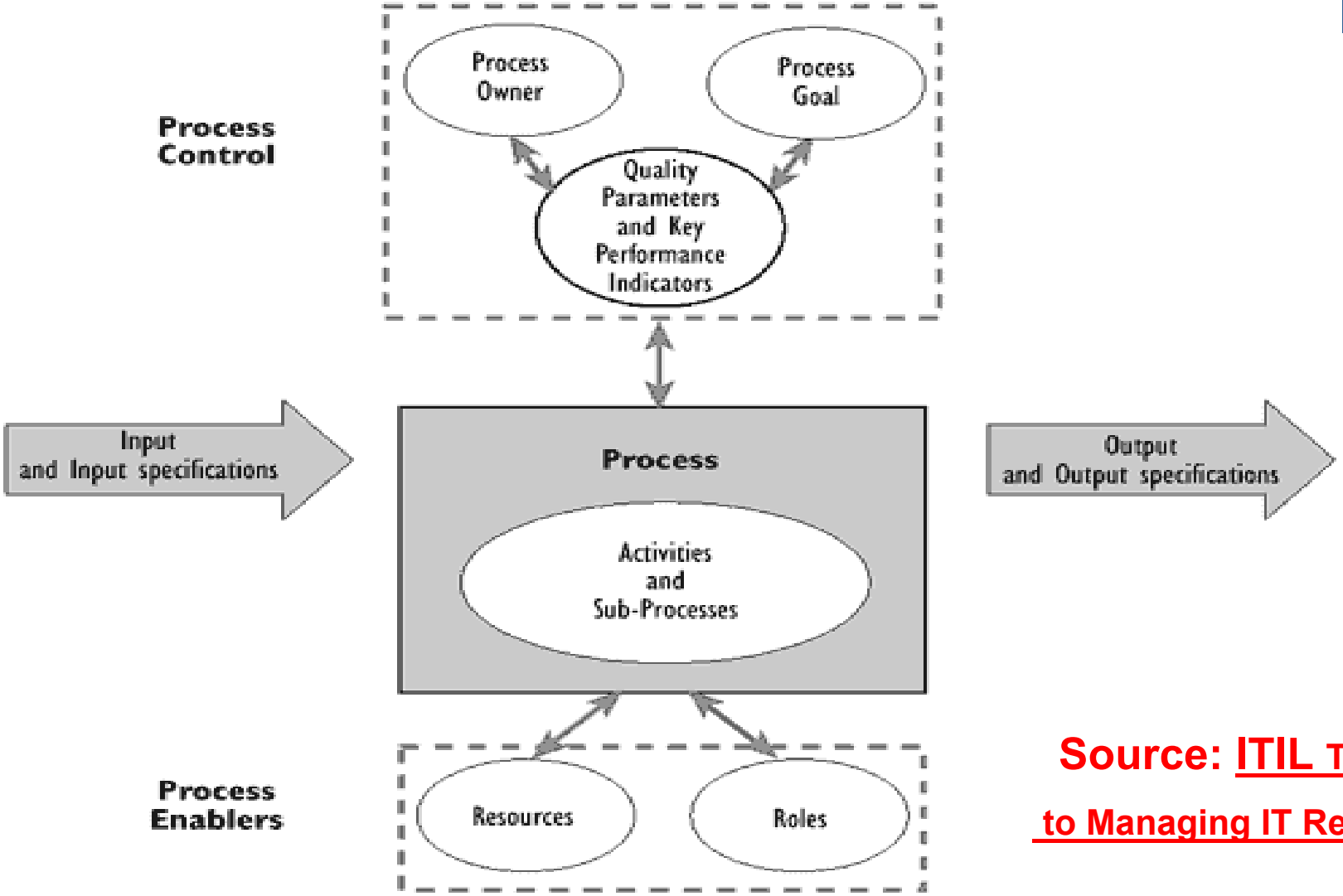
Level 5 – Optimizing-

Continuous process improvement from feedback and from piloting new ideas and technologies

Source: SEI Capability Maturity Model Integration (CMMI)

protiviti
Independent Risk Consulting

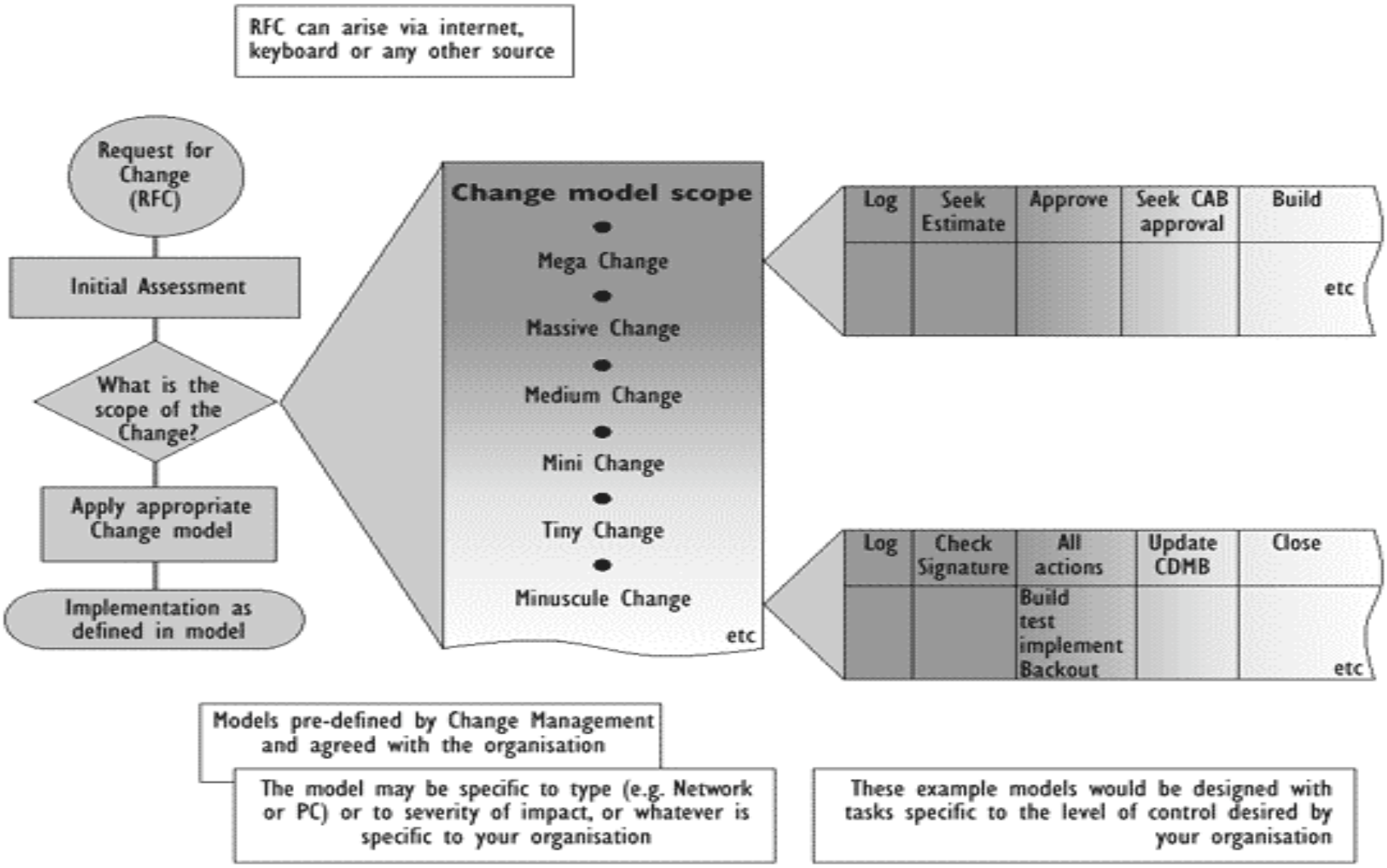
ITIL Generic Process Model



Source: ITIL The Keys to Managing IT Resources

protiviti SM
Independent Risk Consulting

ITIL- Standard Change Management Procedures



Source: ITIL The Keys to Managing IT Resources

protiviti
Independent Risk Consulting

Summary and Key Points

Some thoughts to leave you with and for you to think about if and how they impact your company

- There are significant regulatory and compliance issues facing companies and their IT Organizations
- There are many “lessons learned” from Year 1 of Sarbanes Oxley Projects
- Compliance for Year 2 can take on different forms and approaches
- Many if not all compliance issues relate to being able to substantiate certain processes and that those processes have integrity and perform as designed
- Overall process improvement is necessary to meet quality, cost, and ownership goals

protiviti
Independent Risk Consulting

Questions and Discussion

john.harrison@protiviti.com
713-314-4996

protiviti[SM]
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

All those who need to know their disclosure processes and internal controls over financial reporting are functioning effectively…

Say i