protiviti®
Independent Risk Consulting

Leveraging ITIL® Foundational Controls to Achieve SOX Compliance

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

ISACA San Francisco Fall Conference
September 17th, 2007

Agenda for today

- Introductions & Objectives
- IT Priorities
- Overview of Sarbanes-Oxley Regulations
  - Keys to SOX Compliance
- IT Management Frameworks & Synergy
  - CobiT
  - ITIL
  - Framework Overlap & Implementation Overview
- IT Management Accelerators and Foundational Controls
  - Accelerators – ITPI Research
  - ITPI Foundational Controls
- Q & A

IT's Priorities (REWARDS)…

Top 10 Management Priorities

1. **Align IT and business goals**
2. **IT-enabled process improvement**
3. Business continuity/risk management
4. Improve internal user satisfaction
5. IT staff development
6. Measuring & communicating IT value
7. Improving project management discipline
8. Controlling IT costs
9. **Regulatory compliance**
10. Revenue-generating services / products
11. Data privacy
12. **IT Governance**
13. Internal knowledge management
14. Scaling IT globally

Top 10 Technology Priorities

1. **Integrate/enhance systems & processes**
2. **Ensure data security and integrity**
3. Enable business intelligence
4. New business services / products
5. Mobile / Wireless
6. Service-oriented architecture / enterprise architecture
7. E-commerce
8. Supply chain automation / visibility
9. Open-source software

-State of the CIO Survey, CIO Magazine Jan 07

protiviti® Independent Risk Consulting

...and Barriers to them (RISKS)

1. **Shortage of time for strategic thinking and planning**…
2. Overwhelming **backlog of requests and projects**
3. Inadequate budgets
4. Unknown / unrealistic expectations from the business
5. Lack of business sponsorship / accountability for IT projects
6. Lack of key technical skill sets within IT
7. **Difficulty of proving the value** of IT
8. Lack of business knowledge within IT department
9. Overwhelming pace of technology change
10. **Lack of alignment** between business goals and IT efforts
11. Risk and uncertainty due to volatile economic conditions
12. Inability to negotiate favorable terms with technology vendors

Efficiency

Alignment

Sustainability

-State of the CIO Survey, CIO Magazine Jan 07

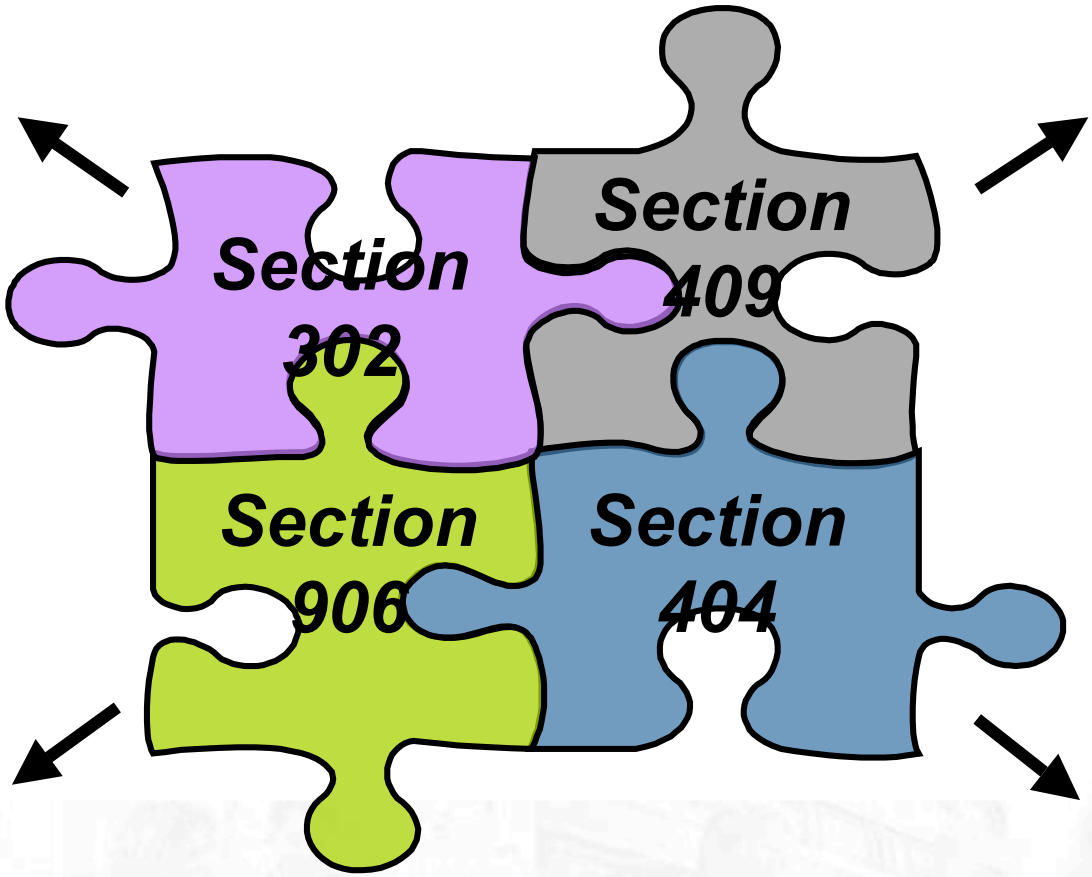
protiviti®
Independent Risk Consulting

Regulatory and Governmental Compliance Issues Affecting IT

- Sarbanes-Oxley Act (SOX)
- Health Information Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS) / AB779
- Patriot Act
- Anti-Money Laundering
- Graham Leach Bliley (GLBA) & Privacy Laws (SB1386)
- OCC, FFIEC, FERC, others
- New York and other Stock Exchange Listing Requirements

Overview of the Sarbanes-Oxley Act

Expanded representations by certifying officers re: disclosure controls



Disclosure of material changes on a "rapid and current basis"

Focused representations by certifying officers linked to criminal provisions of the Act

Assessment of effectiveness of internal controls over financial reporting with external auditor attestation

protiviti®
Independent Risk Consulting

Sarbanes-Oxley is Complex

- Sarbanes-Oxley consists of eleven titles
- Many provisions phase in over time and are dependent on SEC rulemaking
- No one escapes its long reach
- Public reporting is just one aspect of the Act
  - Management is required to file an internal control report with their annual report, stating:
    - Management's responsibilities to establish and maintain adequate internal controls and procedures for financial reporting
    - Management's conclusion on the effectiveness of these internal controls at year end
    - The company's public accountant has attested to and reported on management's internal controls and procedures for financial reporting
  - Management must evaluate design and operational effectiveness of internal controls for financial reporting (as well as its disclosure controls and procedures) on a quarterly basis

protiviti®
Independent Risk Consulting

Overall Key to Regulatory Compliance

- Simply put, management must ensure that key risks are identified and mitigated
- Said another way - key processes are well controlled

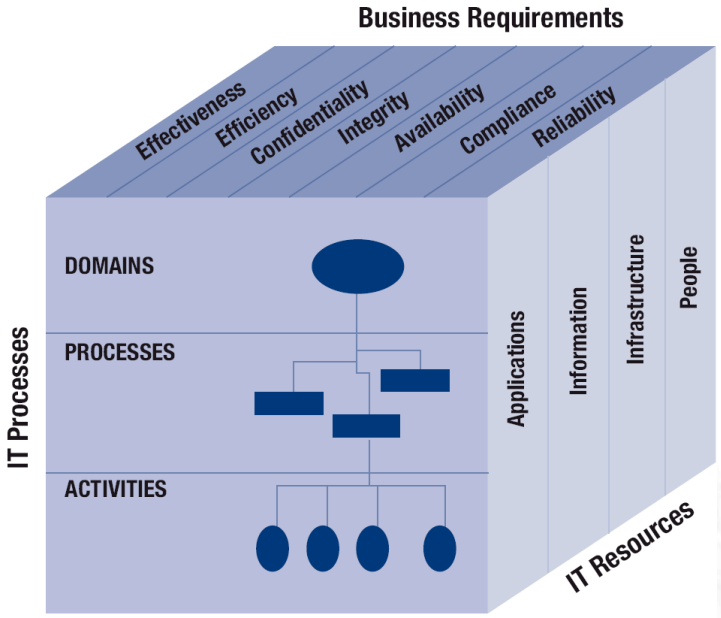
The best way to ensure compliance is through well controlled and documented processes that are understood and operated consistently on a day to day basis

How do you do this in the IT area?

protiviti®
Independent Risk Consulting

CobiT – Identification and Mitigation of Key Risks

- CobiT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks
- The goal of the CobiT framework is to illustrate how IT resources are managed by IT processes to achieve IT goals that support business process requirements, all under one governance umbrella



protiviti®
Independent Risk Consulting

ITIL – Definition of a Process

- A process can be defined as:

  "a connected series of actions, activities, changes etc, performed by agents with the intent of satisfying a purpose or achieving a goal."

- Process control can similarly be defined as:

  "the process of planning and regulating, with the objective of performing a the process in an effective and efficient way."

Source: ITIL - The Keys to Managing IT Resources

protiviti® Independent Risk Consulting

protiviti®
Independent Risk Consulting

IT Management Frameworks & Synergy

CobiT Overview

- "Control Objectives for Information and related Technology"
- Generally accepted internal control framework for IT
- First published in 1996 by ISACA, CobiT is now in version 4.1 (2007)
- Provides products for 3 audiences:
  - Executive Management & Board
  - Business & IT Management
  - Governance, Security, Assurance, and Control Professionals
- Process–driven, but focuses on controls; core elements include:
  - IT processes
  - Control objectives
  - Control practices (activities)
  - Audit Guidelines
- Recent editions also added:
  - Maturity models
  - Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs)
  - Benchmark capability

ITIL Overview

- Developed in the late 1980s, originally published by the UK Government
  - Formulated to capture best practices in managing British government systems
  - Originally published as 2 books (Service Support and Service Delivery)
  - Now includes multiple disciplines in 5 major areas (with many supporting guides)
  - ITIL framework v3 was released May 31, 2007

- ITIL's major theme is IT processes on an enterprise level
  - **Service Design.** 4 processes that "plan ahead" (Availability, Capacity, Continuity, Security)
  - **Service Delivery.** 4 processes that "put it in place" (Change, Release, Config, Service Knowledge)
  - **Service Operation.** 3 processes that "keep it going" (Incident, Problem, Fulfillment)

- Benefits generally credited to ITIL include:
  - **Risk Reduction:** Processes prevent downtime, increase availability and business process / IT system performance
  - **TCO Reduction / ROI Increase:** Standardizing / centralizing processes reduces cost of business support, increases recognized value of IT services to business

- Services and technology demand for ITIL capabilities are at an all-time high, and growing rapidly in the US

Positioning IT Service Management

IT Service Management opens up communications channels between the business and "traditional" IT Operations that improves relationships, increases flexibility, and enables both IT Ops and Application Management to become more strategic partners in business enablement.

"Traditional" IT – Business Alignment

IT – Business Alignment with IT Service Management

protiviti®
Independent Risk Consulting

ITIL Framework Overview (v2)

Service Delivery

Plan IT services based on business needs

- Service Level Mgmt
- Capacity Mgmt
- Availability Mgmt
- Continuity Mgmt
- Financial Mgmt of Services

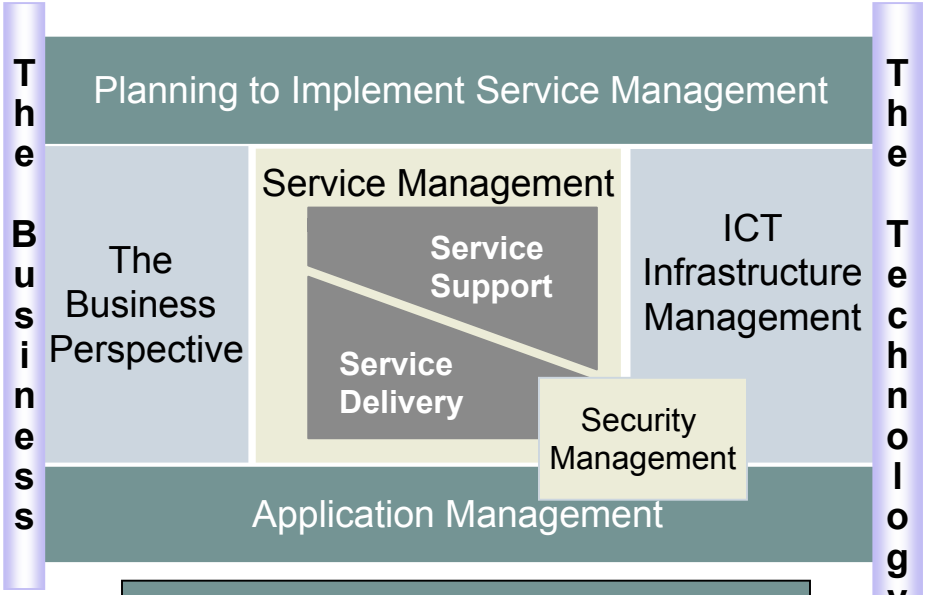
Business Perspective

Define the IT strategy on the business stategy

- Business Continuity Mgmt
- Partnership
- Outsourcing
- Surviving Change
- Transformation

Planning to Implement

Considerations on how to implement ITIL



Managing Applications

Software Development Lifecycle

- Lifecycle Support
- Testing of IT Services

Service Support

Serve the client and operate IT

- Run the Service Desk
- Incident Mgmt
- Problem Mgmt
- Change Mgmt
- Configuration Mgmt
- Release Mgmt

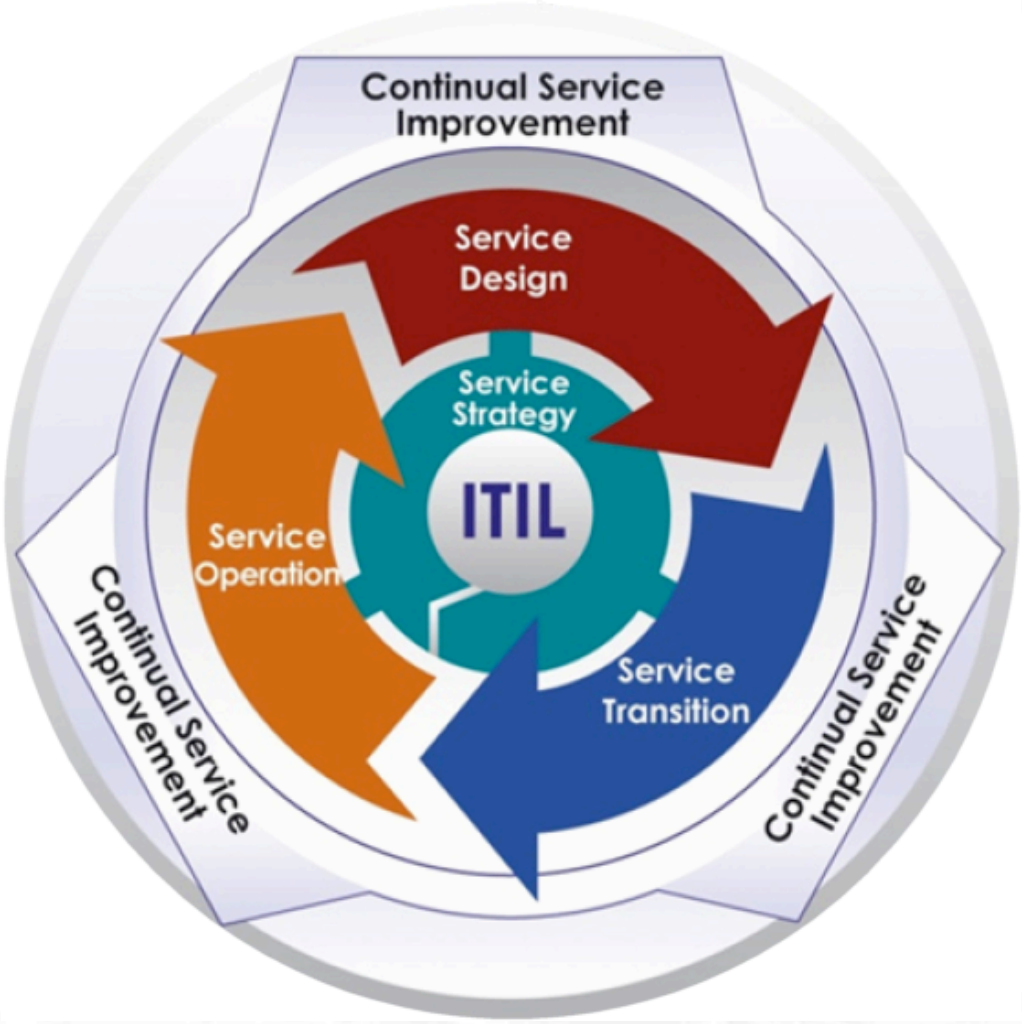
ICT Infrastructure Management

Manage the technical IT components

- Network Service Mgmt
- Operations Mgmt
- IT installation & acceptance
- Systems Mgmt

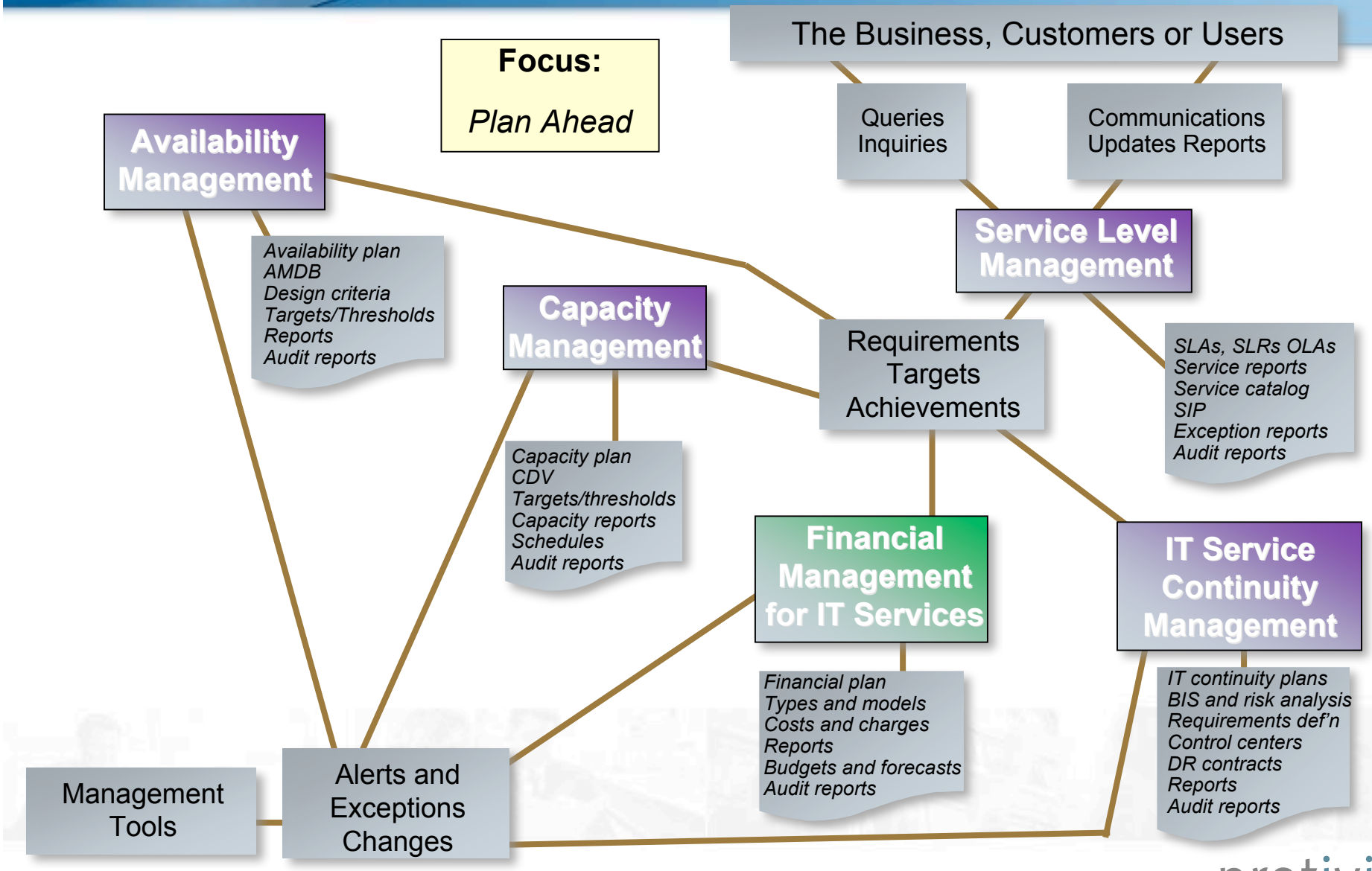
protiviti®
Independent Risk Consulting

ITIL Framework Overview (v3)



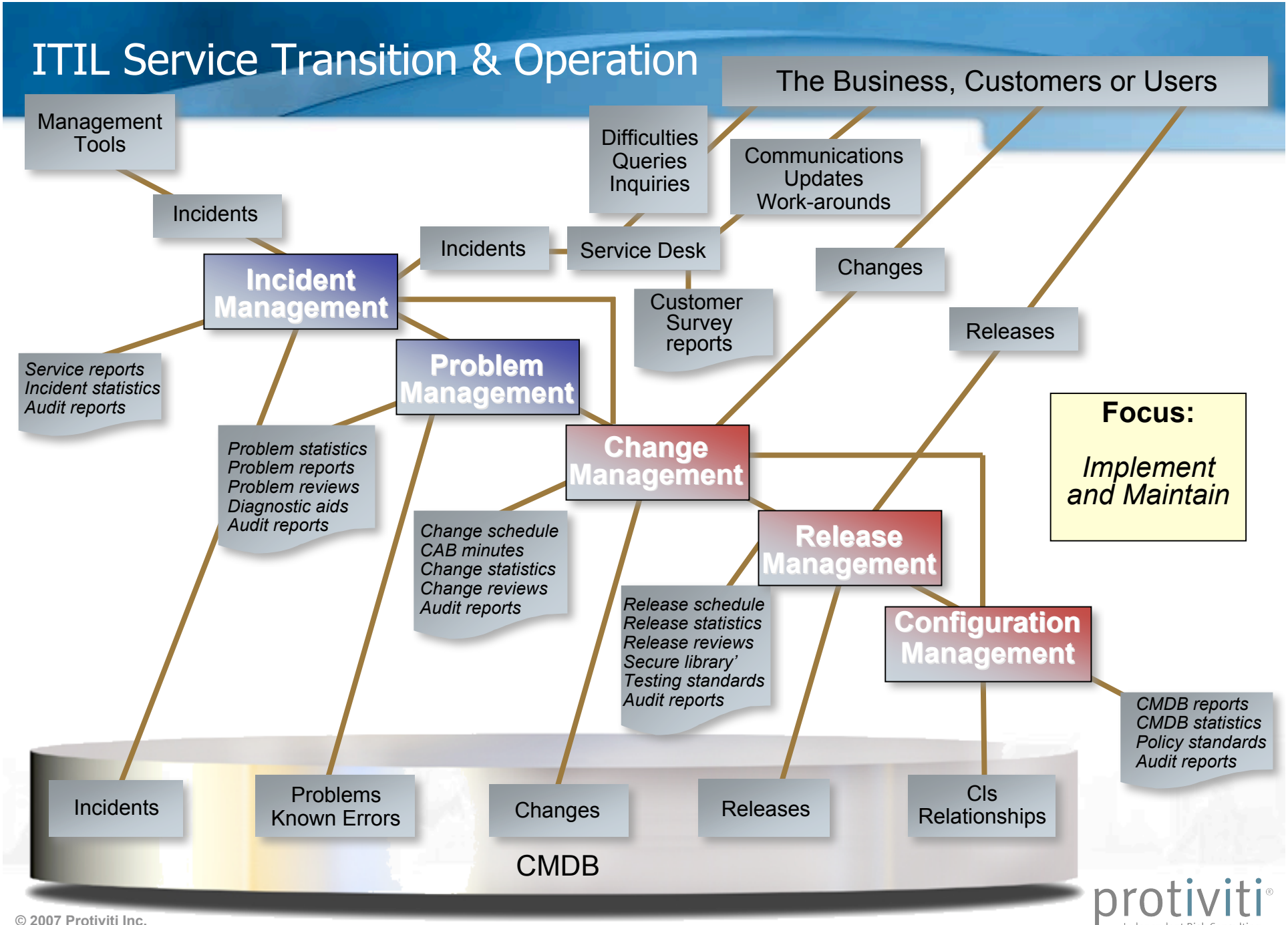
protiviti®
Independent Risk Consulting

ITIL Service Strategy & Design



protiviti®
Independent Risk Consulting

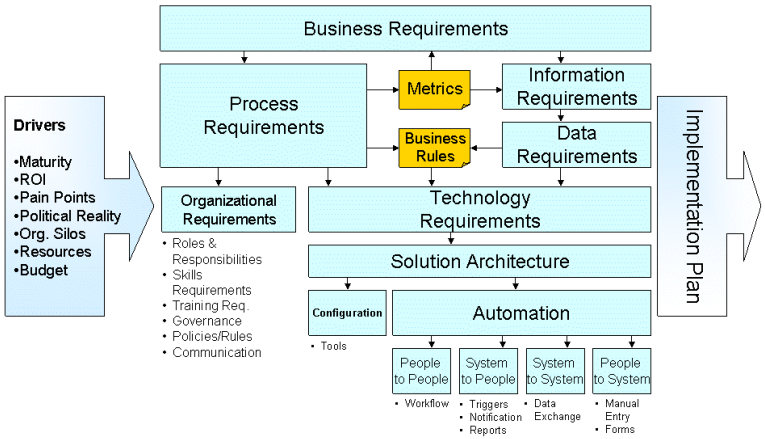
ITIL Service Transition & Operation

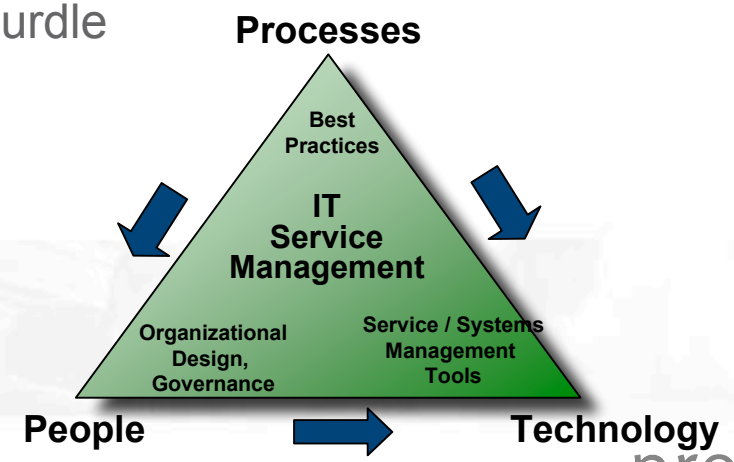


protiviti®
Independent Risk Consulting

Implementing ITIL

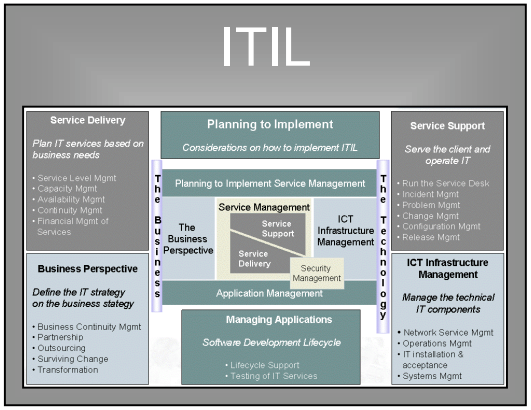
- Not a “project” – it’s a program (continuous improvement)
- Where you start depends on where the pain is:
  - Service Support process areas are common starting point
    - Because they cause most unavailability and draw the most attention
  - Service Delivery processes help prevent problems and enhance alignment
- Can be implemented in multiple ways:
  - Single process at a time: Change, Service Level, Problem, etc.
    - Slower time to value, more risk of program stalling, likely more costly
  - Multi-threaded program: Phased process implementation in parallel
    - Quicker results, but higher implementation management risk and cultural resistance
- Cultural factors often are the biggest hurdle

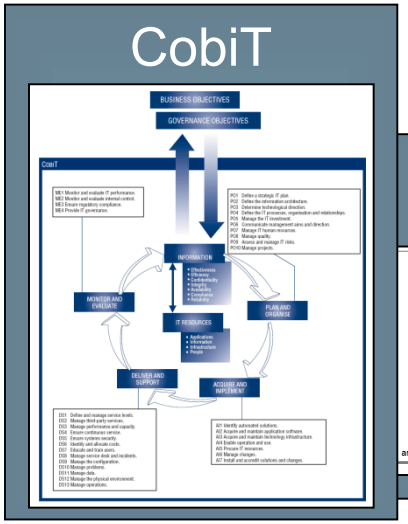


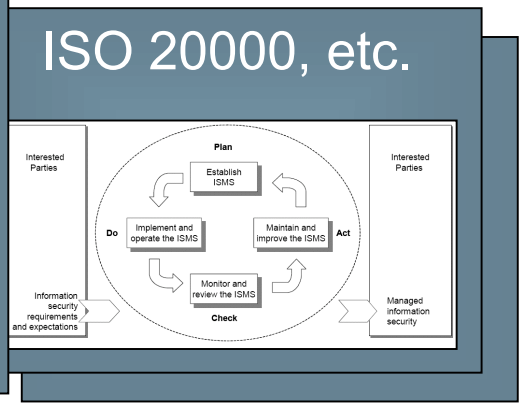


protiviti®
Independent Risk Consulting

Comparing Frameworks







Prescriptive: Describe *how* processes should work

Focus: Effectiveness, Efficiency

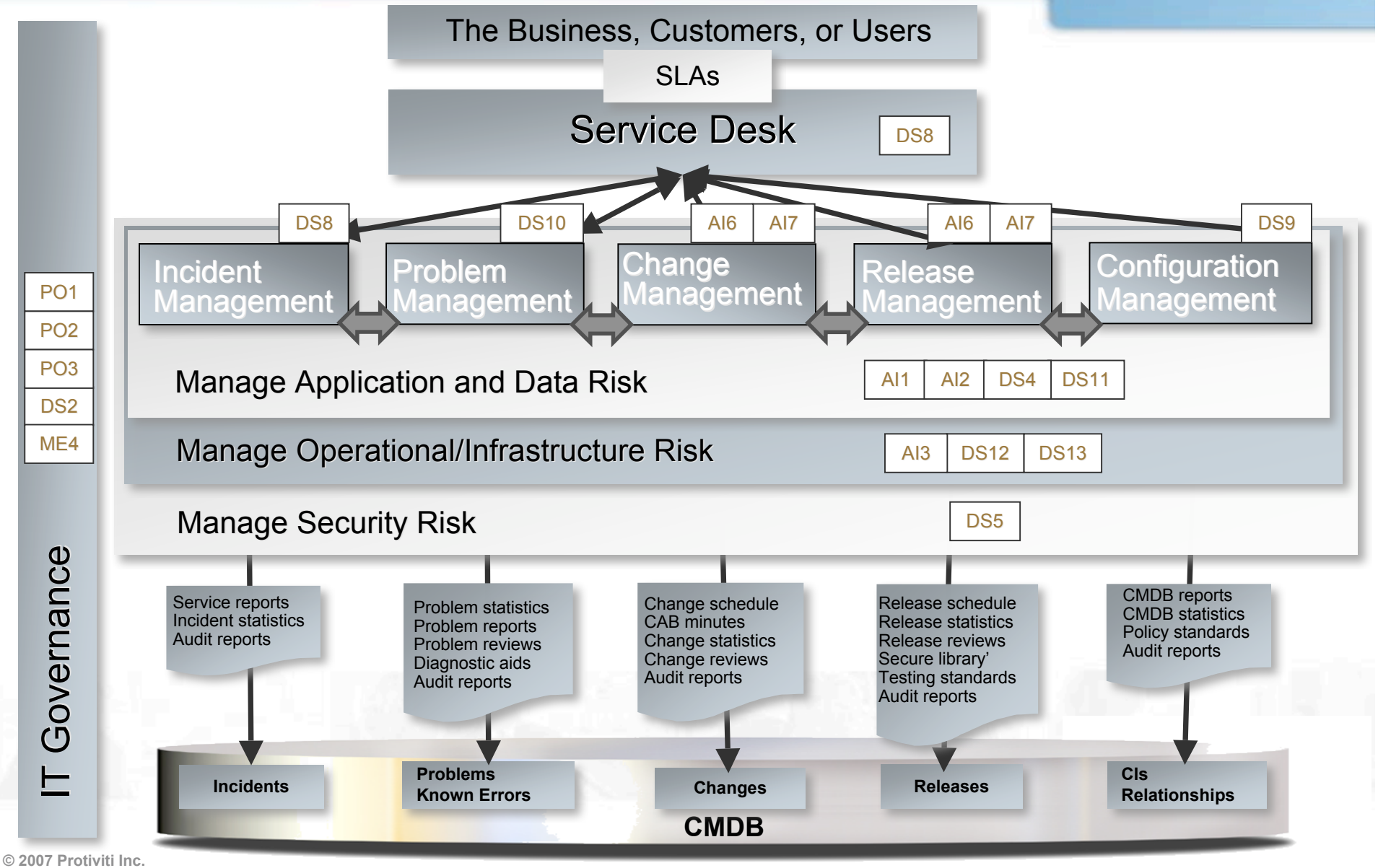
Descriptive: Describe *what* objectives processes ought to achieve

Focus: Effectiveness, Alignment

- Answer: **All** of them…they're not mutually exclusive…
- …example: (CobiT) Controls describe how (ITIL) processes work
- No one framework fits all needs for everyone
  - IT management generally gets more value out of proscriptive frameworks
  - Audit and control practitioners generally "speak" control language

protiviti®
Independent Risk Consulting

Typical SOX / CobiT Objectives in the ITIL Framework



Relating ITIL and CobiT "by the numbers"

- ITGI and other entities have updated relationships between frameworks
  - Strongest relationships are within "Operations" and "Development" areas
  - Somewhat weaker relationships with Governance and Project / Quality Mgt
  - Monitoring / Audit capabilities nearly absent from ITIL

Processes & Domains*	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan & Organize	–	1	–	6	16	–	3	–	15	14			
Acquire & Implement	6	5	6	6	–	35	64						
Deliver & Support	38	15	51	51	3	35	–	58	57	31	2	2	–
Monitor & Evaluate	3	–	–	–									
* Indicates the number of CobiT information requirements mapped													

From ITGI's: Mapping of ITIL with CobiT 4.0

Conclusions

– CobiT is broader in scope, outlines how to build Governance capabilities
– ITIL is more appropriate to design, implement, & improve processes

Both are most useful – *if they applied together* – starting in the right areas

protiviti® Independent Risk Consulting

protiviti®
Independent Risk Consulting

IT Management Accelerators & Foundational Controls

(AKA – Where's the Value?)

Research citation

The following research materials are the property of the Information Technology Process Institute (ITPI)

Visible Ops™ is a registered trademark of ITPI.

All rights reserved.

The IT Controls Performance Study© is a copyright of the ITPI 2007. Permission to cite research used with permission.

Protiviti is a Managing Sponsor of the ITPI, and actively participates in the investment, development, and implementation of ITPI research in the global market.

protiviti® Independent Risk Consulting

ITPI Overview

The IT Process Institute, founded in 2002, is a not-for-profit organization formed by IT practitioners and academics (Carnegie Mellon, FSU) to support IT audit, security, and operations professionals

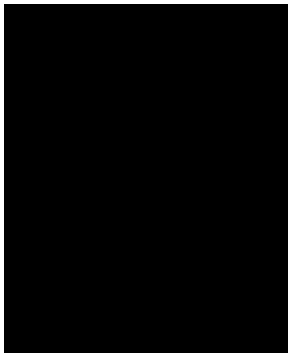
Focus: Research, benchmarking, and prescriptive guidance

Goal: To measurably enhance efficiency & effectiveness of IT operations & controls

Approach: Pairing industry based volunteers with leading university researchers, to identify and study top performing IT organizations

The Visible Ops Handbook™

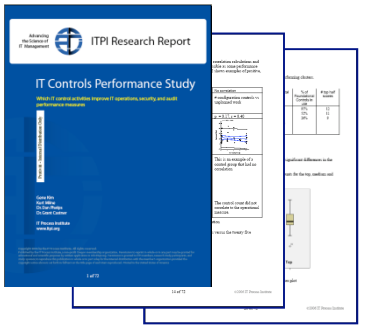
- Based on 5 years studying high-performing IT Operations & Security organizations
- Over 40,000 copies in print
- 100 pages long, dense type but easy to read
- First published in 2004, revised with new content & published again in 2005 / 2007
- Owned by the ITPI, jointly developed by IT practitioners and academic research



IT Controls Performance Study & Benchmark Survey

- Designed to evaluate the performance impact of IT Controls.
- Assumes "controlled" process performs better and defines by how much
- Answer questions about which IT Controls efforts have the greatest impact

Research Accomplishments: 1000+ companies have participated in existing research projects today with an every expanding data pool.



Version 2 of the Controls Performance Study: ***Published May 2007***

protiviti®
Independent Risk Consulting

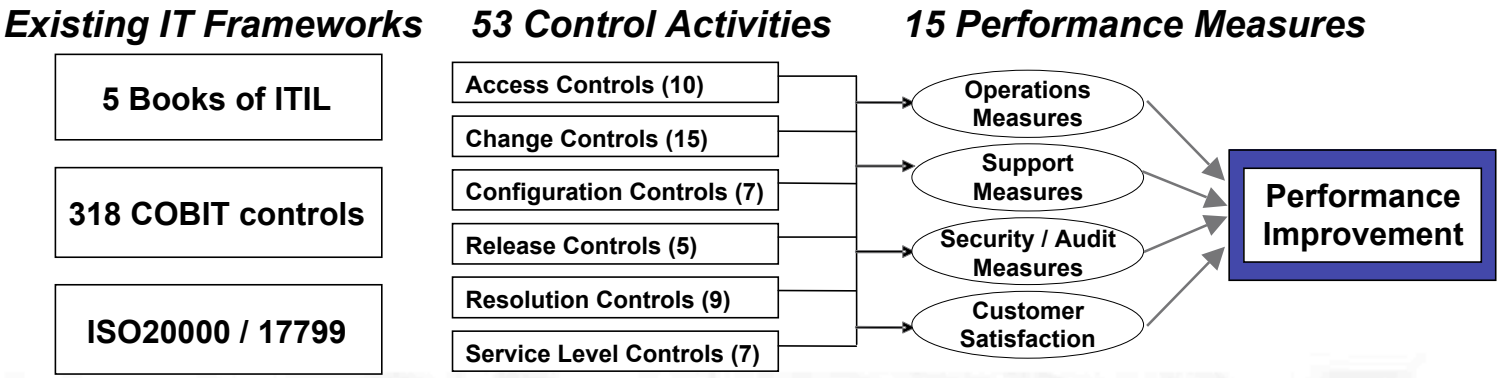
ITPI Controls Performance Study – Key Facts

Study Demographics . . .

- 330 North American companies represented
- Average IT expenditure: $96.8 million
- Mean number of IT employees: 656
- 85% of organizations have 1000+ employees
- 37% have 10,000+ employees
- A broad range of revenue / operating budgets:
  - 42% between $250M and $1B,
  - 41% between $1B and $10B, and
  - 14% from companies with >$10B

Study Details . . .

- Benchmark surveys completed Dec06 / Jan07
- 53% of respondents are IT Director, VP or CXO
- 89 total questions:
  - 13 Demographic Questions
  - 53 Control Activity Questions
  - 12 General IT Effectiveness Questions
  - 11 Specific Control Performance Questions
- New Control Maturity (Likert) Scale



ITPI Controls Performance Study – Research Approach

1: Cluster participants by control use & performance
2: Identify Foundational Controls that best predict performance variation
3: Assess impact of control process maturity
4: Quantify performance improvement potential

protiviti® Independent Risk Consulting

Control Maturity: What it means and how it's used

The ITPI Controls Performance Study (May 2007) and benchmark introduces the concept of control maturity. This perspective is reinforced by the CMMI, CobiT v4.0, and related frameworks (and as used by Protiviti).

	Maturity Level	Process Capability Description	Control Maturity Levels *(as used in ITPI Benchmark)*	Distinguishing Factors
5	Optimizing	**Continuous Improvement**. Process management continuously improving enterprise-wide	Used very consistently, exceptions have consequences	Continuously Improving Process
4	Managing	**Quantitative**. Risks managed quantitatively enterprise-wide; "Chain of accountability"	Used consistently, exceptions are detected	Predictable Process
3	Defined	**Qualitative / Quantitative**. Policies, process and standards defined and institutionalized	Used consistently, exceptions cannot be detected	Standard, consistent process
2	Repeatable	**Intuitive** – Process established and repeating; continued reliance on people; documentation weak	Documented, but only used inconsistently	Disciplined Process
1	Initial	**Ad Hoc** – Control is not a priority – Unstable environment leads to dependency on heroics	Documented, but not in use	Process Recognition
0	Non-existent	**Chaotic** – Management Processes not applied at all	Control not used	

Risk ↓ Quality ↑

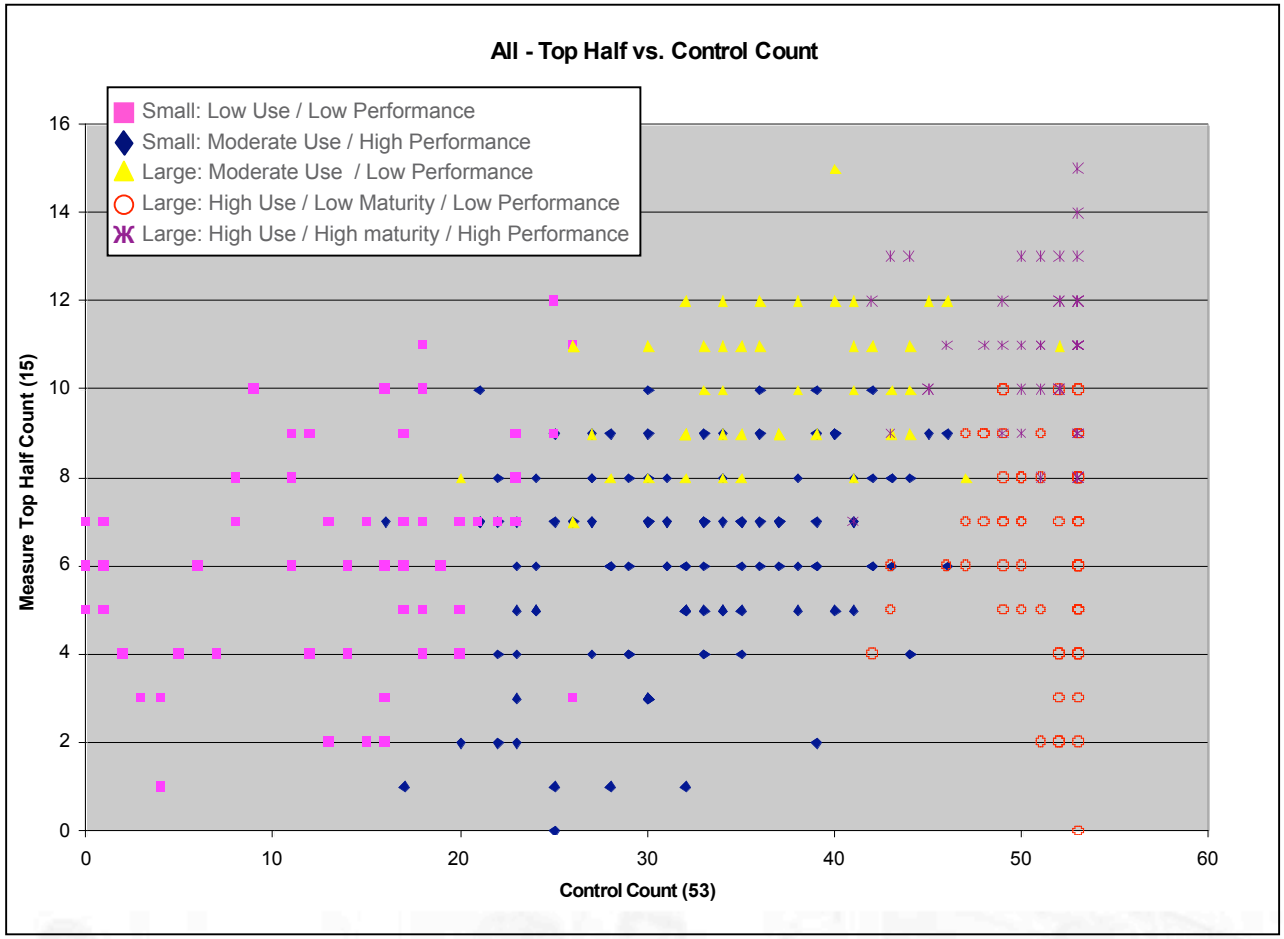
Controls are considered "In Use" at a Level 3 and above on this scale.

"In Use"

"Not In Use"

protiviti® Independent Risk Consulting

1: Use of IT Controls Affects IT Performance



Basic Analysis:

5 Performance Clusters are evident, with:

- Similar maturity of controls
- Distinct profiles of IT performance

…but there is no single determinant of performance!!

Several important trends:

- No companies with low control maturity had high IT performance
- IT Controls affect performance *differently* at Small vs. Large companies
- Control Maturity matters, *especially* in Larger companies

How to Read this Graph:

Control Count (horizontal axis): The number of controls (of 53) a company self-assessed at a control maturity level of 3 or higher. Companies with more defined / mature controls are to the right.

Measure Top Half Count (vertical axis): The number of performance measures for which a company had (of 15 KPIs) was in the top-half (50th percentile or above) of the population of 330. Higher performers are toward the top.

protiviti® Independent Risk Consulting

2A: Foundational Controls (Smaller Organizations)

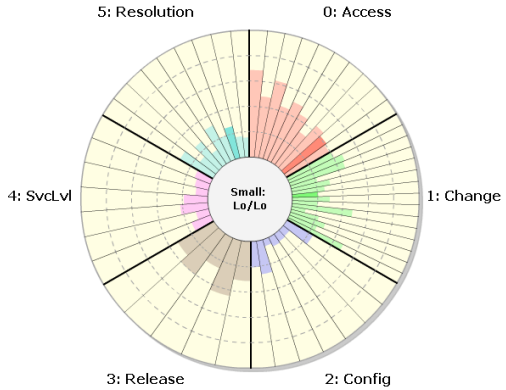
Research Question: What subset of controls impact <u>smaller</u> organization performance the most?

Methodology: Use regression to determine relationship between controls and performance for two smaller organization clusters with Low and Moderate control use

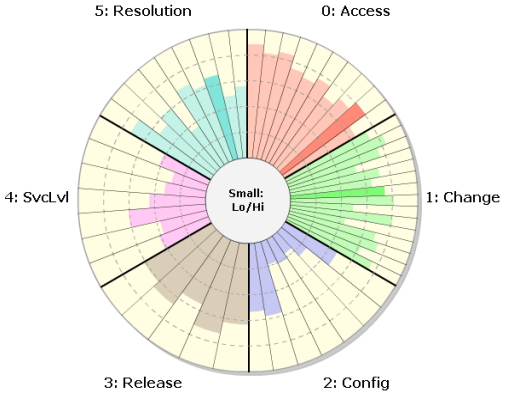
Findings: Three controls predict 45% of performance variation in smaller organizations with Low to Moderate control use:

1. A defined process to detect unauthorized access
2. Defined consequences for intentional, unauthorized changes
3. A defined process for managing known errors

Low Use / Low Perf. (18%)



Moderate Use / High Perf. (14%)



Important Note:

In this Study, there is no single, distinct boundary between "Smaller" and "Larger" companies – the distinction found was between companies that tended to "use" more controls *(with a tendency to be "Large")* and those that did not *(with a tendency to be "Small")*

protiviti®
Independent Risk Consulting

2B: Foundational Controls (Larger Organizations)

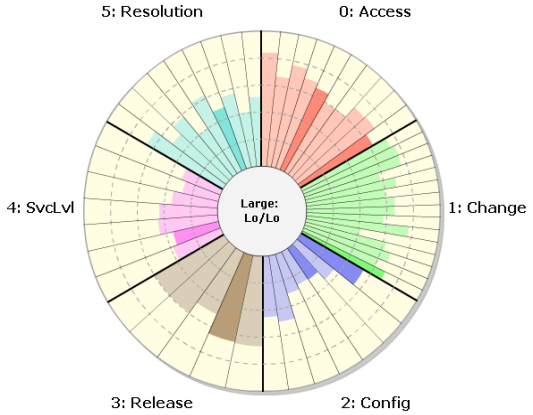
Research Question: What subset of controls impact larger organization performance the most?

Methodology: Use regression to determine relationship between controls and performance for two larger organizational clusters

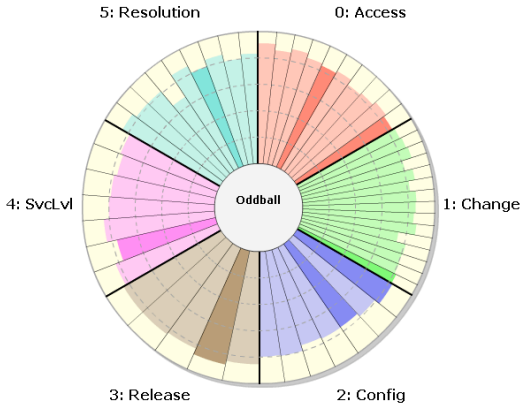
Findings: Nine foundational controls predict 60% of performance variation in smaller organizations

1. A defined process to analyze & diagnose root cause of problems
2. Provide IT personnel with accurate information about the current configuration
3. Changes are thoroughly tested before release
4. Well-defined roles and responsibilities for IT personnel
5. A defined process to review logs of violation and security activity to identify and resolve unauthorized access incidents
6. A defined process to identify consequences if service level targets are not met
7. A defined process for IT configuration management
8. A defined process for testing releases before moving to the production environment
9. CMDB describes the relationships and dependencies between configuration items (infrastructure components)

Moderate Use / Low Perf. (35%)



High Use / Low Perf. (19%)



protiviti®
Independent Risk Consulting

3: Assess impact of control process maturity

Research Question: Does process maturity explain performance difference between two larger organization clusters – both with High control use – but different levels of performance?

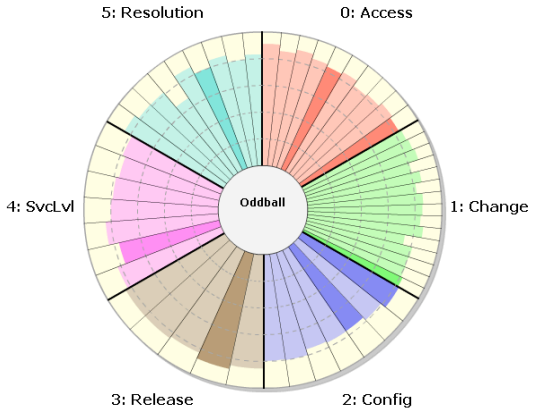
Methodology: Test control use and control maturity measures to determine if they are statistically different for these two groups.

- Group respondents by performance, and assess various maturity measures for practical use
- Count of foundational controls at process maturity level 4 and 5 had strongest correlation with performance

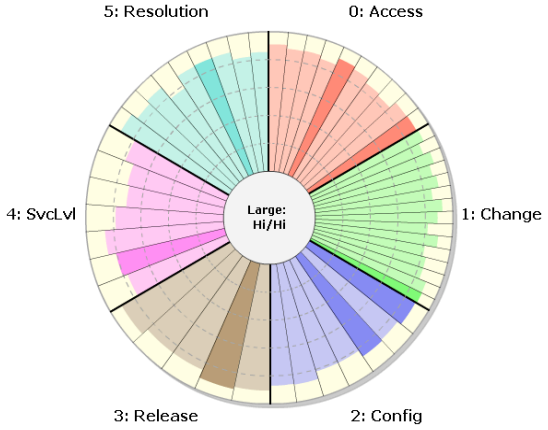
Findings: Both overall control maturity and foundational control maturity are statistically higher for high performing cluster:

- Process maturity explains – in part – the difference in performance of these two organization types
- Possible Conclusions:
  - Foundational IT controls should be implemented at higher level of process maturity in order to achieve performance improvement
  - Some Process should be monitored for exceptions, and exceptions should be managed with consequences

High Use / Low Perf. (19%)



High Use / High Perf. (14%)



protiviti®
Independent Risk Consulting

4: Quantify performance improvement potential

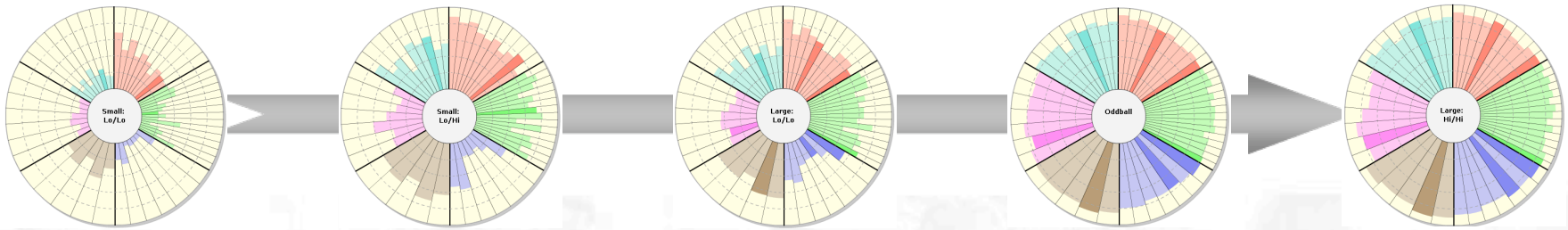
Research Question: What is the performance improvement potential for using foundational controls at higher levels of process maturity?

Methodology: Separate Top 15th percentile of performers, and quantify performance difference with other Medium and Low performers

Findings: Top performers have significantly higher results in key operating measures

Relative to Low and Medium Performers, Top Performers on average…

- …spend 35%–58% less time to repair large IT system outages
- …authorize and implement 5–14 X more IT changes
- …have 11%–25% better change success rates
- …process 29%–55% fewer "emergency" change requests
- …support 2.6–6.6 times more software applications per IT staff
- …support 1.3–1.9X more servers per System Administrator
- …have 20%–50% fewer late projects
- …have 18%–30% higher customer satisfaction
- …have 12%–37% lower unplanned IT work
- …automatically detect 12%–76% more potential security breaches
- …have 39%–52% lower repeat audit findings



A significant portion of performance differential is due to Foundational Control Use

protiviti® Independent Risk Consulting

Key Findings Summary & Conclusions

1. Controls impact smaller and larger organizations differently
2. Three Foundational Controls predict 45% of the performance variation in Smaller organizations
3. Nine Foundational Controls predict 60% of the performance variation in Larger organizations
4. Organizations should monitor and manage process exceptions for Foundational Controls in order to achieve performance improvement
5. Performance improvement potential is significant

Top Performers get *more* done with *less*…

Top Performers have *much fewer* audit & regulatory issues…

…and the cost savings associated with improvements such as reduced unplanned work, increased change success and higher first-fix rates goes *directly to the bottom line*

protiviti® Independent Risk Consulting

The ITPI 12 "Foundational Controls"

Control Area	Foundational Control	Top Performer Control Use	
		Small Orgs	Large Orgs
"Building Block" foundational controls – Predict 45% of performance variance in Smaller companies			
Access	A defined process to detect unauthorized access	93%	98%
Change	Defined consequences for intentional, unauthorized changes	74%	100%
Resolution	A defined process for managing known errors	78%	100%
"Essential" foundational controls – Predict 60% of performance variance in Larger companies			
Access	Well-defined roles and responsibilities for IT personnel	85%	100%
	A defined process to review logs of violation and security activity to identify & resolve unauthorized access incidents	72%	98%
Change	Changes are thoroughly tested before release	89%	100%
Configuration	Provide IT personnel with accurate information about the current configuration	67%	96%
	A defined process for IT configuration management	54%	98%
	CMDB describes the relationships and dependencies between configuration items (infrastructure components)	20%	100%
Release	A defined process for testing releases before moving to the production environment	89%	100%
Resolution	A defined process to analyze and diagnose the root cause of problems	74%	100%
Service Level	A defined process to identify consequences if service level targets are not met	43%	87%

Note: *Controls are only considered "In Use" at a Control Maturity Level 3 or above*

protiviti®
Independent Risk Consulting

ITPI Performance Measures for Top Performers

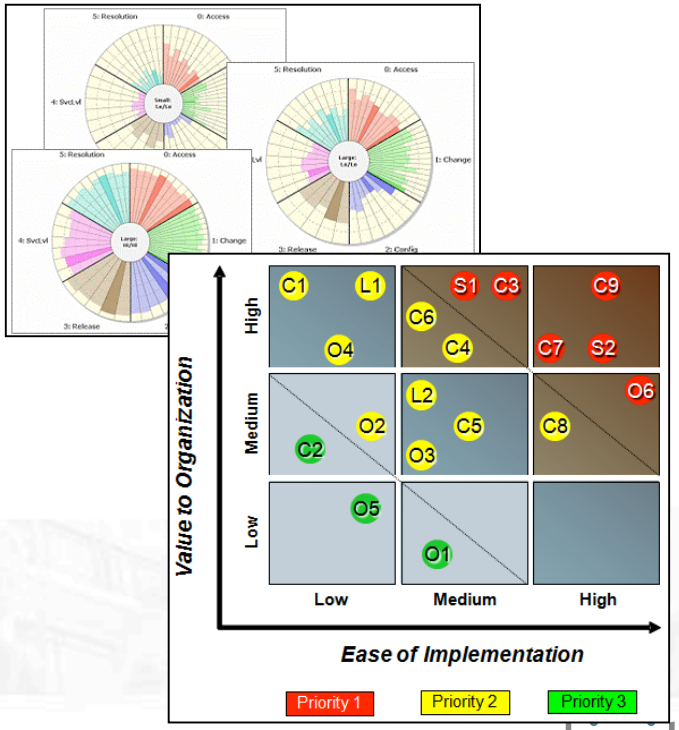
Performance Measure	Smaller Top Performers	Larger Top Performers
Operations Measures	**25th-75th Percentile**	
Change Success Rate (%)	95–98%	95–99%
Emergency Change Rate (%)*	3–10%	5–10%
Late Project Rate (%)*	10–50%	10–29%
Server / System Admin Ratio (ratio)	25–120	11–70
Support Measures	**25th-75th Percentile**	
First Fix Rate (%)	83–95%	80–95%
Incident SLA Rate (%)	90–98%	90–99%
Large Outage Mean Time To Repair (hours)*	1–4	0.6–5.5
Security and Audit Measures	**25th-75th Percentile**	
Security Breaches No Loss (%)	99–100%	96–100%
Security Breaches Corrected (%)	90–100%	90–100%
Security Breaches Auto Detected (%)	80–96%	75–99%
Repeat Audit Findings (%)*	0–47%	0–33%
Customer Satisfaction Measures	**Average**	
End User Satisfaction (1-5 scale)**	3.8	4.3
Business Management Satisfaction (1-5)**	3.6	4.3
IT Staff Customer Awareness (1-5)**	4.2	4.6
IT Staff Customer Communication (1-5)**	3.6	4.3
** –mean used instead of median	* –lower is better	

The Inclusion of Maturity

The use of the 12 “Foundational Controls“, based on the CobiT and ITIL frameworks, identified by the ITPI Study has been shown to have a significant, positive effect on IT performance. The ITPI Study data empirically shows that companies with the Foundational Controls in place, and companies that performed those controls well, had the greatest performance impacts.

What this means for SOX:

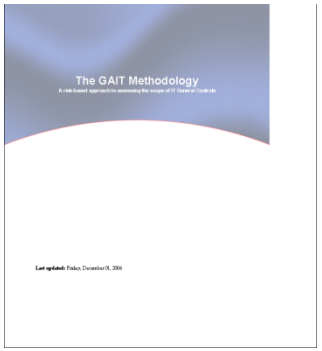
- You now have the ability to evaluate not only the existence of key controls, but also their maturity
- You can better target areas for remediation based on the greatest overlap of impact on compliance and operational effectiveness/efficiency
- You can more easily identify areas for potential automation, based on the greatest positive impacts for the organization
- You can better understand which areas of compliance are the most immature and prone to failure, focusing testing and awareness efforts appropriately

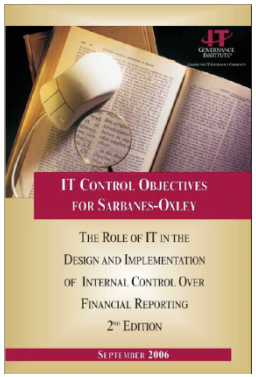


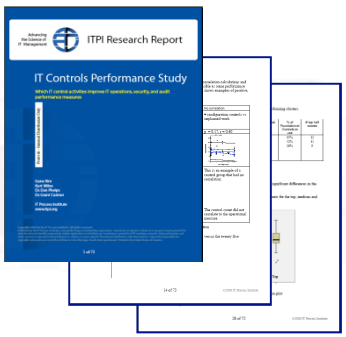
protiviti®
Independent Risk Consulting

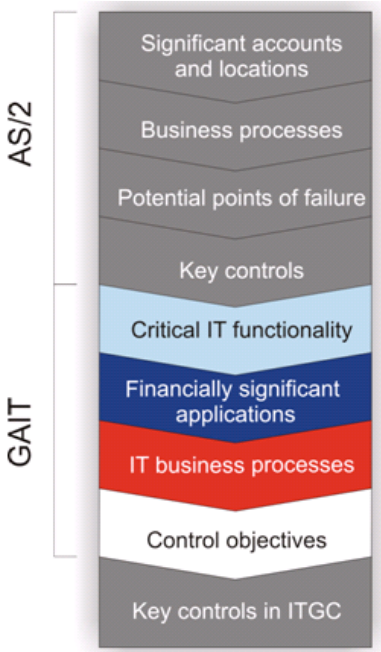
An Example Approach

- The SOX team uses the **GAIT** (Guide to the Assessment of IT General Controls Scope) Methodology from the Institute of Internal Auditors for overall scoping of IT General Controls (ITGC) and the IT Governance Institute's **'IT Control Objectives for Sarbanes-Oxley**' to guide us in our defining specific control objectives for the IT department.
- By applying GAIT, a **linkage is established between the key business cycles and the underlying technology** that supports those processes. This defines the technology that will be in-scope for SOX.
- By including the **ITPI benchmarks**, another dimension of controls is exposed, allowing better decision-making for compliance and value-added Internal Audit activities, by **defining those areas that will require the most time and attention or would benefit the most from remediation/automation**.



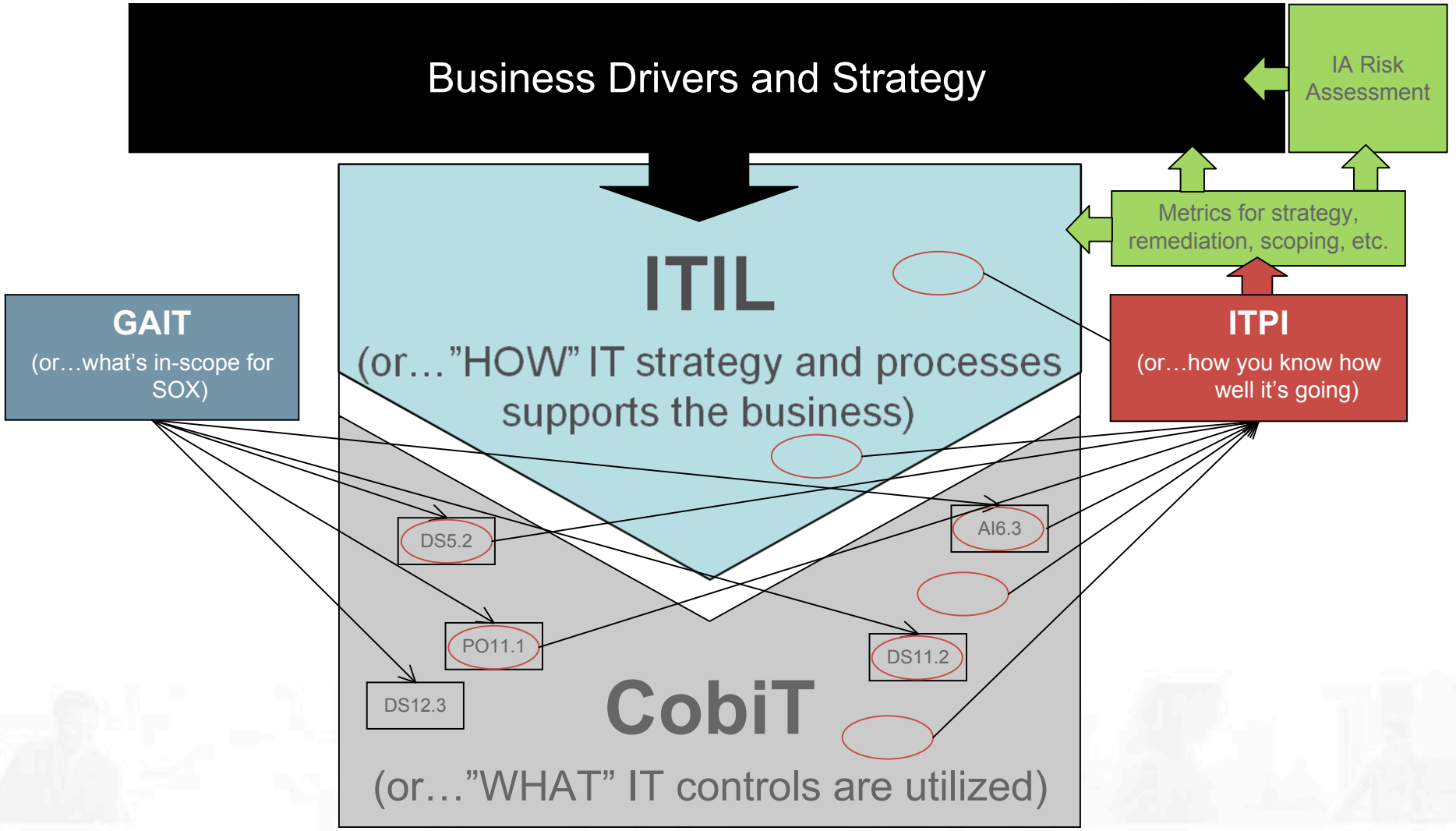






protiviti®
Independent Risk Consulting

In Other Words



protiviti®
Independent Risk Consulting

The Benefits of Understanding Maturity

For the CIO:

•Better understanding of the integration between business and IT

•Understanding of priorities for developing and executing IT strategy

•Assistance in developing metrics for communicating the value of IT

For the CFO:

•Better understanding of how your IT spend is being utilized via clear benchmarking to others in your industry

•The identification of areas from an operational and compliance standpoint which need greater attention to support your business

For the Internal Audit Director:

•Understanding of the maturity of your current controls for use in better scoping and executing on compliance efforts – focusing on those areas most in need of remediation and providing the most value organizationally

•Better leverage of compliance-specific activities (SOX et al.) into value-added Internal Audit initiatives – focusing your future IT Audit efforts on the intersection of those areas of highest risk and lowest maturity in the organization

protiviti®
Independent Risk Consulting

Closing and Q&A

Questions

Comments

Thank You!

Chad Kalmes
Associate Director – San Francisco
CISA, CISSP-ISSMP
chad.kalmes@protiviti.com
415.402.365

Paulina Fraser
Manager – San Francisco
CISA, PMP
paulina.fraser@protiviti.com
415.402.6422

protiviti®
Independent Risk Consulting