Integrating COBIT® into the IT Audit Process (Planning, Scope Development, Practices)

April 20, 2006

San Francisco ISACA Chapter Luncheon Seminar

Presented By

Lance M. Turcato, CISA, CISM, CPA
Deputy City Auditor – Information Technology
City of Phoenix

Audience Poll

CobiT Knowledge

- First exposure?
- General understanding?
- Strong knowledge of CobiT framework?

Current Users of CobiT

- Incorporated Into Audit Process?
- Adopted by IT Management?
- Users of a framework other than CobiT?

AGENDA

Topic
Overview of COBIT® Components
Integrating COBIT® Domains into IT Audit Planning & Scope Development
- *Audit Universe* Considerations
- Ensuring Consistent Coverage
- Integrating Relevant Industry Standards, Guidelines, and Best Practices
- Organizational IT Policy, Standard, Guideline, and Procedure Considerations
Integrating COBIT® into the IT Audit Lifecycle
Using COBIT® to Establish IT Risk & Control Measurement
Resources & Wrap-up

Overview of COBIT® Components

IT Governance Institute
(http://www.itgi.org/)

COBIT® - Background

"Generally applicable and accepted international standard of good practice for IT control"

C Control
OB OBjectives
I for Information
T and Related Technology

"An authoritative, up-to-date, international set of generally accepted *Information Technology Control Objectives* for day-to-day use by business managers and auditors."

COBIT's Scope & Objectives

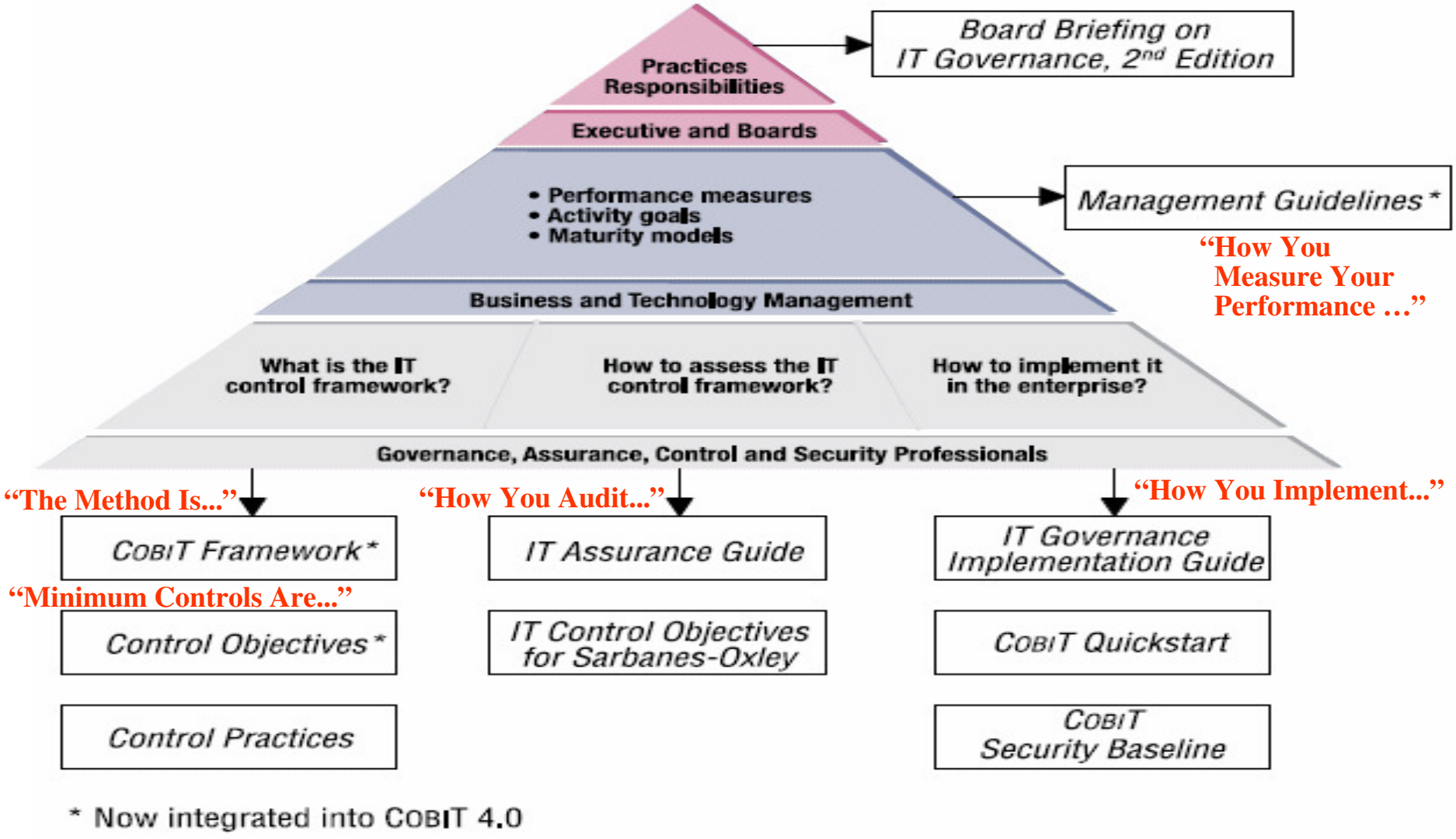
- COBIT® 4.0 was developed and by the IT Governance Institute (www.itgi.org) and was released in December, 2005.

- COBIT® has evolved into an IT governance / control framework:
  - A toolkit of "best practices" for IT control representing the consensus of experts
  - IT Governance focus
  - Linkage with business requirements (bridges the gap between control requirements, technical issues, and business risks).
  - Management – process owner – orientation (accountability)
  - Measurement and maturity driven
  - Generic focus – applicable to multiple environments
  - Organizes IT activities into a generally accepted process model (in alignment with ITIL, ISO, and other relevant 'best practices')
  - Identifies the major IT resources to be leveraged
  - Defines control objectives and associated assurance guidelines

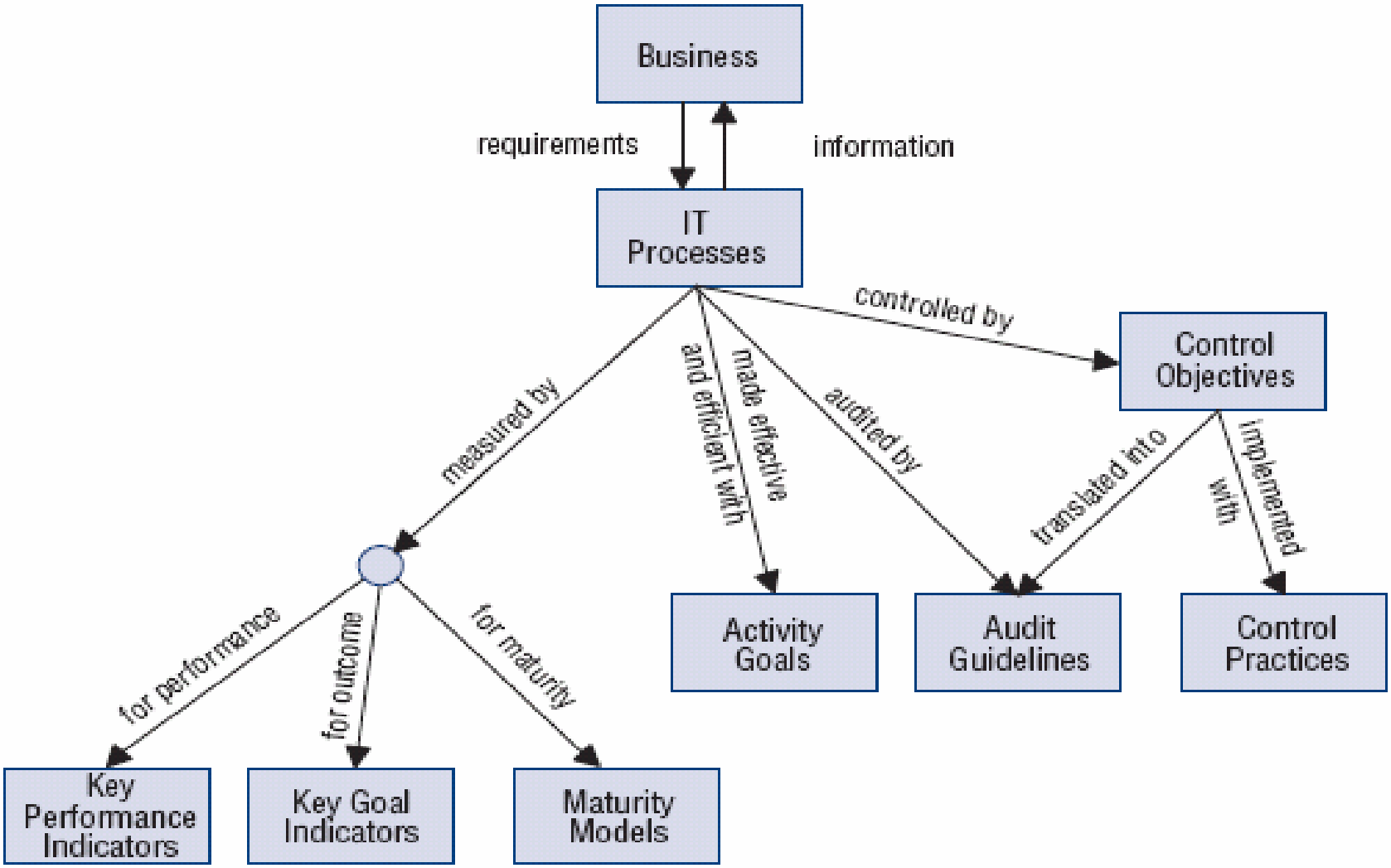
COBIT® As A Framework

- Enables the **auditor** to review specific IT processes against COBIT's Control Objectives to determine where controls are sufficient or advise management where processes need to be improved.
- Helps **process owners** answer questions - "Is what I'm doing adequate and in line with best practices? If not, what should I be doing and where should I focus my efforts?"
- COBIT® is a framework and is NOT exhaustive or definitive. The scope and breadth of a COBIT® implementation varies from organization to organization.
- COBIT® prescribes "what" best practices should be in place. An effective implementation requires that COBIT® be supplemented with other sources of best practice that prescribe the "how" for IT governance and controlled process execution.

Hierarchy of COBIT® Components



Relationship of COBIT® Components



COBIT® Structure
Overview

- Starts from the premise that IT needs to *deliver the information* that the enterprise needs to *achieve its objectives*
- Promotes *process focus* and *process ownership*
- Divides IT into 34 processes belonging to four domains (providing a high level control objective for each process)
- Looks at fiduciary, quality and security needs of enterprises, providing seven *information criteria* that can be used to <u>generically</u> define what the business requires from IT
- Is supported by a set of over 200 detailed control objectives

IT Domains

- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

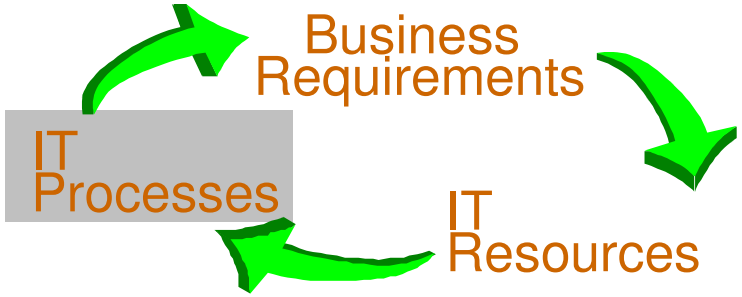
Information Criteria

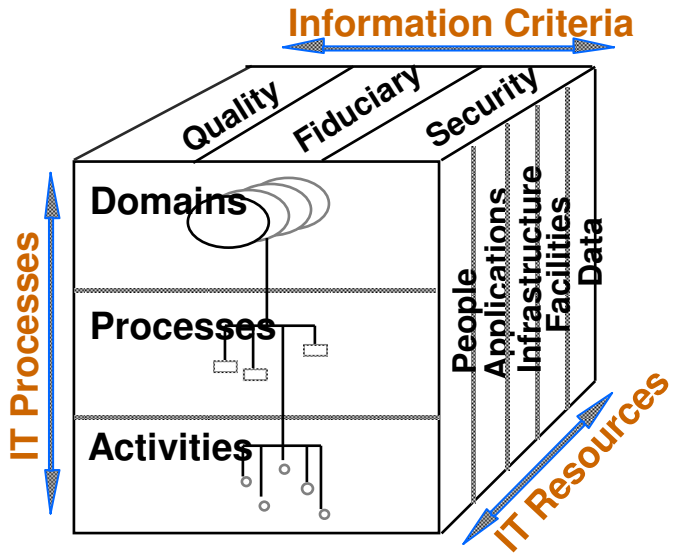
- Effectiveness
- Efficiency
- Availability
- Integrity
- Confidentiality
- Reliability
- Compliance

Business Requirements

COBIT® Structure

Aligning Requirements, Processes, Resources & Activities





Domains

- **Natural grouping of processes, often matching an organizational domain of responsibility.**

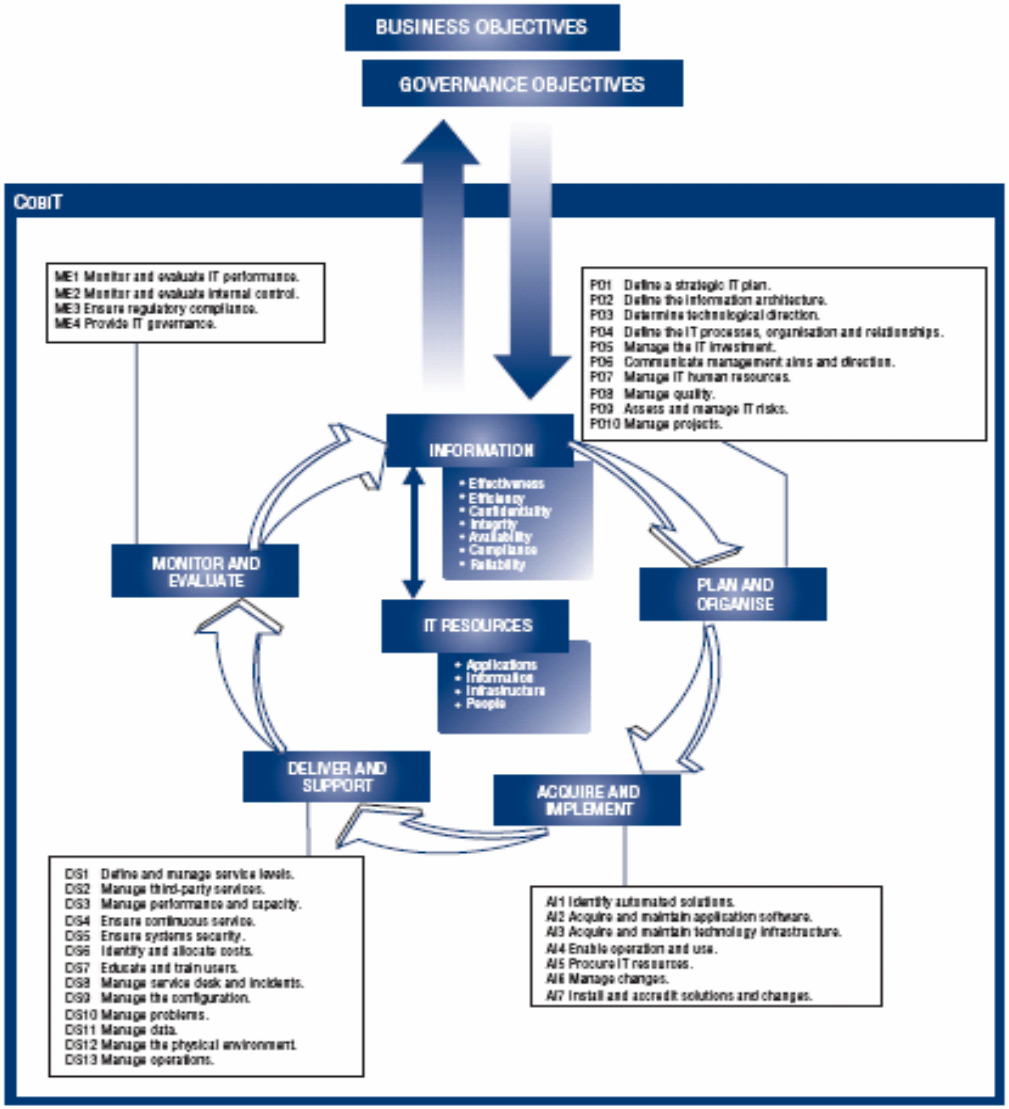
Processes

- **A series of joined activities with natural (control) breaks.**

Activities

- **Actions needed to achieve a *measurable* result. Activities have a life-cycle whereas tasks are discreet.**

COBIT® Structure
Example

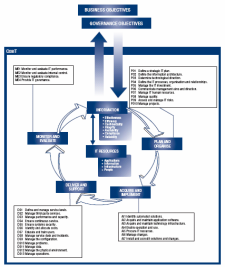


IT Domains
- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

IT Processes
- Change Management
- Contingency Planning
- Problem Management
- Policy & Procedures
- Acceptance Testing
- etc...

Activities
- Record new problem
- Analyze problem
- Propose solution
- Monitor solution
- Record known problem
- etc...

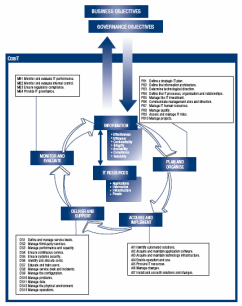
COBIT® *High-Level* Processes / Objectives



Plan & Organize

PO 1	Define a Strategic IT Plan
PO 2	Define the Information Architecture
PO 3	Determine Technological Direction
PO 4	Define the IT Processes, Organization, & Relationships
PO 5	Manage the IT Investment
PO 6	Communicate Management Aims and Direction
PO 7	Manage IT Human Resources
PO 8	Manage Quality
PO 9	Assess & Manage IT Risks
PO 10	Manage Projects

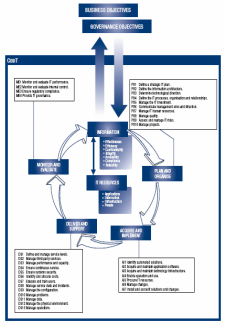
COBIT® *High-Level* Processes / Objectives



Acquire & Implement

AI 1	Identify Automated Solutions
AI 2	Acquire and Maintain Application Software
AI 3	Acquire and Maintain Technology Infrastructure
AI 4	Enable Operation and Use
AI 5	Procure IT Resources
AI 6	Manage Changes
AI7	Install and Accredit Solutions and Changes

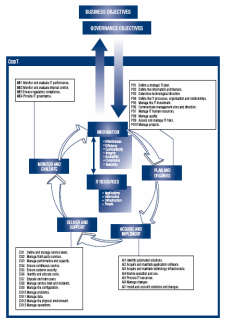
COBIT® *High-Level* Processes / Objectives



Deliver & Support

DS 1	Define and Manage Service Levels
DS 2	Manage Third-Party Services
DS 3	Manage Performance and Capacity
DS 4	Ensure Continuous Service
DS 5	Ensure Systems Security
DS 6	Identify and Allocate Costs
DS 7	Educate and Train Users
DS 8	Manage Service Desk and Incidents
DS 9	Manage the Configuration
DS 10	Manage Problems
DS 11	Manage Data
DS 12	Manage the Physical Environment
DS 13	Manage Operations

COBIT® *High-Level* Processes / Objectives



Monitor & Evaluate

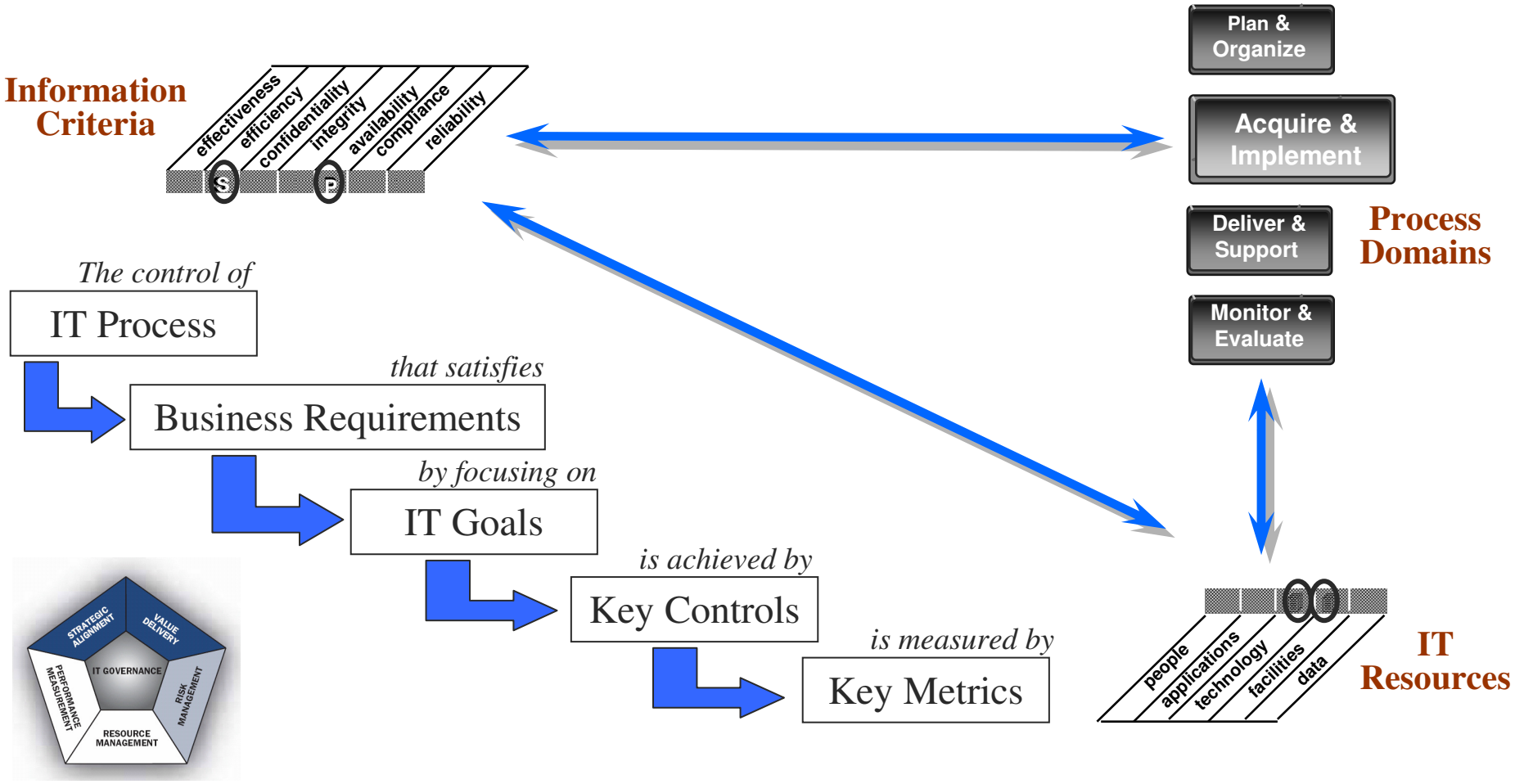
M 1 Monitor and Evaluate IT Performance
M 2 Monitor and Evaluate Internal Control
M 3 Ensure Regulatory Compliance
M 4 Provide IT Governance

Linking The Processes To Control Objectives

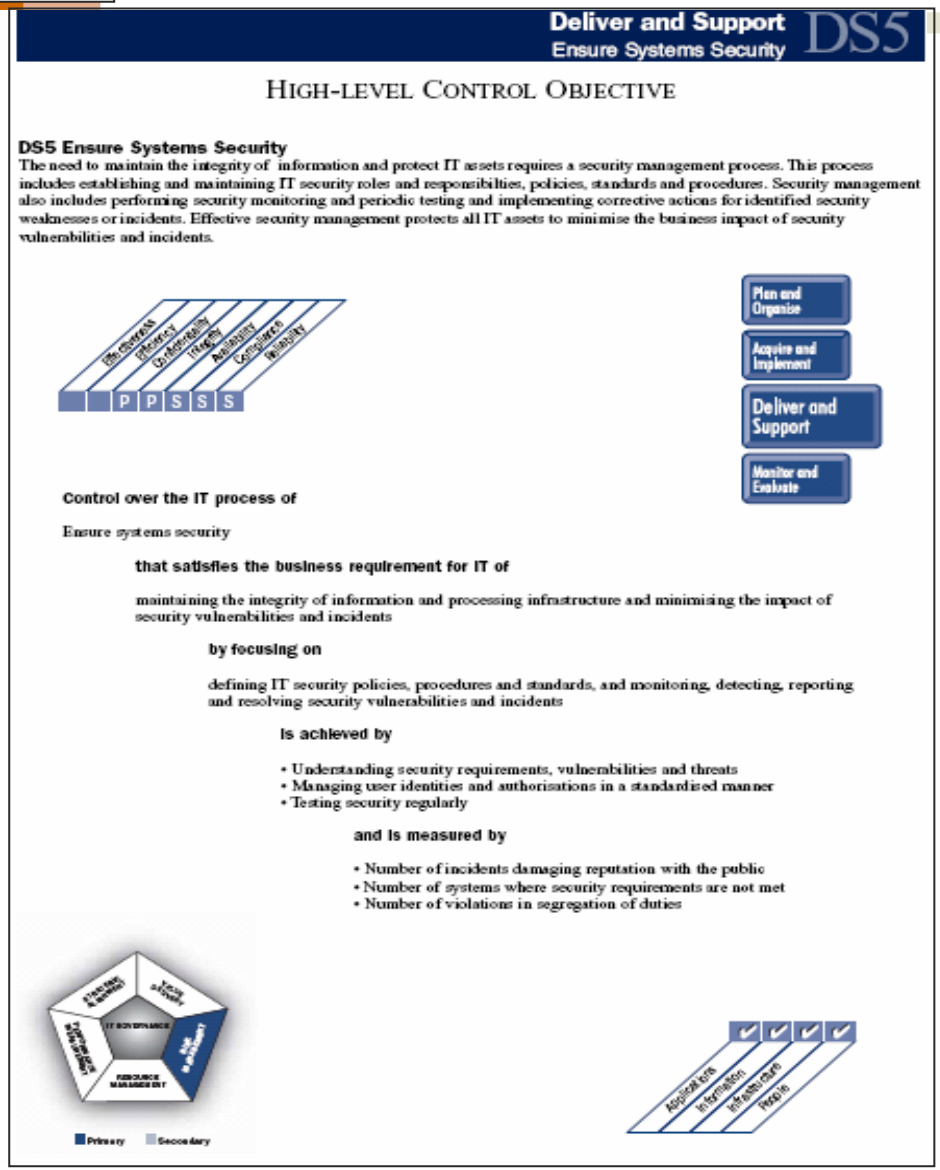
(34 High-level and 200+ Detailed Objectives)

CobiT's Waterfall and Navigation Aids

Linking *Process, Resource & Criteria*



Example of COBIT® 4.0 - DS5 (page 1)



Deliver and Support DS5
Ensure Systems Security

HIGH-LEVEL CONTROL OBJECTIVE

DS5 Ensure Systems Security
The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Ensure systems security

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

by focusing on

defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Testing security regularly

and is measured by

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties

Primary Secondary

Applications
Information
Infrastructure
People

- Process Description
- IT Domains & Information Indicators
- IT Goals
- Process Goals
- Key Practices
- Key Metrics
- IT Governance & IT Resource Indicators

Example of CobiT® 4.0 - DS5 (page 2)

DS5 Deliver and Support
Ensure Systems Security

Detailed Control Objectives

DS5 Ensure Systems Security

DS5.1 Management of IT Security
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan
Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users.

DS5.3 Identity Management
All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance and Monitoring
Ensure that IT security implementation is tested and monitored proactively. IT security should be reaccredited periodically to ensure the approved security level is maintained. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed. Access to the logging information is in line with business requirements in terms of access rights and retention requirements.

DS5.6 Security Incident Definition
Ensure that the characteristics of potential security incidents are clearly defined and communicated so security incidents can be properly treated by the incident or problem management process. Characteristics include a description of what is considered a security incident and its impact level. A limited number of impact levels are defined and for each the specific actions required and the people who need to be notified are identified.

DS5.7 Protection of Security Technology
Ensure that important security-related technology is made resistant to tampering and security documentation is not disclosed unnecessarily, i.e., it keeps a low profile. However, do not make security of systems reliant on secrecy of security specifications.

DS5.8 Cryptographic Key Management
Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

DS5.9 Malicious Software Prevention, Detection and Correction
Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).

DS5.10 Network Security
Ensure that security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to authorise access and control information flows from and to networks.

DS5.11 Exchange of Sensitive Data
Ensure sensitive transaction data are exchanged only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

Detailed Control Objectives

COBIT® Management Guidelines

COBIT 3rd Edition added a *Management* and *Governance* layer, providing management with a toolbox containing…

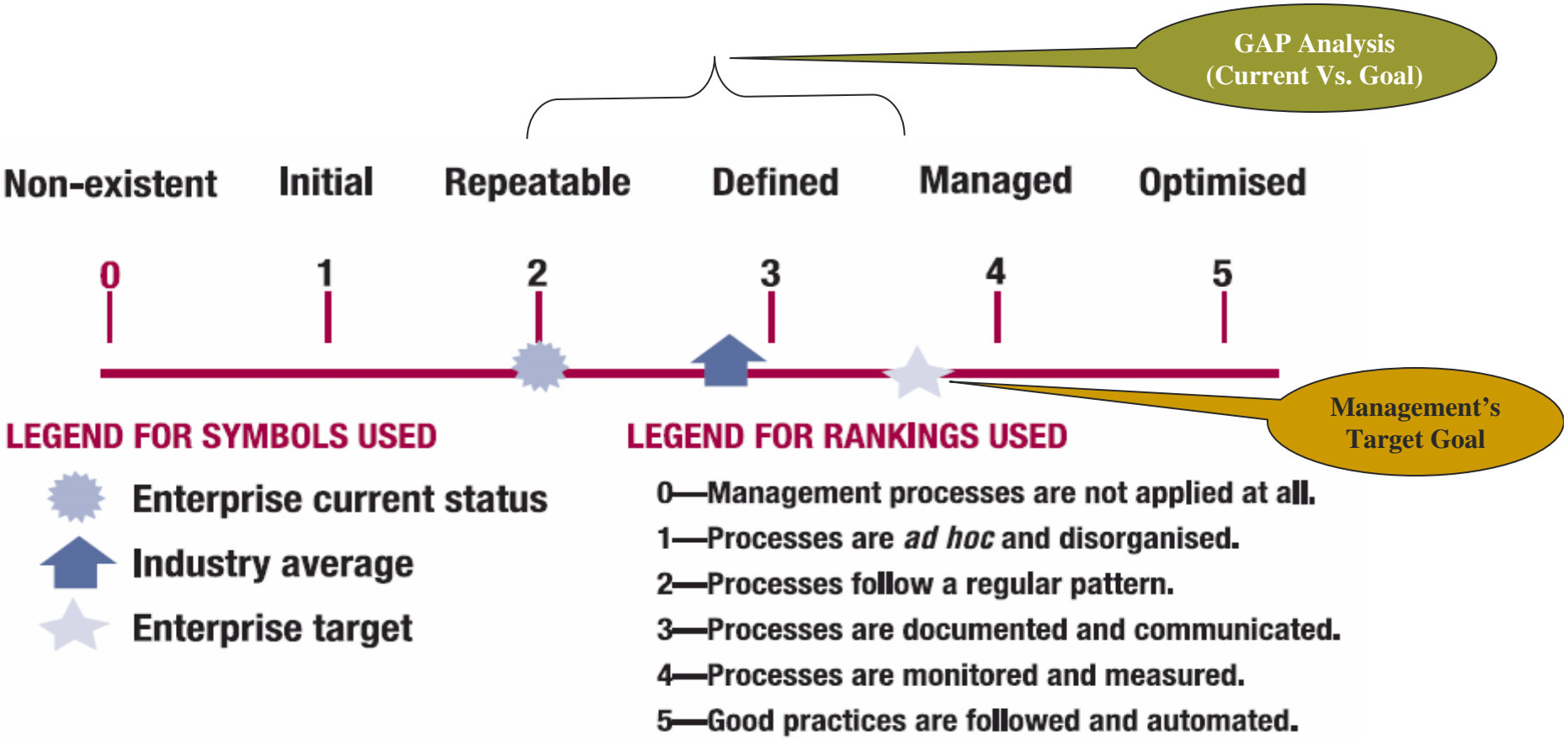
- A *maturity model* to assist in benchmarking and decision-making for control over IT
- A list of *critical success factors (CSF)* that provides succinct non-technical best practices for each IT process
- Generic and action oriented *performance measurement* elements (*key performance indicators [KPI]* and *key goal indicators [KGI]* - outcome measures and performance drivers for all IT processes)

Purpose…

- **IT Control profiling – what is important?**
- **Awareness – where is the risk?**
- **Benchmarking - what do others do?**

COBIT® Maturity Model

Maturity Model: Method of scoring the maturity of IT processes…



Metrics as CSF, KPI, & KGI

- **Critical Success Factors (CSF)**

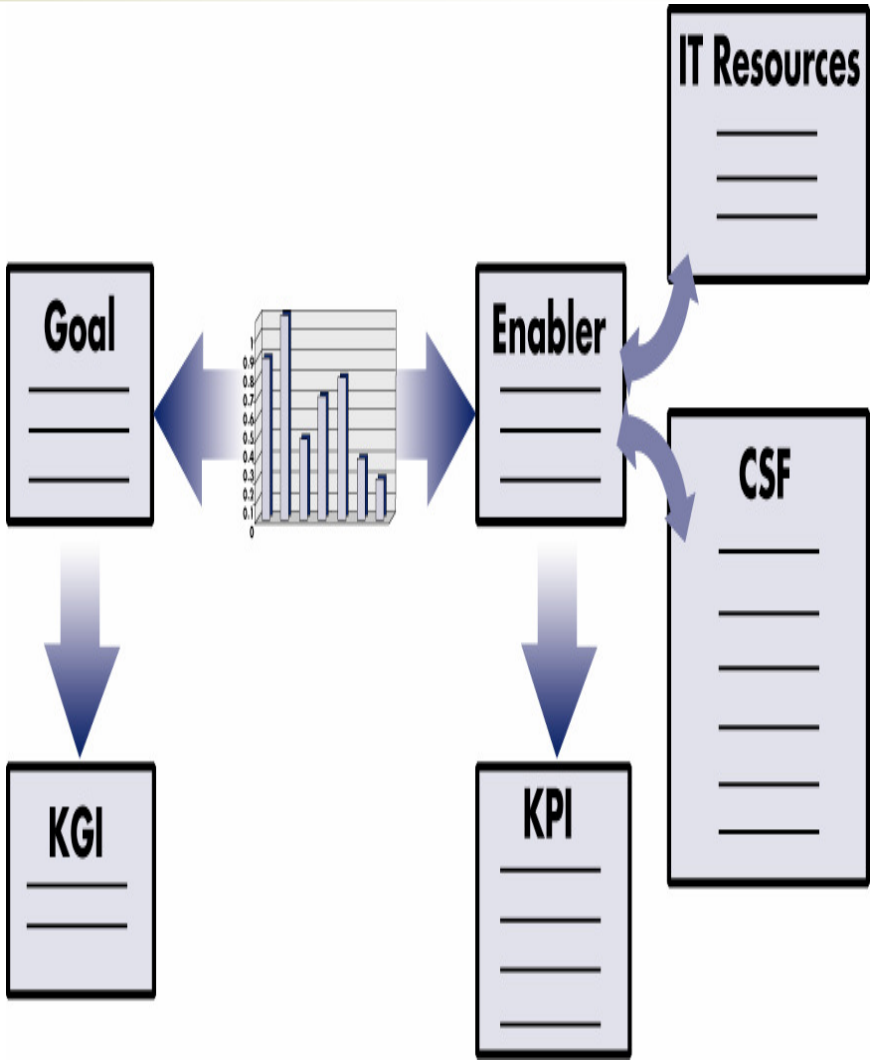
  What are the most important things to do to increase the probability of success of the process?

- **Key Performance Indicators (KPI)**

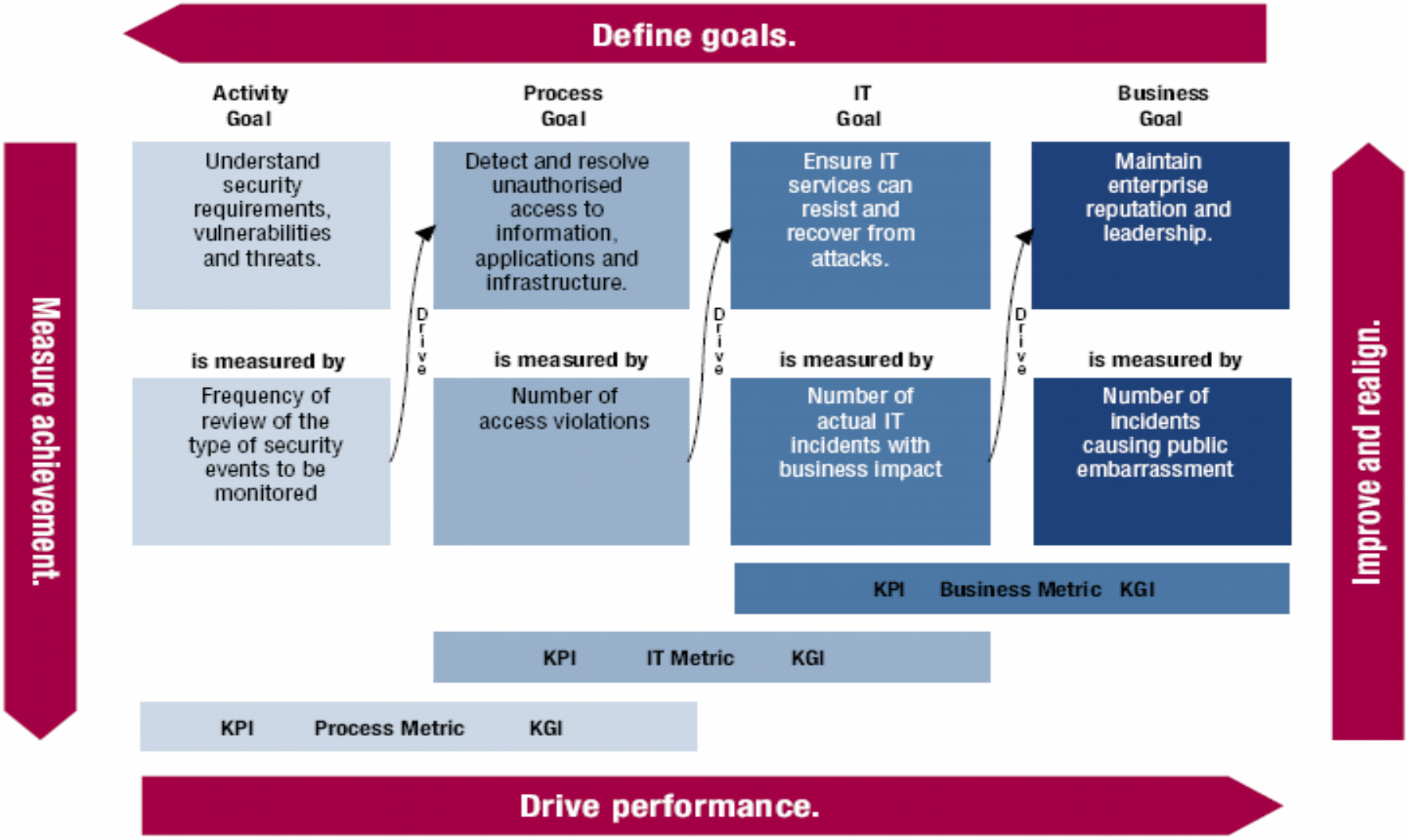
  Measure how well a process is performing.

- **Key Goal Indicators (KGI)**

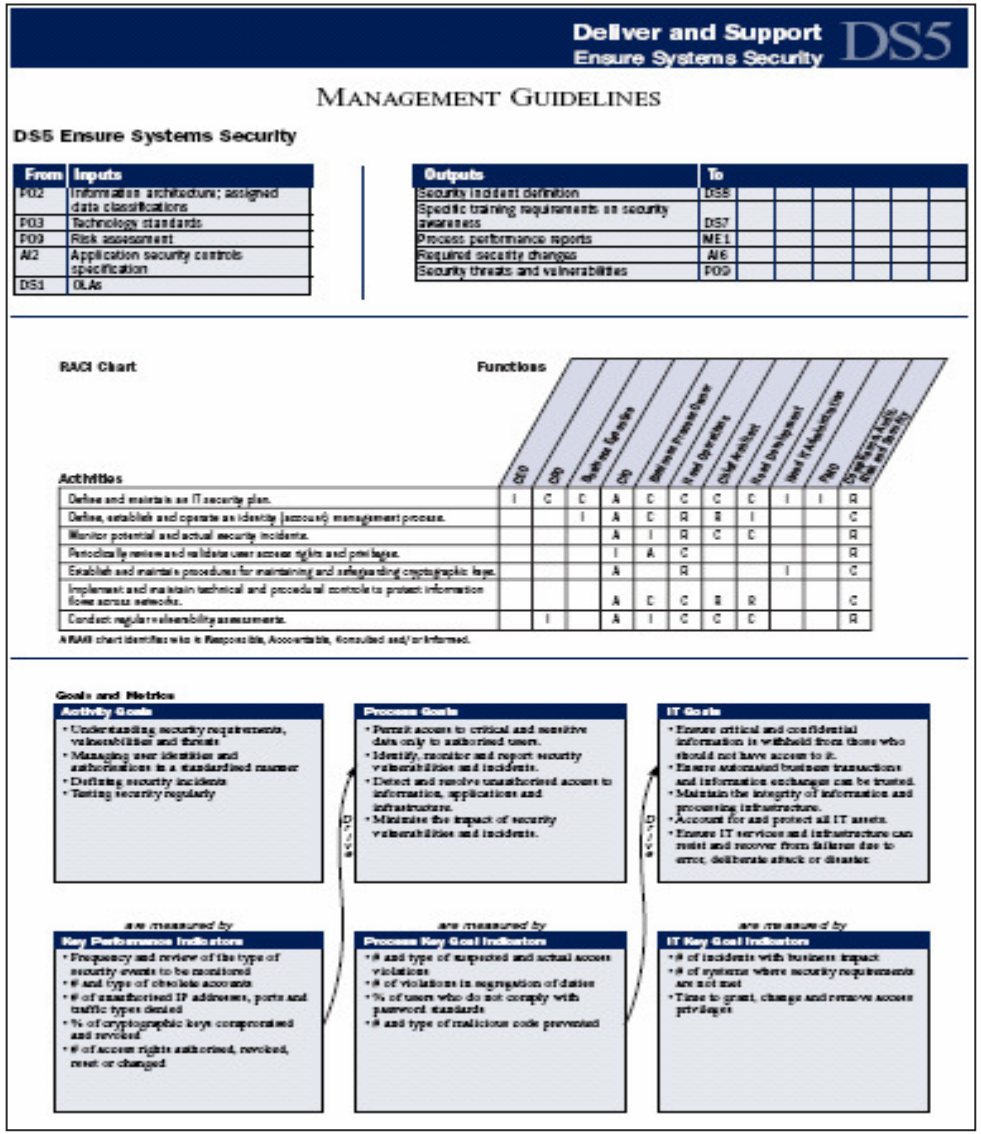
  Measure whether a process achieved its business requirements.



Measuring Success – Example of COBIT® DS5



Example of COBIT® 4.0 - DS5 (page 3)



Deliver and Support
Ensure Systems Security DS5

MANAGEMENT GUIDELINES

DS5 Ensure Systems Security

From	Inputs
PO2	Information architecture; assigned data classifications
PO3	Technology standards
PO9	Risk assessment
AI2	Application security controls specification
DS1	OLAs

Outputs	To
Security incident definition	DS8
Specific training requirements on security awareness	DS7
Process performance reports	ME1
Required security changes	AI6
Security threats and vulnerabilities	PO9

RACI Chart — Functions

Activities	CEO	CIO	Business Process Owner	Chief Operating Officer	Business Executive	Chief Architect	Head Development	Head IT Administration	PMO	Chief Information Security Officer
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Goals and Metrics

Activity Goals
- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorizations in a standardized manner
- Defining security incidents
- Testing security regularly

Process Goals
- Permit access to critical and sensitive data only to authorized users.
- Identify, monitor and report security vulnerabilities and incidents.
- Detect and resolve unauthorized access to information, applications and infrastructure.
- Minimize the impact of security vulnerabilities and incidents.

IT Goals
- Ensure critical and confidential information is withheld from those who should not have access to it.
- Ensure automated business transactions and information exchanges can be trusted.
- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.

are measured by

Key Performance Indicators
- Frequency and review of the type of security events to be monitored
- # and type of obsolete accounts
- # of unauthorized IP addresses, ports and traffic types denied
- % of cryptographic keys compromised and revoked
- # of access rights authorized, revoked, reset or changed

are measured by

Process Key Goal Indicators
- # and type of suspected and actual access violations
- # of violations in segregation of duties
- % of users who do not comply with password standards
- # and type of malicious code prevented

are measured by

IT Key Goal Indicators
- # of incidents with business impact
- # of systems where security requirements are not met
- Time to grant, change and remove access privileges

Process Relationships

RACI Chart
(Major activities and associated responsibilities)

IT Goals & Performance Metrics

Example of COBIT® 4.0 - DS5 (page 4)

DS5 Deliver and Support
Ensure Systems Security

MATURITY MODEL

DS5 Ensure Systems Security

Management of the process of *Ensure systems security* that satisfies the business requirements for IT of *maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents* is:

0 Non-existent when
The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/*Ad Hoc* when
The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when
Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see that IT security is within its domain.

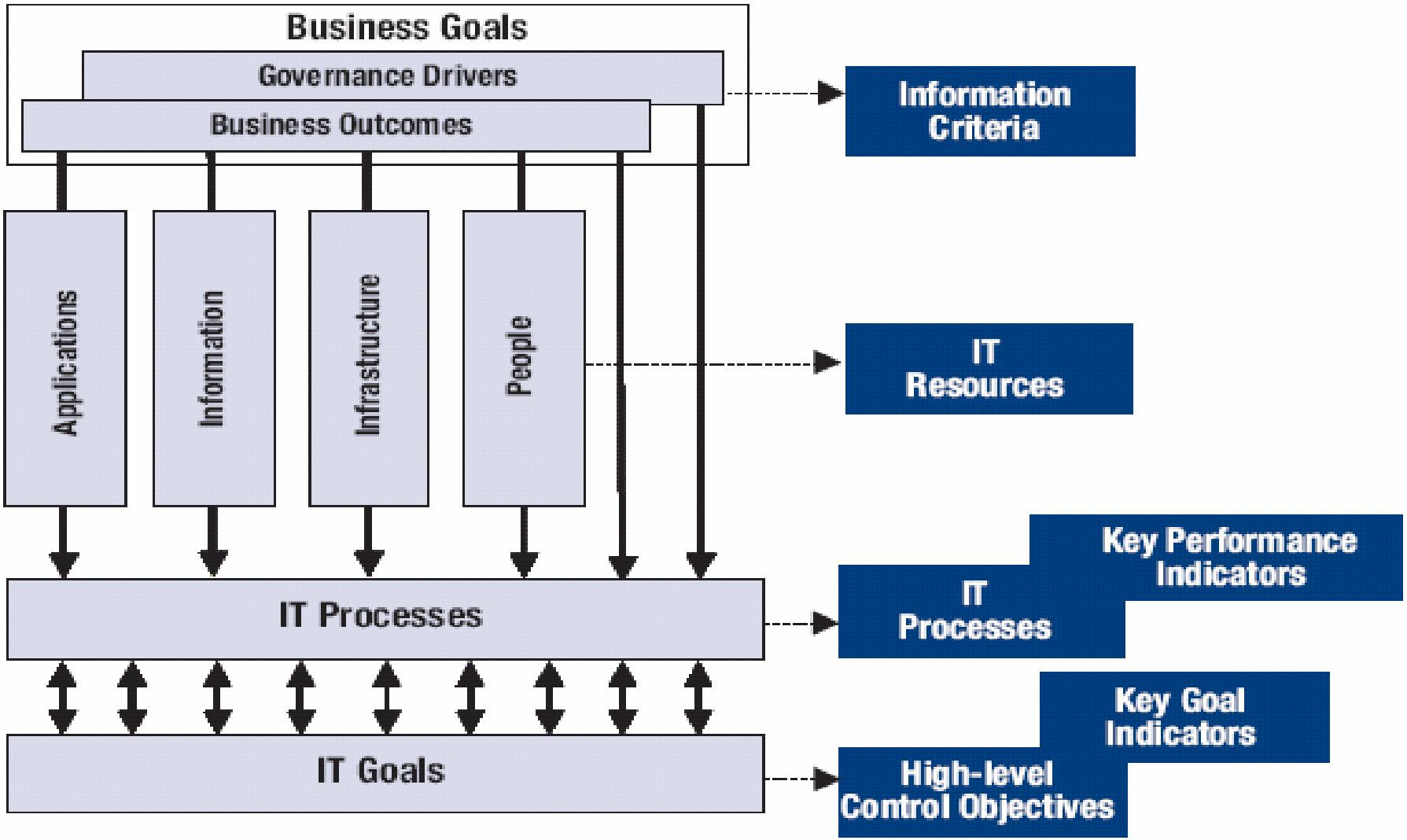
3 Defined Process when
Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. *Ad hoc* security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business but is only informally scheduled and managed.

4 Managed and Measurable when
Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff who are responsible for the audit and management of security. Security testing is done using standard and formalised processes leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. KGIs and KPIs for security management have been defined but are not yet measured.

5 Optimised when
IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. KGIs and KPIs for security management are collected and communicated. Management uses KGIs and KPIs to adjust the security plan in a continuous improvement process.

Process Specific Maturity Model

Summing It All Up
Business Goals Drive IT Goals



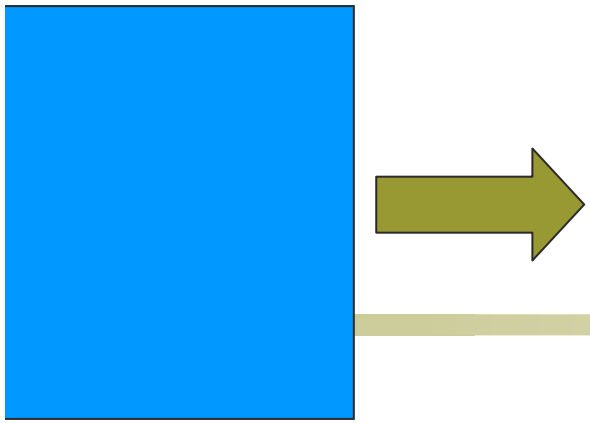
Integrating COBIT® Domains Into IT Audit Planning & Scope Development

Integration Overview

Integrating COBIT Into IT Audit Approach

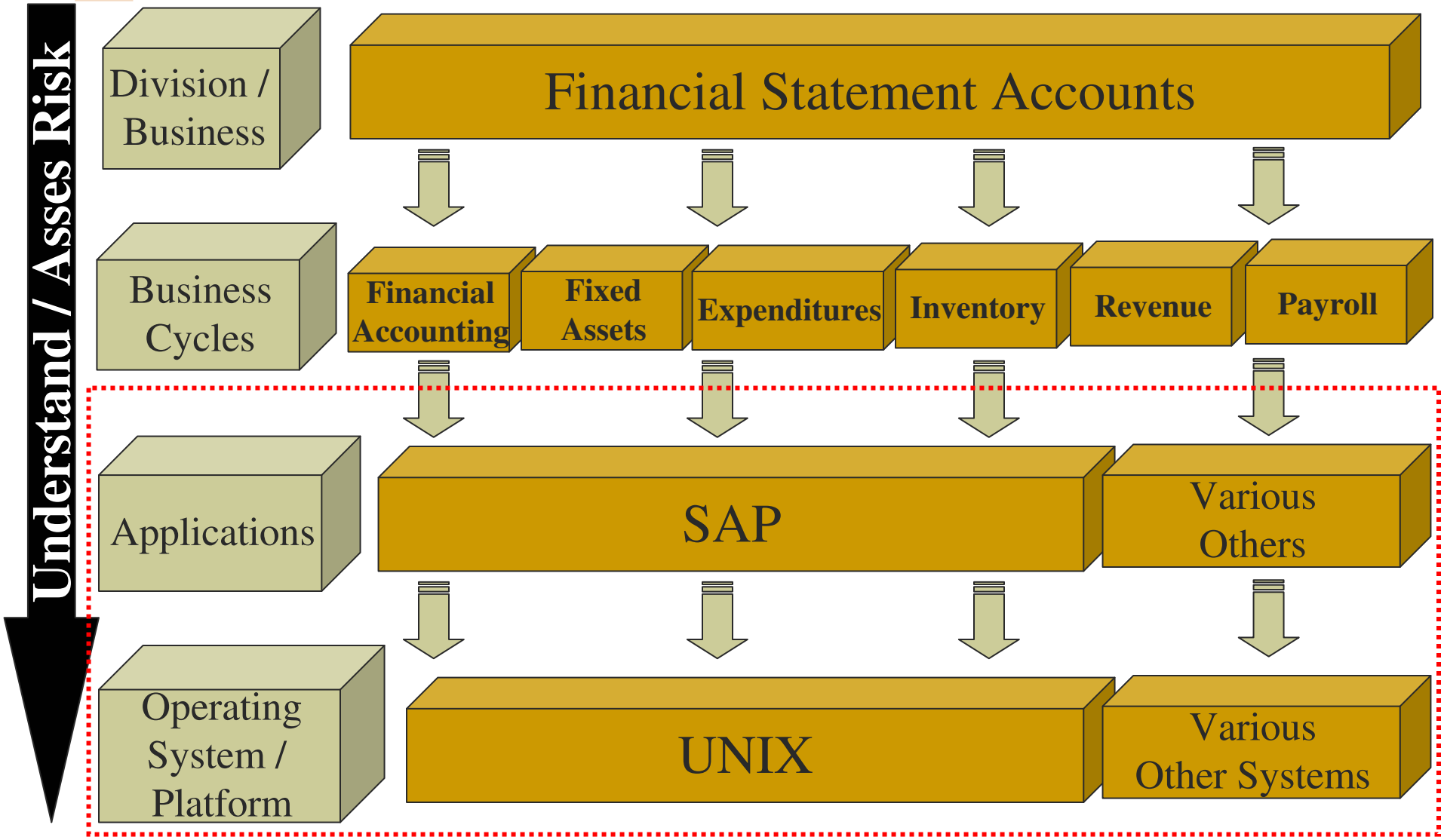
- ***Map COBIT to the Technology Audit Universe***
- ***Ensure Consistent Audit Coverage By Establishing IT Audit Focal Points***
- ***Map COBIT to Relevant Regulatory, Industry, and Technology Specific Standards / Guidelines /Best Practice and the Organization's IT Policies, Standards, Guidelines, and Procedures***
- ***Integrate COBIT Into the IT Audit Lifecycle***
  - ***Map COBIT to the Annual and Rotational Audit Plans***
  - ***Develop Work Programs (Supplement Existing Work Programs With COBIT Audit Guidelines)***
  - ***Joint Risk Self-Assessments***
  - ***Analyze, Document, Validate Results***
  - ***Report To Management***
- ***Use COBIT To Establish IT Risk & Control Measurement***

ISACA®
Serving IT Governance Professionals

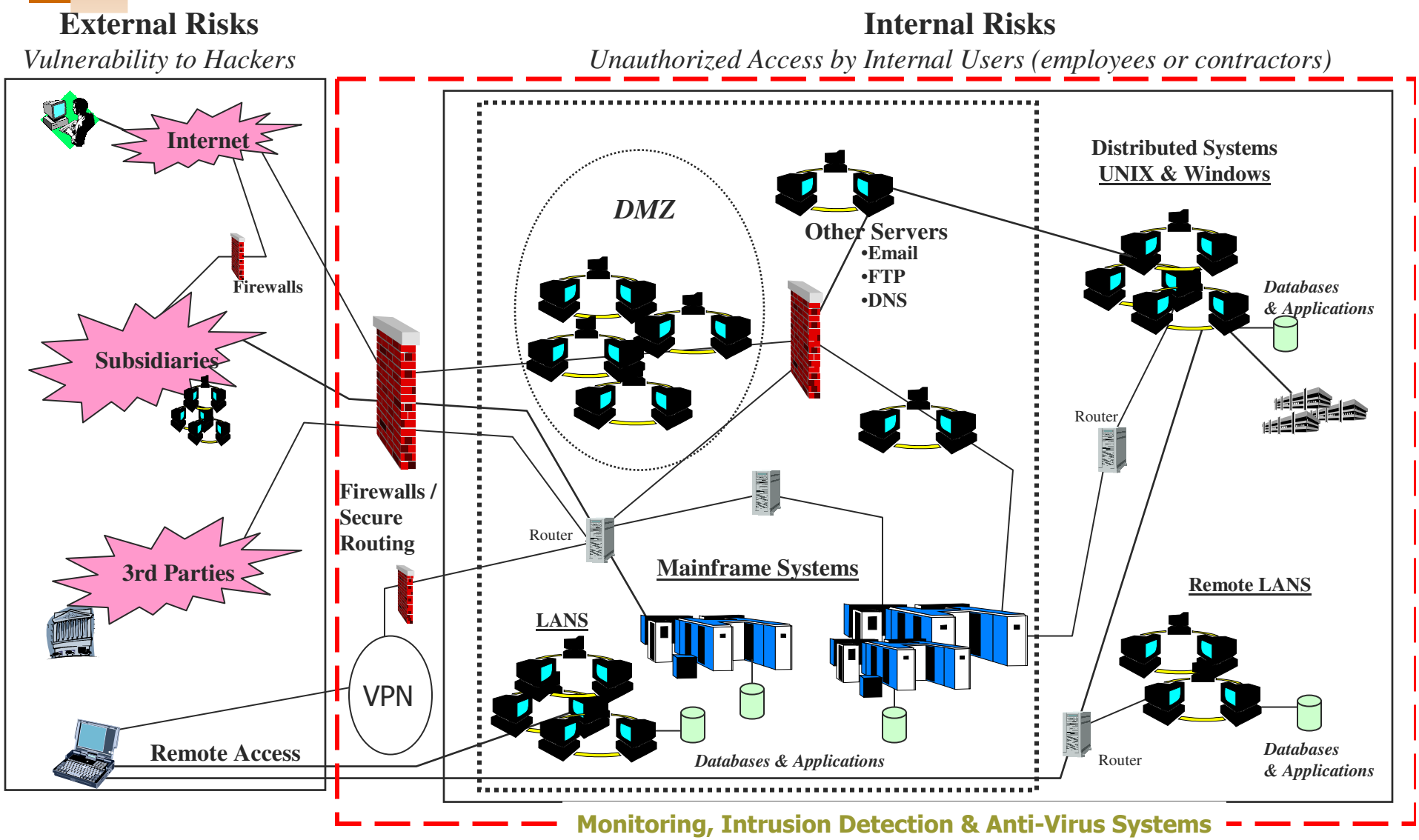


Mapping COBIT® to the *Technology Audit Universe*

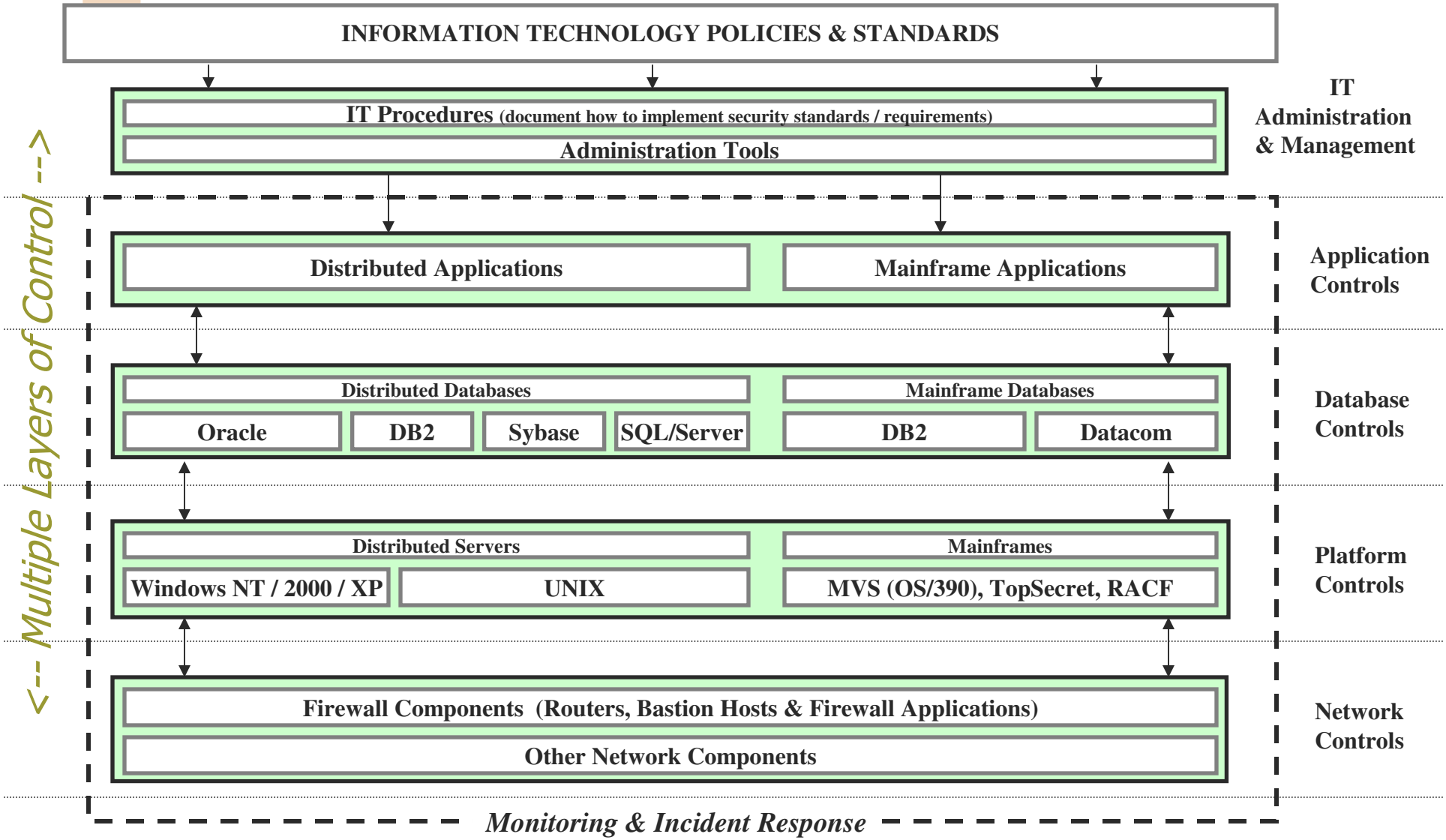
Drilling Down to the Technology Infrastructure



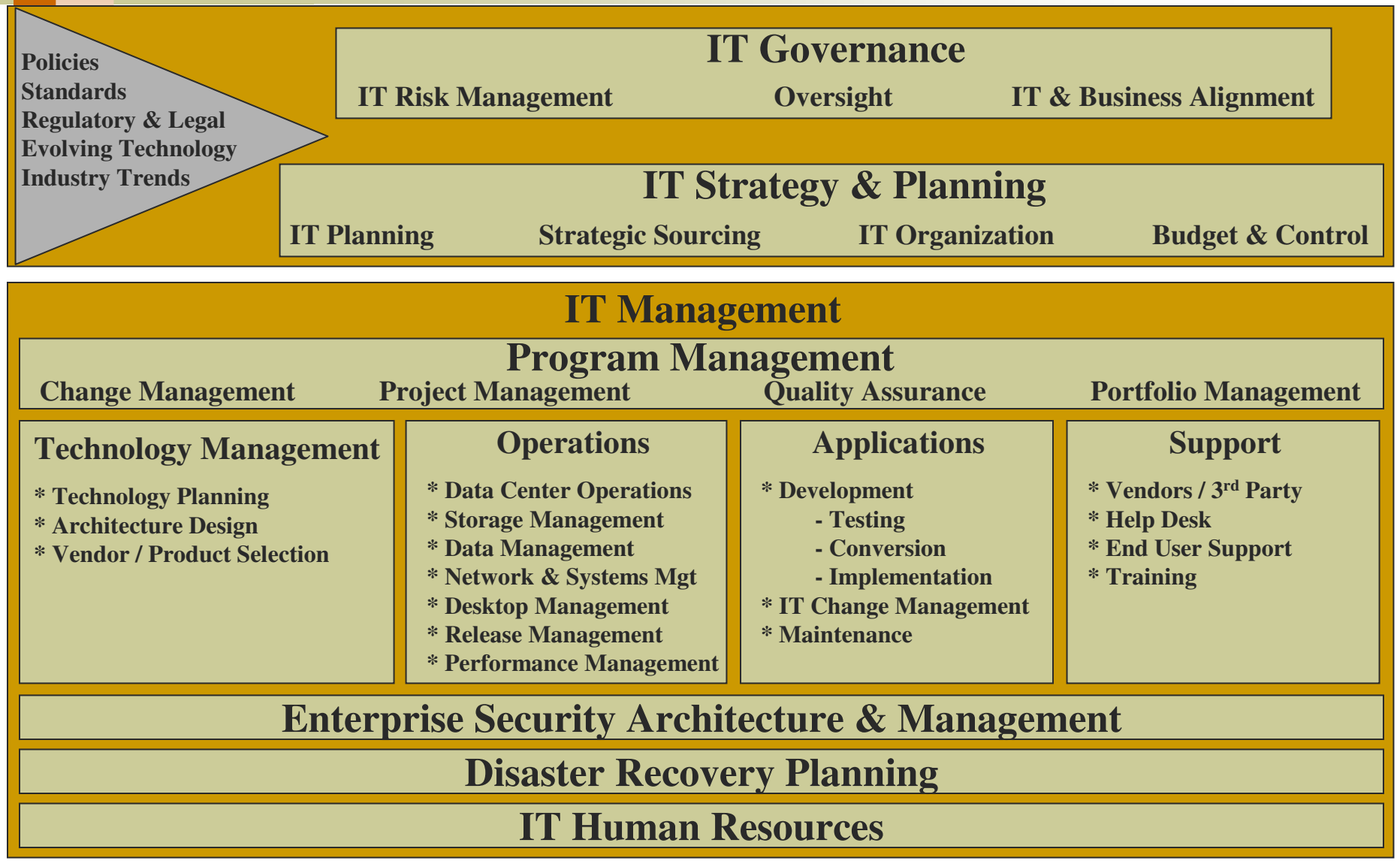
Understanding the Technology Infrastructure



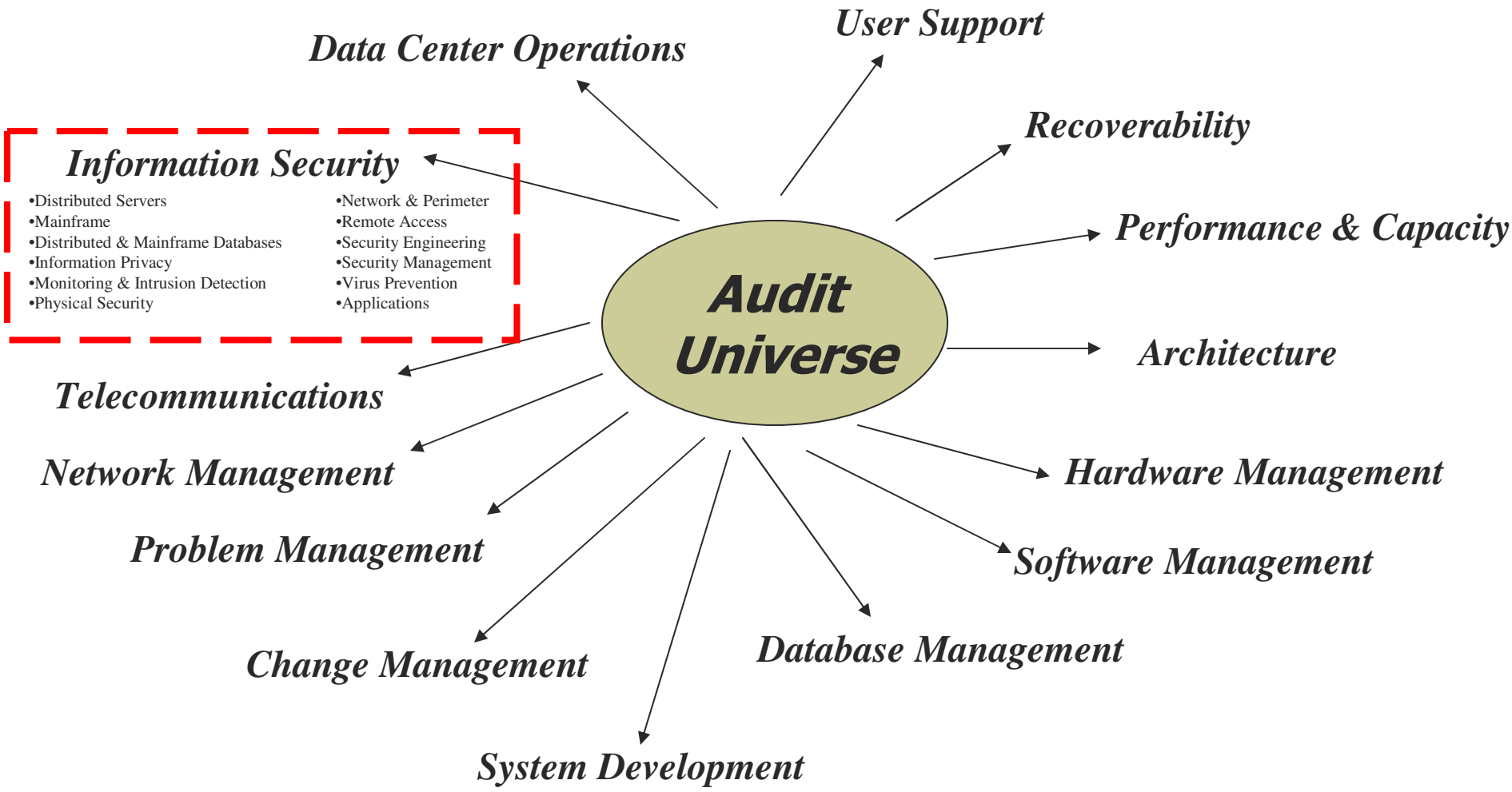
Identifying Relevant Technology "Layers"



Understanding the IT Governance Framework



Defining the *Technology Audit Universe*



Security Audit Universe

Information Security

- •Distributed Servers
- •Mainframe
- •Distributed & Mainframe Databases
- •Information Privacy
- •Monitoring & Intrusion Detection
- •Physical Security
- •Network & Perimeter
- •Remote Access
- •Security Engineering
- •Security Management
- •Virus Prevention
- •Applications

Mainframe Security
•O/S (OS/390)
•Security Systems (Top Secret / RACF)
•Sub-systems (CICS, TSO, IMS DC, MQ)
•Mainframe Databases (DB2, Datacom)

Distributed Server Security
•UNIX (Solaris, AIX, HP-UX)
•Windows NT / 2000 / XP
•Netware

Network & Perimeter Security
•Firewalls
•Subsidiary Connectivity
•3rd Party Connectivity

Distributed Database Security
•DB2 6000
•Oracle
•SQL/Server
•Sybase

Remote Access Security
•VPNs
•Modem Usage
•Other Remote Access Facilities
•Vendor Access

Information Privacy
•Privacy Office Compliance Program

Monitoring & Incident Response
•System Logging & Reporting
•Automated Intrusion Detection Systems (IDS)
•Vulnerability Assessment Process
•Incident Response Program

Virus Prevention
•Anti-Virus Program

Application Security
•ETS Audit Coverage
•System Development Projects

Security Management
•Policy, Standards, & Procedures Maintenance Process
•Security Awareness Program
•Security Metrics & Performance Reporting

Security Engineering
•Research & Development
•Security Self-Assessments

Physical Security

Map Audit Universe To COBIT®

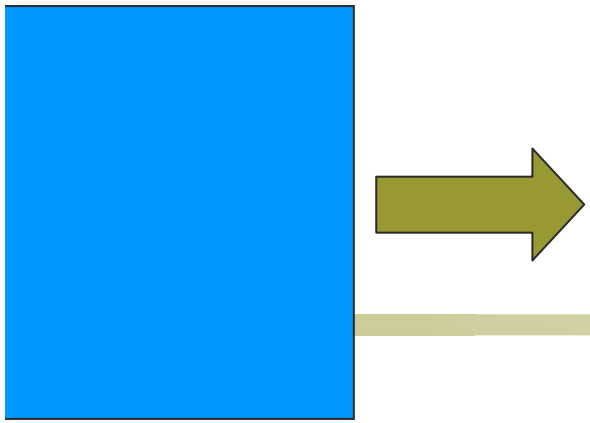
High Level Objective (e.g. PO2)

Ref.	COBIT Domains & High-Level Control Objectives	Infrastructure Audit Universe													Security Audit Universe											
		Architecture	Change Management	Data Center Operations	Database Management	Hardware Management	Network Management	Performance & Capacity	Problem Management	Recoverability	Software Management	Telecom. Management	User Support	Database	Distributed Server	Information Privacy	Monitoring & IDS	Mainframe	Network & Perimeter	Remote Access	Engineering	Management	Virus Prevention	Physical Security
	PLANNING & ORGANIZATION																								
PO1	Define a Strategic IT Plan	X								X												X			
PO2	Define the Information Architecture	X																			X	X			
PO3	Determine the Technological Direction	X																			X	X			
PO4	Define the IT Organization and Relationships	X																							
PO5	Manage the Information Technology Investment	X																							
PO6	Communicate Management Aims and Direction	X								X												X			
PO7	Manage Human Resources	X																				X			
PO8	Ensure Compliance with External Requirements	X								X											X	X			
PO9	Assess Risks	X								X											X	X			
PO10	Manage Projects																				X				
PO11	Manage Quality			X	X	X	X	X			X	X	X												
	ACQUISITION & IMPLEMENTATION																								
AI1	Identify Automated Solutions			X	X		X			X	X	X									X				
AI2	Acquire and Maintain Application Software		X																		X				
AI3	Acquire and Maintain Technology Infrastructure			X	X	X	X														X				
AI4	Develop and Maintain Procedures	X	X	X	X		X			X	X	X									X				
AI5	Install and Accredit Systems			X	X																X				
AI6	Manage Changes		X	X	X	X	X				X	X									X				
	DELIVERY & SUPPORT																								
DS1	Define and Manage Service Levels		X	X	X	X	X			X	X	X	X								X				
DS2	Manage Third-Party Services			X	X	X	X				X	X									X				
DS3	Manage Performance & Capacity						X	X				X					X								
DS4	Ensure Continuous Service			X	X	X	X	X		X	X	X					X								
DS5	Ensure System Security											X		X	X	X	X	X	X	X			X	X	
DS6	Identify & Allocate Costs				X		X					X									X				

Applicable Objectives Noted With 'X'

Illustration Only

ISACA®
Serving IT Governance Professionals



Ensuring Consistent Coverage

IT Audit Focal Points

Audit Focal Points

Audit Focal Points
ensure consistent coverage across audits and allow for trending the "state of controls" over time.

Infrastructure

- **Strategy & Structure**
- **Methodologies & Procedures**
- **Measurement & Reporting**
- **Tools & Technology**

Information Security

- **Access Control**
- **System Security Configuration**
- **Monitoring, Vulnerability Assessment, & Response**
- **Security Management & Administration**

Example

Security Audit Focal Points / Areas of Emphasis
(Example)

Access Control

Standards & Procedures
Standards and procedures for access control are documented, approved, and communicated.

Account Management
Account management procedures exists and are effective.

Password Management
Password management mechanisms are in place to ensure that user passwords comply with Schwab password syntax and management criteria.

User Profile Configurations
User profile configurations are defined based on job responsibilities.

Group Profile Configurations
Group profile configurations are defined to ensure consistent access by users performing similar job responsibilities.

Privileged & Special User Accounts
Privileged and Special User accounts are authorized and restricted.

Generic & Shared Accounts
Generic & Shared accounts are not used as per Schwab standards.

Logon / Logoff Processes
Systems should be configured to lock after consecutive invalid attempts.

System Boot Process
System boot process is configured to ensure that only authorized security settings and system services are initiated during the system boot / IPL process.

Remote Access
Appropriate mechanisms are in place to control and monitor remote user access to Schwab's internal network.

Resource Safeguards (File/Dataset & Directory/Volume Protection)
System level security has been configured to appropriately protect critical system resources (files/datasets, directories/volumes, applications, etc.).

System Security Configuration

Standards
Standards for secure platform configuration are documented, approved, and communicated.

Configuration Management
Procedures are in place to facilitate an effective configuration management process for standard images, patches and other updates. Procedures are in place for handling exceptions for non-standard configurations.

Procedures
Defined procedures exist to ensure that systems are configured in compliance with Schwab security standards. The procedures are tested, documented and approved by management.

System Security Parameters
Systems are configured with security parameters consistent with corporate standards.

System Utilities
System utilities are managed effectively.

Monitoring, Vulnerability Assessment & Response

Standards & Procedures
Formal standards and procedures for monitoring and incident response are documented, approved and communicated.

Logging
Critical system and security events are logged according to logging standards.

Reporting & Review
Reports are produced and reviewed by management periodically.

Incident Response
Security incident response procedures exist and are applied consistently in an event of a security breach. Escalation protocols have been defined.

Security Management & Administration

Security Program Strategy
Overall security strategy and direction has been established and communicated.

Security Policy & Standards
Overall security policy and standards are documented, approved and communicated.

Procedures
Daily operational procedures have been defined, documented and communicated to ensure that individuals with administrative responsibilities are able to effectively execute standard administration procedures.

Roles, Responsibilities, & Staffing
Roles and responsibilities have been defined, documented and communicated to ensure that individuals are informed of their responsibilities.

User Education & Awareness
Awareness and education programs have been established to ensure that users are aware of appropriate corporate security policy and standards.

Security Advisories & Alerts
Industry security advisories and alerts should be closely monitored to ensure that appropriate mitigating controls are in place for identified vulnerabilities / exposures.

Security Administration
Responsibility for security administration is appropriately assigned and accountability has been established.

Environment Understanding
Gain a comprehensive understanding of the computer-processing environment and the relevant controls in place.

Security Audit Focal Points
ensure consistent coverage across audits and allow for trending the "state of security" over time.

Map Focal Points / Areas of Emphasis to COBIT®
(Example)

Access Control

Standards & Procedures
Standards and procedures for access control are documented, approved, and communicated.

Account Management
Account management procedures exists and are effective.

Password Management
Password management mechanisms are in place to ensure that user passwords comply with Schwab password syntax and management criteria.

User Profile Configurations
User profile configurations are defined based on job responsibilities.

Group Profile Configurations
Group profile configurations are defined to ensure consistent access by users performing similar job responsibilities.

Privileged & Special User Accounts
Privileged and Special User accounts are authorized and restricted.

Generic & Shared Accounts
Generic & Shared accounts are not used as per Schwab standards.

Logon / Logoff Processes
Systems should be configured to lock after consecutive invalid attempts.

System Boot Process
System boot process is configured to ensure that only authorized security settings and system services are initiated during the system boot / IPL process.

Remote Access
Appropriate mechanisms are in place to control and monitor remote user access to Schwab's internal network.

Resource Safeguards (File/Dataset & Directory/Volume Protection)
System level security has been configured to appropriately protect critical system resources (files/datasets, directories/volumes, applications, etc.).

Record Applicable Focal Points & Areas of Emphasis

Detailed Objectives

Ref.	COBIT Domains & Control Objectives	COBIT Control Objectives (with "X")
	PLANNING & ORGANIZATION	
PO1	**Define a Strategic IT Plan**	
1.1	IT as Part of the Organization's Long- and Short-Range Plan	
1.2	IT Long-Range Plan	
1.3	IT Long-Range Planning, Approach & Structure	
1.4	IT Long-Range Plan Changes	
1.5	Short-Range Planning for the IT Function	
1.6	Communication of IT Plans	
1.7	Monitoring & Evaluating of IT Plans	
1.8	Assessment of Existing Systems	
PO2	**Define the Information Architecture**	
2.1	Information Architecture Model	
2.2	Corporate Data Dictionary & Data Syntax Rules	
2.3	Data Classification Scheme	
2.4	Security Levels	
PO3	Determine Technological Direction	
3.1	Technological Infrastructure Planning	
3.2	Monitor Future Trends & Regulations	
3.3	Technological Infrastructure Contingency	
3.4	Hardware and Software Acquisition Plans	
3.5	Technology Standards	
PO4	**Define the IT Organization and Relationships**	
4.1	IT Planning or Steering Committee	
4.2	Organizational Placement of the IT Function	
4.3	Review of Organizational Achievements	
4.4	Roles & Responsibilities	

ISACA®
Serving IT Governance Professionals

Mapping COBIT® to Relevant Industry Standards, Guidelines & Best Practices

ITIL®
IT Service Management

COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

NIST

PMI®

Vendor-Specific Guidance

ISO

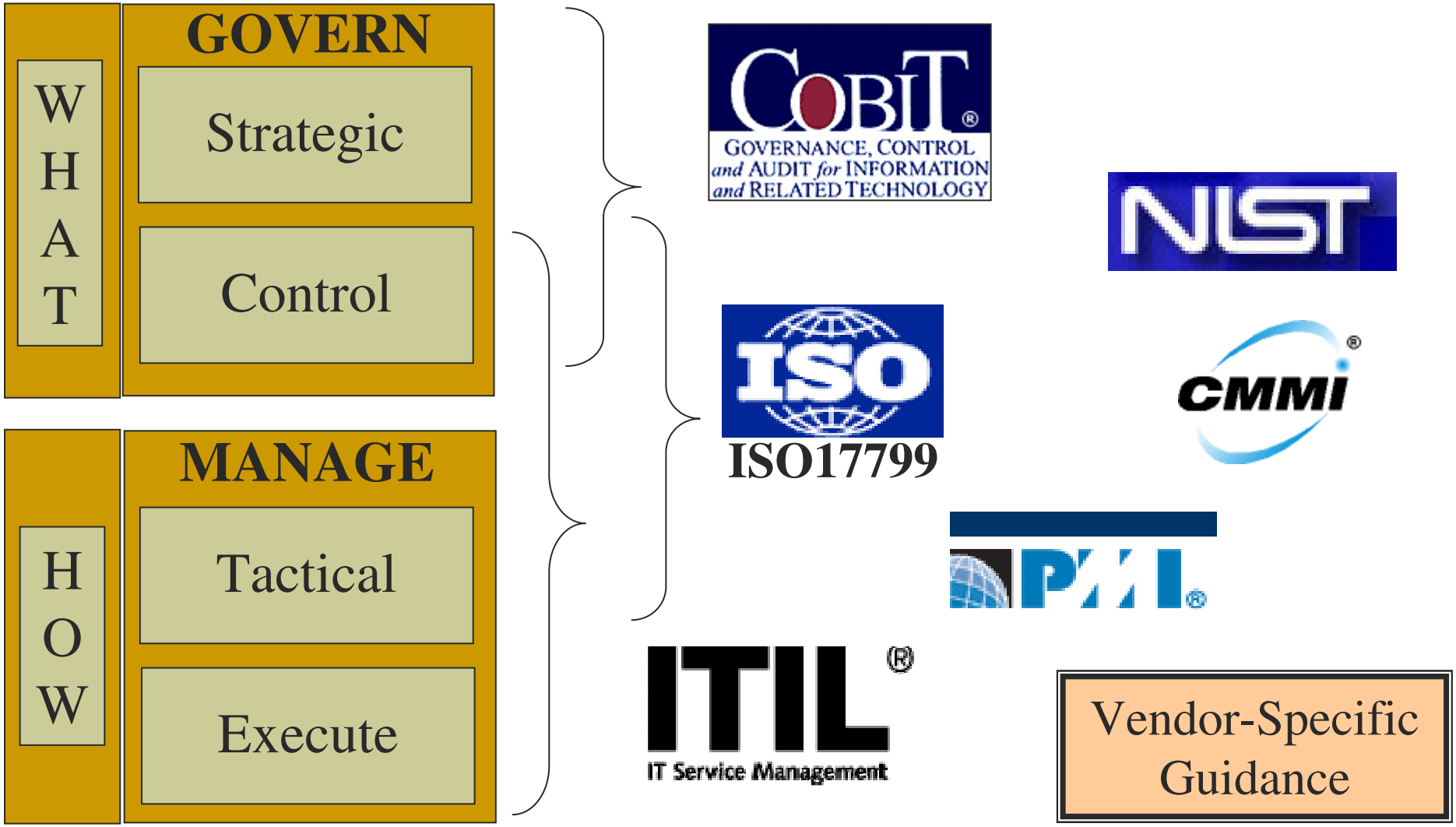
CMMI®

Classifying Sources

Identify relevant industry standards, guidelines, and best practices (classify by purpose)…

- *Governance* (strategic) focus versus *Management* (tactical) focus.
- Process *Control* focus versus process *Execution* focus.
- *What To Do* versus *How To Do IT*

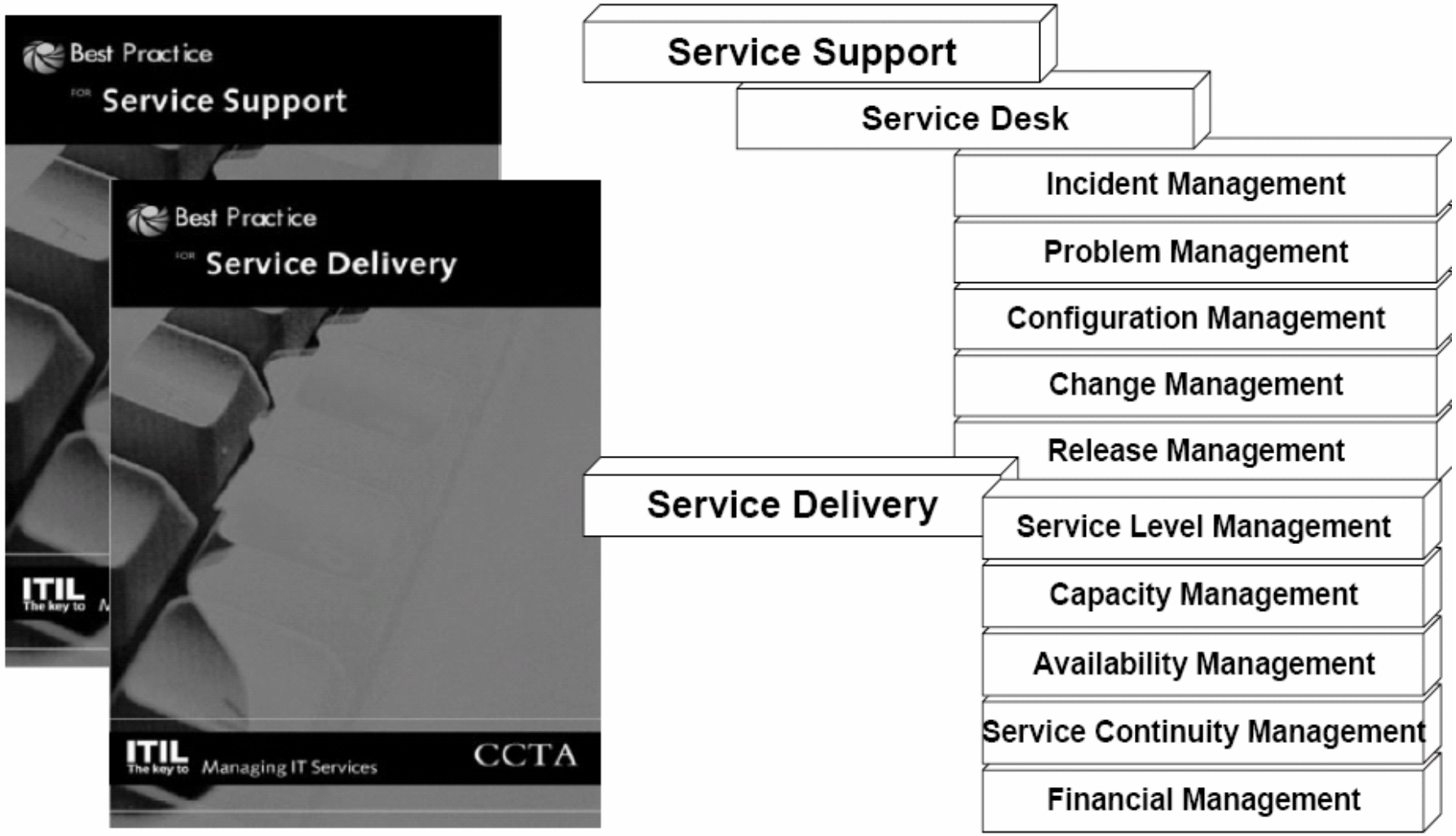
Classification (Example)



ITIL Overview

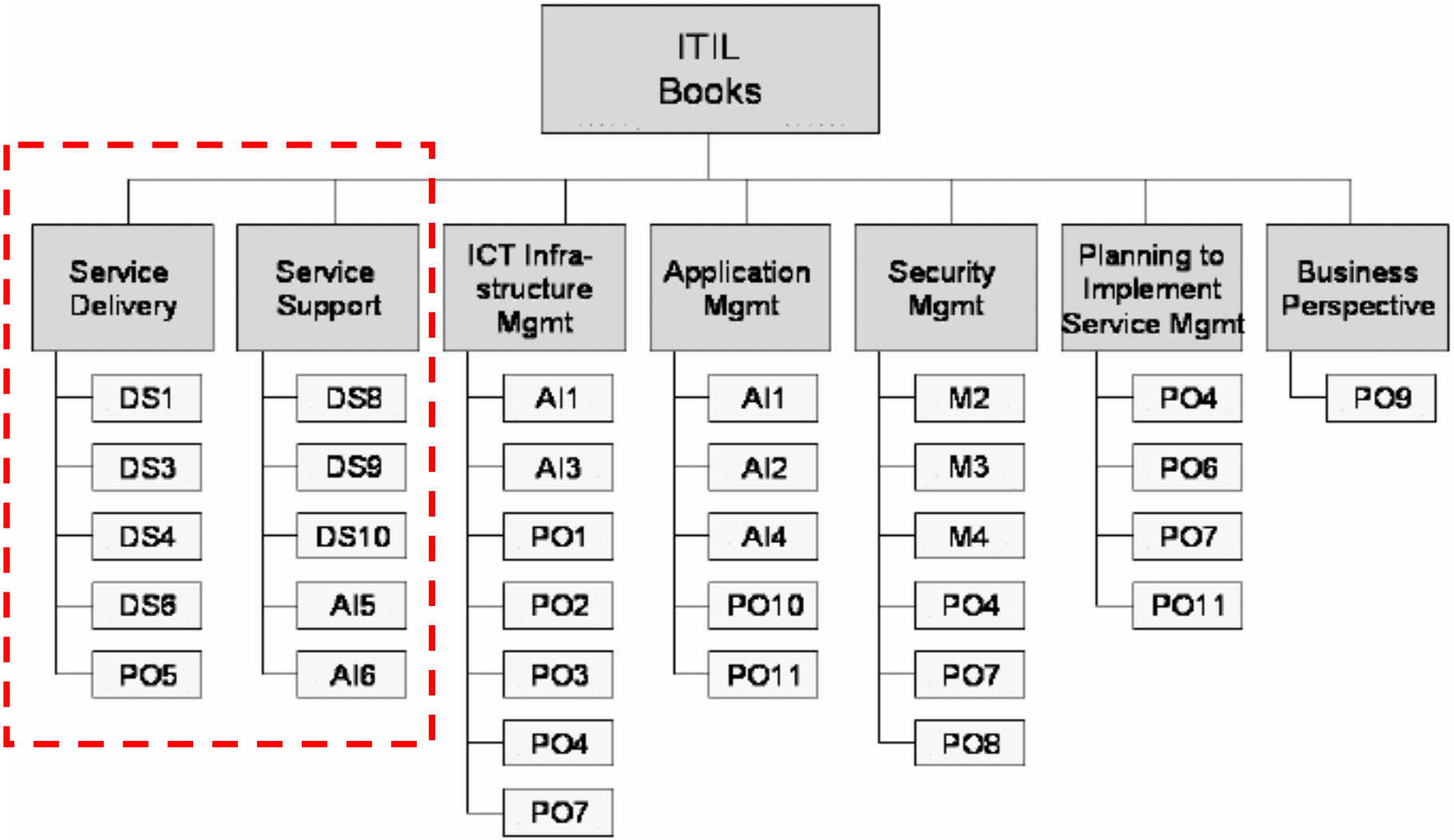
- Information Technology Infrastructure Library (ITIL)
- Set of books detailing best practices for IT Service Management (the ***"how"***)
- Originally developed by the UK government to improve IT Service Management
- Now more globally accepted
- Currently under revision
- www.itil.co.uk

ITIL – The Most Popular Books



Source: 2005 COBIT User Convention

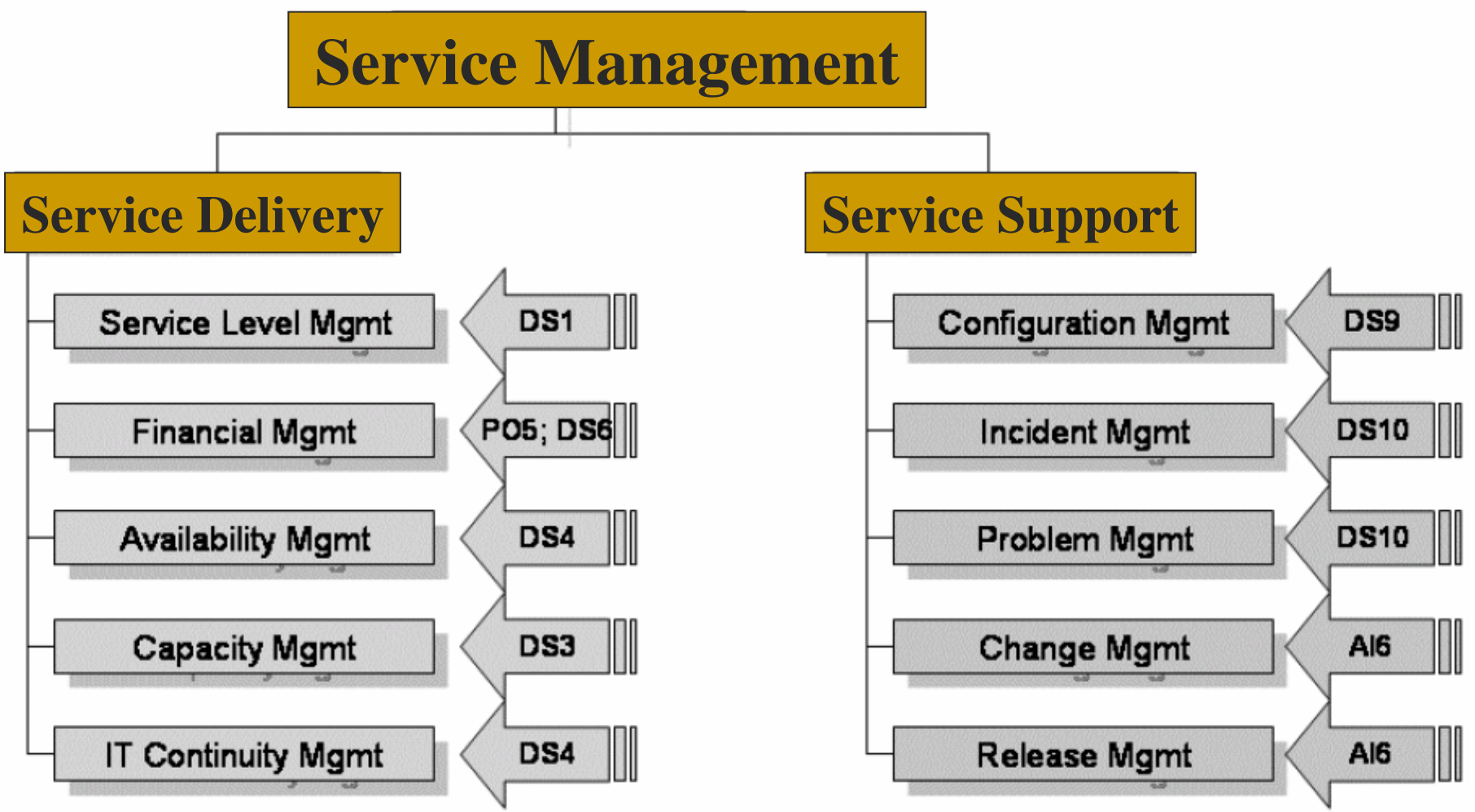
ITIL Mapping To COBIT®



Source: 2005 COBIT User Convention

ITIL Mapping To COBIT®

(continued)



Source: 2005 COBIT User Convention

ISO 17799 Overview

- ISO/IEC 17799:2005
  Code of Practice for Information Security Management
- Established guidelines and general principles for initiating, implementing, maintaining, and improving information security management.
- Objectives outlined provide general guidance on the commonly accepted goals of information security management.
- Updated in 2005
- www.iso.org

ISO 17799 Components

ISO 17799 contains best practices for control objectives and controls in the following areas…

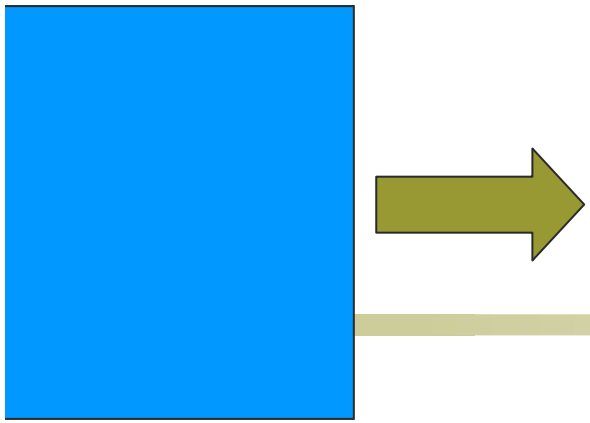
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Aligning COBIT® , ITIL, and ISO 17799

A Management Briefing from ITGI and OGC…

- IT Governance Institute
- Office of Government Commerce.
- Useful guidance for implementing COBIT, ITIL and ISO17799
- Useful mapping of ITIL and ISO17799 to COBIT (3rd edition)
- Available at *ISACA.ORG*
  - Go to *Downloads*
  - Then *COBIT*

ISACA®
Serving IT Governance Professionals



Mapping COBIT® to Organizational IT Policies, Standards, Guidelines & Procedures

Policies, Standards, Guidelines & Procedures

WHAT

IT Policies

Policies:
High-level statements. When there is no specific standard to follow, policies provide general guidance.

IT Standards

Standards:
Standards establish a point of reference, providing criteria that may be used to measure the accuracy and effectiveness of procedures / mechanisms that are in place.

HOW

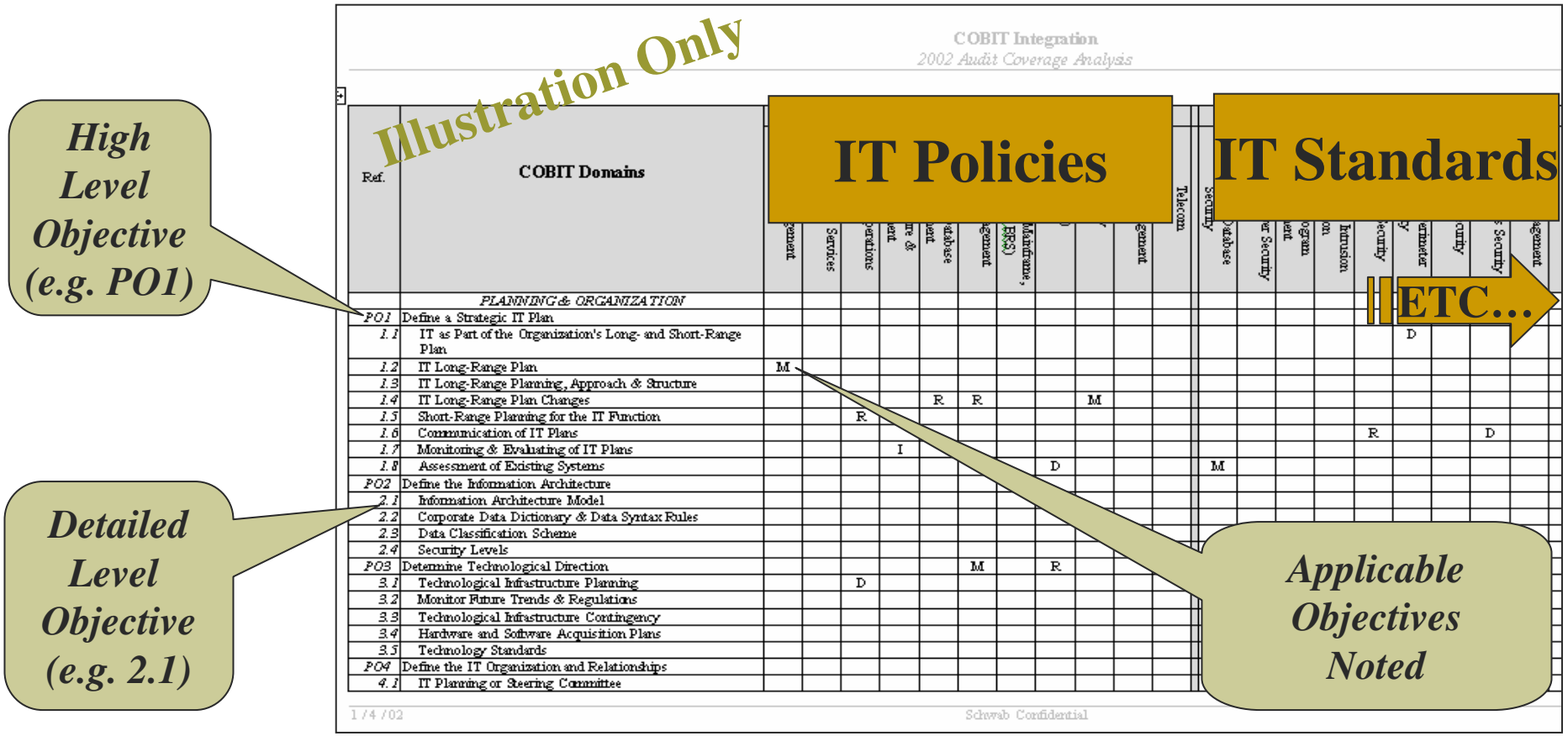
IT Guidelines

Guidelines:
Guidelines provide specific and detailed requirements relative to implementing specific IT standards (i.e., platform specific; function specific; component specific, etc.).

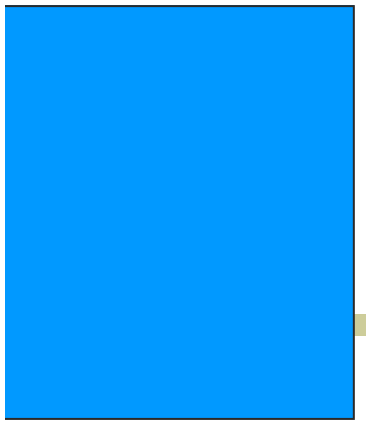
IT Procedures

Procedures:
Procedures provide step-by-step instructions for end-users and technical staff for the execution of specific IT processes.

Map COBIT® To IT Policies, Standards, Guidelines & Procedures



ISACA®
Serving IT Governance Professionals



Integrating COBIT® Into the *IT Audit Lifecycle*

IT Audit Approach Overview

COBIT Manuals & Other Best Practice Material

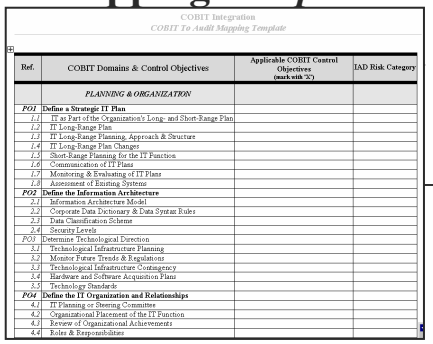
1

Audit Planning Session

Audit Team

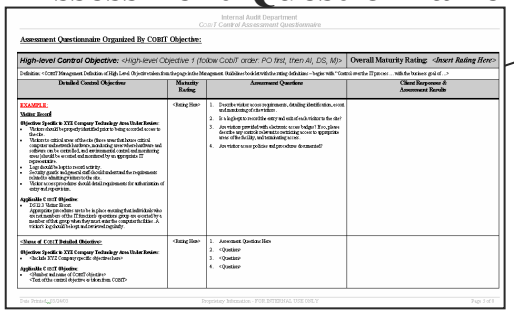
2

COBIT To Audit Mapping *Template*



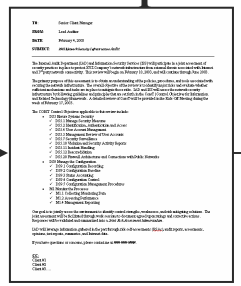
Ref.	COBIT Domains & Control Objectives	Applicable COBIT Control Objectives (mark with 'X')	IAD Risk Category
	PLANNING & ORGANIZATION		
PO1	**Define a Strategic IT Plan**		
1.1	IT as Part of the Organization's Long- and Short-Range Plan		
1.2	IT Long-Range Plan		
1.3	IT Long-Range Planning, Approach & Structure		
1.4	IT Long-Range Plan Changes		
1.5	Short-Range Planning for the IT Function		
1.6	Communication of IT Plans		
1.7	Monitoring & Evaluating of IT Plans		
1.8	Assessment of Existing Systems		
PO2	**Define the Information Architecture**		
2.1	Information Architecture Model		
2.2	Corporate Data Dictionary & Data Syntax Rules		
2.3	Data Classification Scheme		
2.4	Security Levels		
PO3	Determine Technological Direction		
3.1	Technological Infrastructure Planning		
3.2	Monitor Future Trends & Regulations		
3.3	Technological Infrastructure Contingency		
3.4	Hardware and Software Acquisition Plans		
3.5	Technology Standards		
PO4	**Define the IT Organization and Relationships**		
4.1	IT Planning or Steering Committee		
4.2	Organizational Placement of the IT Function		
4.3	Review of Organizational Achievements		
4.4	Roles & Responsibilities		

COBIT Risk & Control Assessment Questionnaire



3

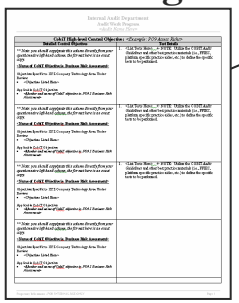
Engagement Scope



4

Kick-Off Meeting

Work Program



5

Client Work Sessions

6

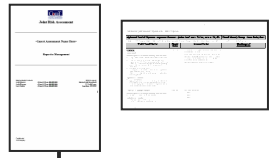
Audit Testing

7

Exit Meeting

8

Reporting



9

QAR

Map Audit Scope To COBIT®

COBIT Integration

COBIT To Audit Mapping Template

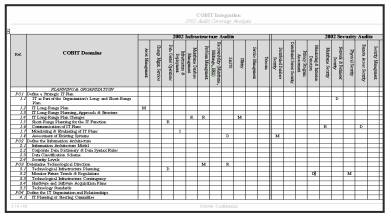
Ref.	COBIT Domains & Control Objectives	Applicable COBIT Control Objectives (mark with 'X')
	PLANNING & ORGANIZATION	
PO1	**Define a Strategic IT Plan**	
1.1	IT as Part of the Organization's Long- and Short-Range Plan	
1.2	IT Long-Range Plan	
1.3	IT Long-Range Planning, Approach & Structure	
1.4	IT Long-Range Plan Changes	
1.5	Short-Range Planning for the IT Function	
1.6	Communication of IT Plans	
1.7	Monitoring & Evaluating of IT Plans	
1.8	Assessment of Existing Systems	
PO2	**Define the Information Architecture**	
2.1	Information Architecture Model	
2.2	Corporate Data Dictionary & Data Syntax Rules	
2.3	Data Classification Scheme	
2.4	Security Levels	
PO3	Determine Technological Direction	
3.1	Technological Infrastructure Planning	
3.2	Monitor Future Trends & Regulations	
3.3	Technological Infrastructure Contingency	
3.4	Hardware and Software Acquisition Plans	
3.5	Technology Standards	
PO4	**Define the IT Organization and Relationships**	
4.1	IT Planning or Steering Committee	
4.2	Organizational Placement of the IT Function	
4.3	Review of Organizational Achievements	
4.4	Roles & Responsibilities	

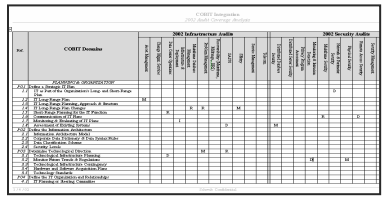
High Level Objective (e.g. PO1)

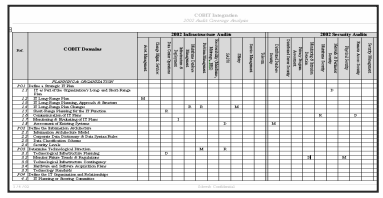
Detailed Level Objective (e.g. 2.1)

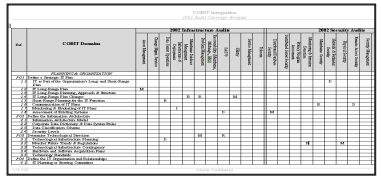
Applicable Objectives Noted In This Column

Supplemented by other mapping results…









Using COBIT® Framework To Tie It All Together…

Audit Scope Memo Defined

TO: Senior Client Manager
FROM: Lead Auditor
DATE: February 4, 2003
SUBJECT: *2003 Network Security Infrastructure Audit*

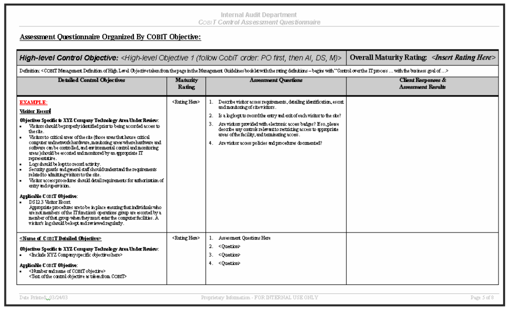
The Internal Audit Department (IAD) and Information Security Services (ISS) will participate in a joint assessment of security practices in place to protect XYZ Company's network infrastructure from external threats associated with Internet and 3rd party network connectivity. This review will begin on February 18, 2003, and will continue through June 2003.

The primary purpose of this assessment is to obtain an understanding of the policies, procedures, and tools associated with securing the network infrastructure. The overall objective of the review is to identify major risks and evaluate whether sufficient mechanisms and tasks are in place to mitigate those risks. IAD and ISS will assess the network security infrastructure by following guidelines and principles that are set forth in the CobiT (Control Objectives for Informat… and Related Technology) framework. A detailed review of CobiT will be provided in the Kick-Off Meeting du… week of February 17, 2003.

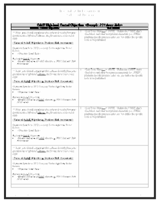
The COBIT Control Objectives applicable to this review include:

- DS5 Ensure Systems Security
  - ✓ DS5.1 Manage Security Measures
  - ✓ DS5.2 Identification, Authentication and Access
  - ✓ DS5.4 User Account Management
  - ✓ DS5.5 Management Review of User Accounts
  - ✓ DS5.7 Security Surveillance
  - ✓ DS5.10 Violation and Security Activity Reports
  - ✓ DS5.11 Incident Handling
  - ✓ DS5.12 Reaccreditation
  - ✓ DS5.20 Firewall Architectures and Connections with Public Networks
- DS9 Manage the Configuration
  - ✓ DS9.1 Configuration Recording
  - ✓ DS9.2 Configuration Baseline
  - ✓ DS9.3 Status Accounting

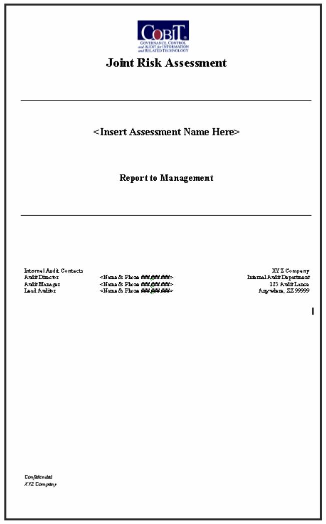
COBIT Risk & Control Assessment Questionnaire



Work Program



Audit Report



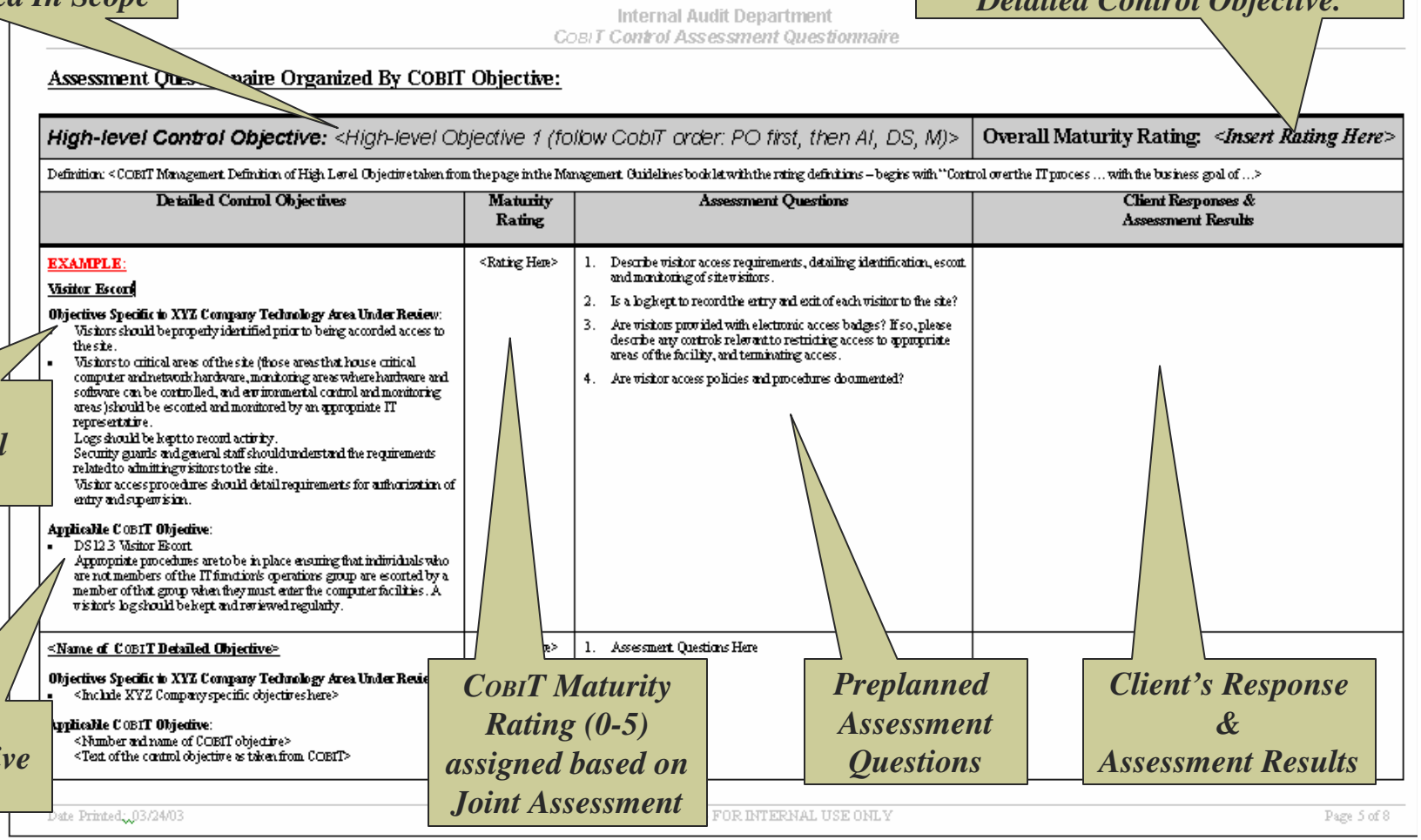
Use of a *Framework* ensures consistent coverage across audits and allows for trending the "state of controls" over time.

COBIT® Control Assessment Questionnaire

Questionnaire is used during joint work sessions held with clients to complete a joint risk assessment of the area under review.

One Table For Each High-Level COBIT Objective Included In Scope

Overall Maturity Rating for each High-Level Control Objective assigned based on results of joint assessments of each Detailed Control Objective.



Internal Audit Department
COBIT Control Assessment Questionnaire

Assessment Questionnaire Organized By COBIT Objective:

High-level Control Objective: <High-level Objective 1 (follow CobiT order: PO first, then AI, DS, M)>			Overall Maturity Rating: <Insert Rating Here>
Definition: <COBIT Management Definition of High Level Objective taken from the page in the Management Guidelines booklet with the rating definitions – begins with "Control over the IT process ... with the business goal of ...>			
Detailed Control Objectives	**Maturity Rating**	**Assessment Questions**	**Client Responses & Assessment Results**
EXAMPLE: **Visitor Escort** **Objectives Specific to XYZ Company Technology Area Under Review:** Visitors should be properly identified prior to being accorded access to the site. ▪ Visitors to critical areas of the site (those areas that house critical computer and network hardware, monitoring areas where hardware and software can be controlled, and environmental control and monitoring areas) should be escorted and monitored by an appropriate IT representative. Logs should be kept to record activity. Security guards and general staff should understand the requirements related to admitting visitors to the site. Visitor access procedures should detail requirements for authorization of entry and supervision. **Applicable COBIT Objective:** ▪ DS12.3 Visitor Escort Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.	<Rating Here>	1. Describe visitor access requirements, detailing identification, escort and monitoring of site visitors. 2. Is a log kept to record the entry and exit of each visitor to the site? 3. Are visitors provided with electronic access badges? If so, please describe any controls relevant to restricting access to appropriate areas of the facility, and terminating access. 4. Are visitor access policies and procedures documented?	
<Name of COBIT Detailed Objective> **Objectives Specific to XYZ Company Technology Area Under Revie** ▪ <Include XYZ Company specific objectives here> **Applicable COBIT Objective:** <Number and name of COBIT objective> <Text of the control objective as taken from COBIT>	<Rating Here>	1. Assessment Questions Here	

Date Printed: 03/24/03 FOR INTERNAL USE ONLY Page 5 of 8

XYZ Company Specific Control Objectives

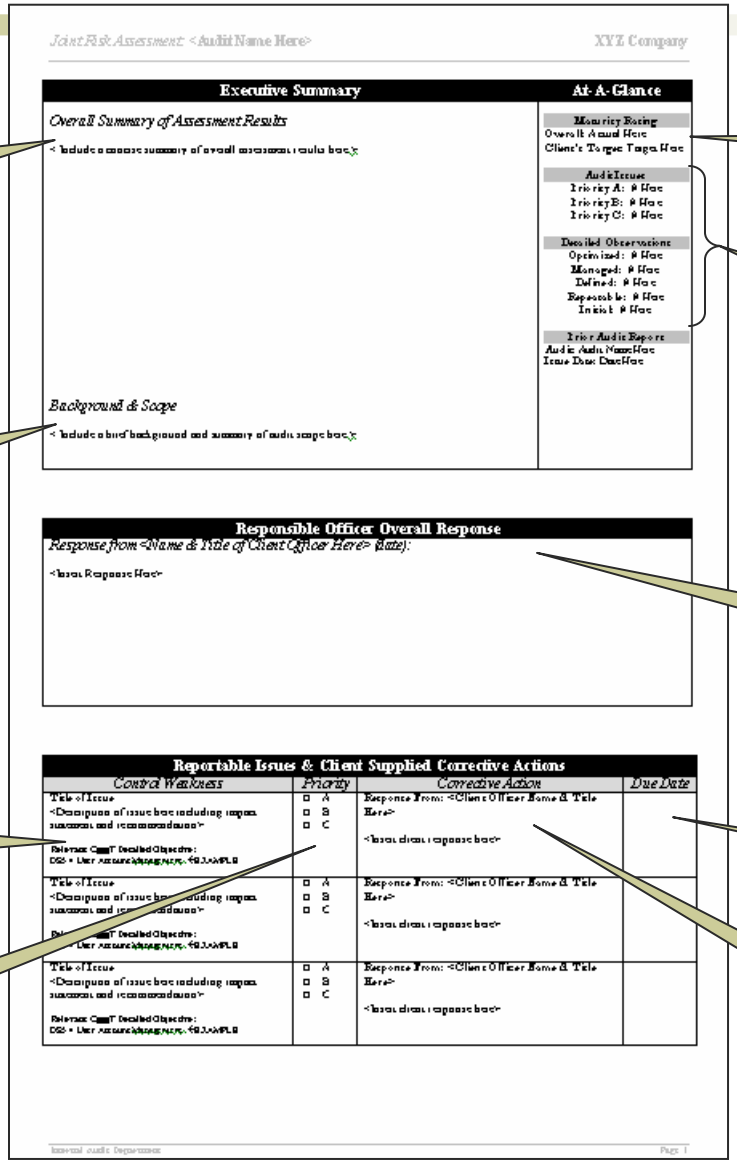
One COBIT Control Objective Per Row

COBIT Maturity Rating (0-5) assigned based on Joint Assessment

Preplanned Assessment Questions

Client's Response & Assessment Results

COBIT® Based Executive Audit Report



Overall Conclusion Statements Supporting Overall Rating

Concise Background & Scope

Control Weakness highlighting business impact

Issue Priority (A, B, C)

Overall Rating Clients Target Goal

Audit Metrics

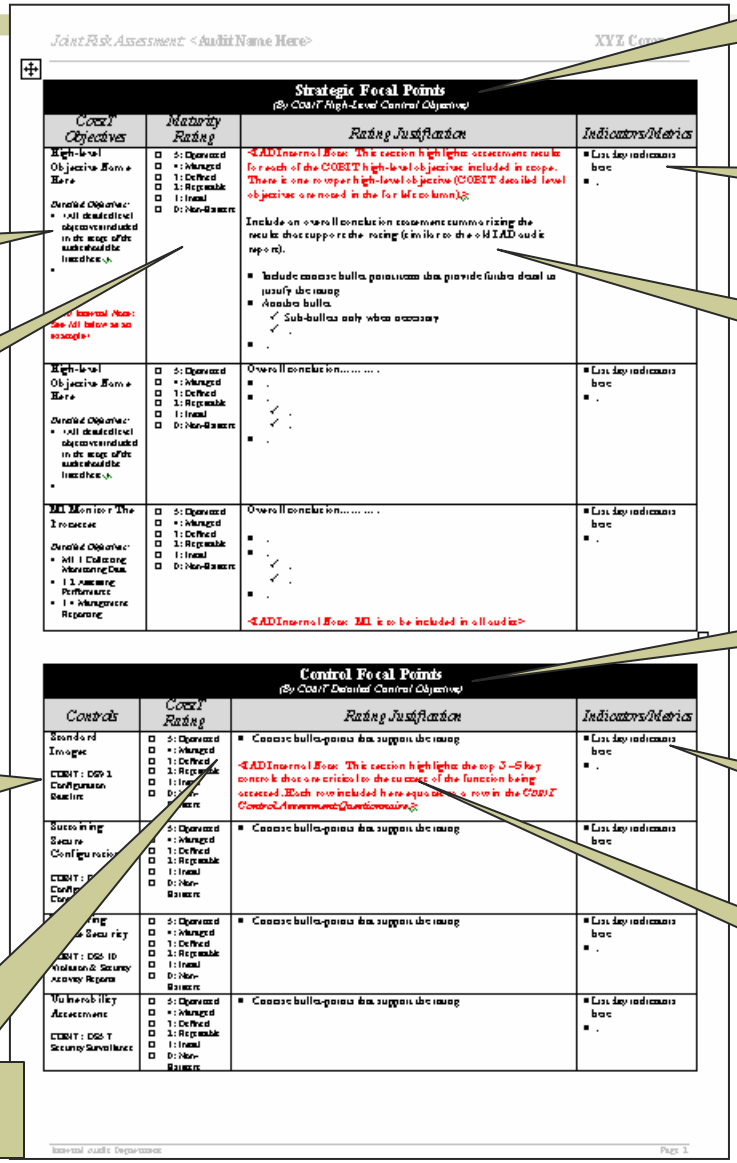
MGT Reports

Responsible Manager Provided Response

Due Date

Client Provided Responses

COBIT® Based Audit Report
(continued)



Strategic Focal Point Table (one row for each high-level objective included in scope)

Highlighting Key Performance Indicators (i.e., Metrics)

Detailed Control Objectives Included In Scope Listed

Summary Conclusions and Points Supporting Rating

Overall Rating For High-Level Control Objective

Control Focal Point Table (highlighting key controls)

Applicable Detailed Control Objective (one per row; corresponds to a row in the Assessment Questionnaire)

Highlighting Key Performance Indicators (i.e., Metrics)

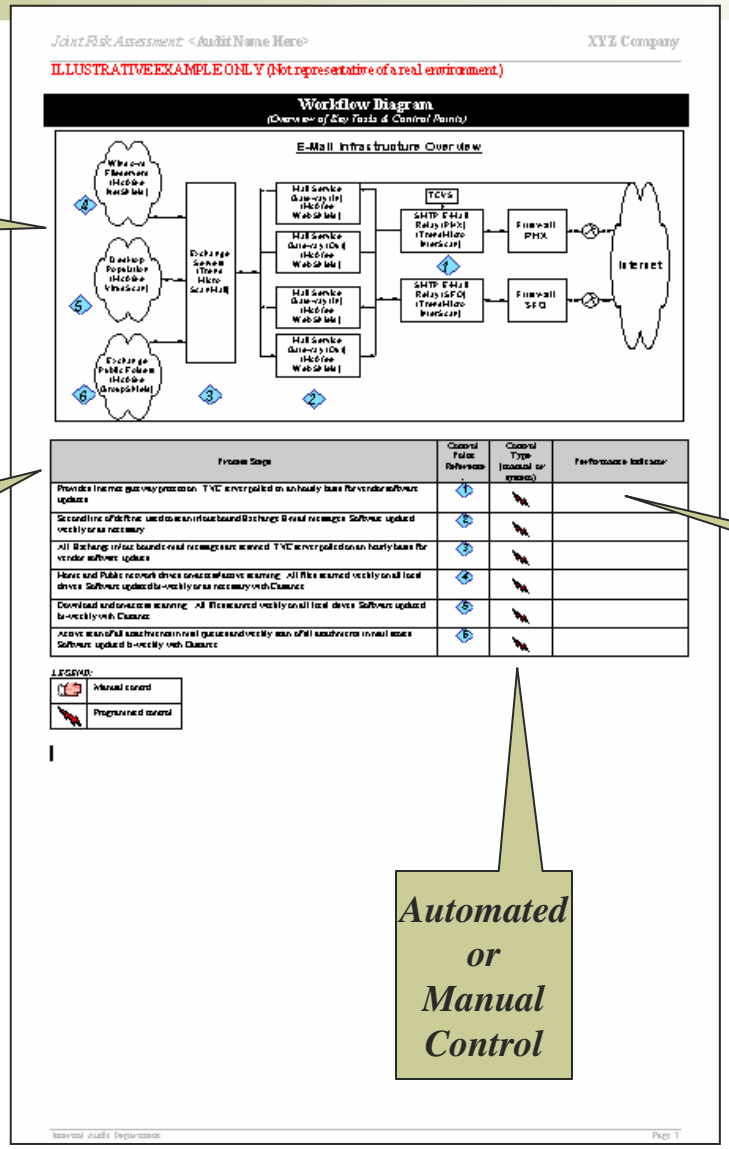
Assigned Maturity Rating

Summary Conclusions and Points Supporting Rating

COBIT® Based Audit Report
(continued)

Process Workflow Diagram For Area Assessed

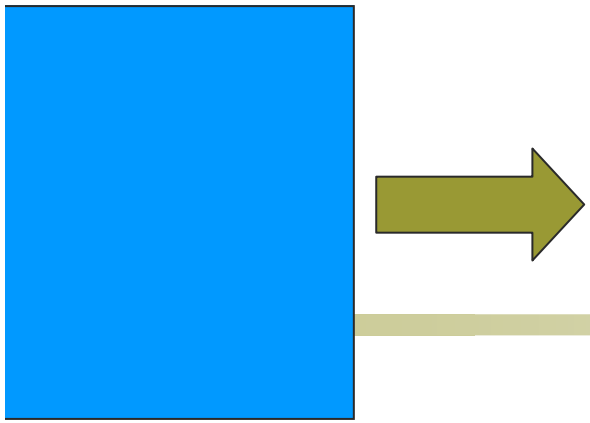
Table Defining Key Control Points In Process Flow



Highlighting Key Performance Indicators (i.e., Metrics)

Automated or Manual Control

ISACA®
Serving IT Governance Professionals



Using COBIT® to Establish *IT Risk & Control Measurement*

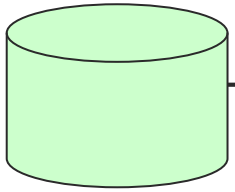
Analysis of Audit & Key Technology Metrics

Goal is to proactively monitor audit results and IT metrics on an ongoing basis to focus the scope of audits on high-risk processes and tasks where performance indicators indicate potential problems.

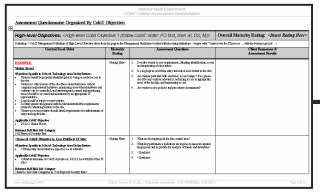
Results of metric analysis is presented to client management on a periodic basis via management reports. The analysis indicates any changes to the audit scope planned for upcoming audits.

COBIT® Measurement Repository

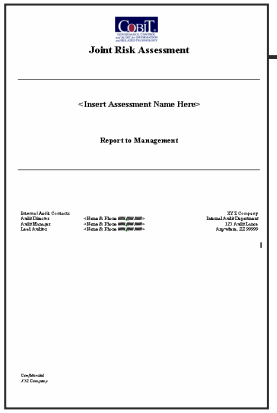
Continuous Monitoring



Questionnaire



Audit Reports

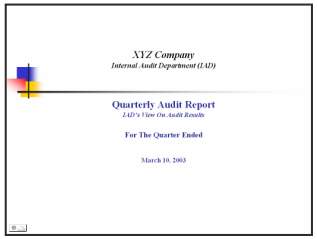


COBIT Integration

2002 Audit Coverage Analysis

Ref.	COBIT Domains	2002 Infrastructure Audits											2002 Security Audits								
		Asset Management	Change Mgmt Services	Data Center Operations	Infrastructure & Deployment	Mainframe Database Management	Problem Management	Recoverability (Mainframe, Midrange, ERP)	SAS70	SEntry	Service Management	Telecom	Distributed Database Security	Distributed Server Security	Privacy Program Assessment	Monitoring & Intrusion Detection	Mainframe Security	Network & Perimeter Security	Physical Security	Remote Access Security	Security Management
	PLANNING & ORGANIZATION																				
PO1	Define a Strategic IT Plan																				
1.1	IT as Part of the Organization's Long- and Short-Range Plan																	D			
1.2	IT Long-Range Plan	M																			
1.3	IT Long-Range Planning, Approach & Structure																				
1.4	IT Long-Range Plan Changes					R	R			M											
1.5	Short-Range Planning for the IT Function			R																	
1.6	Communication of IT Plans																R			D	
1.7	Monitoring & Evaluating of IT Plans				I																
1.8	Assessment of Existing Systems								D				M								
PO2	Define the Information Architecture																				
2.1	Information Architecture Model																				
2.2	Corporate Data Dictionary & Data Syntax Rules																				
2.3	Data Classification Scheme																				
2.4	Security Levels																				
PO3	Determine Technological Direction						M		R												
3.1	Technological Infrastructure Planning			D																	
3.2	Monitor Future Trends & Regulations															D			M		
3.3	Technological Infrastructure Contingency																				
3.4	Hardware and Software Acquisition Plans																				
3.5	Technology Standards																				
PO4	Define the IT Organization and Relationships																				
4.1	IT Planning or Steering Committee																				

1/4/02 Schwab Confidential



MGT REPORTS

Trending Audit Results Over Time…

Periodic Management Reports

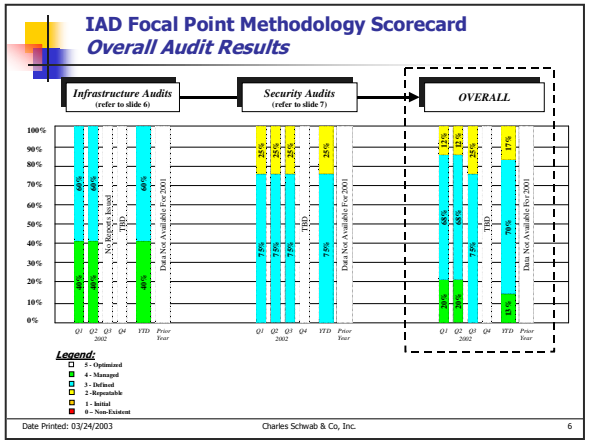
XYZ Company
Internal Audit Department (IAD)

Report to IT Management

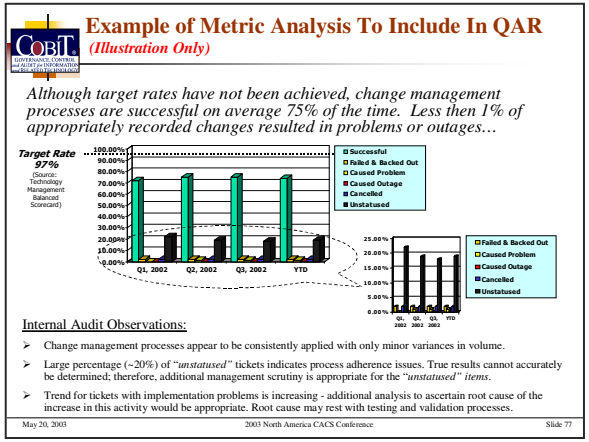
Audit Results
&
Analysis of Key Technology Metrics

For the Quarter Ended
March 31, 2006

Audit Results Metrics

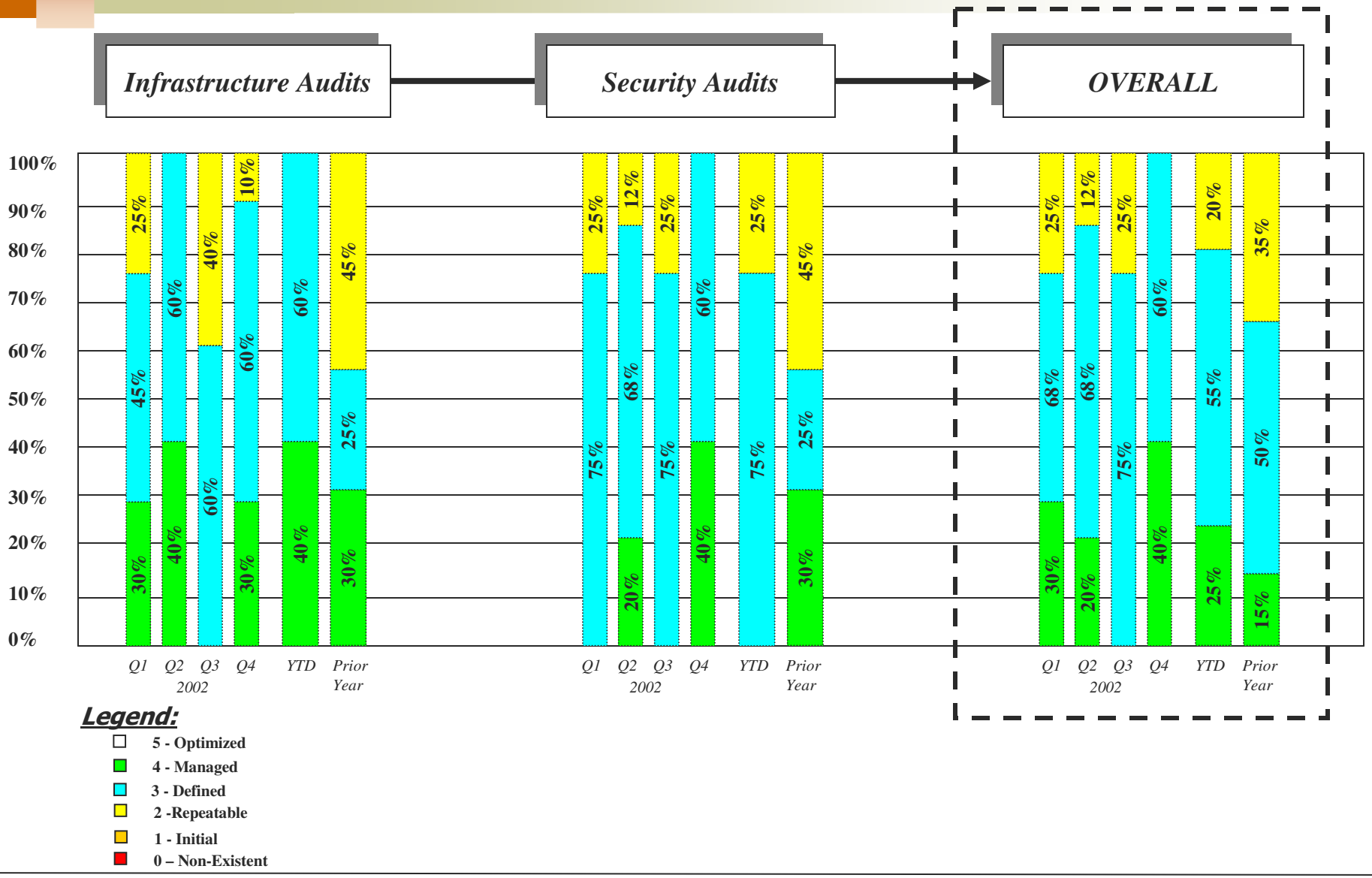


Analysis of Key Technology Metrics



Example of Audit Result Metrics

(Illustration Only)

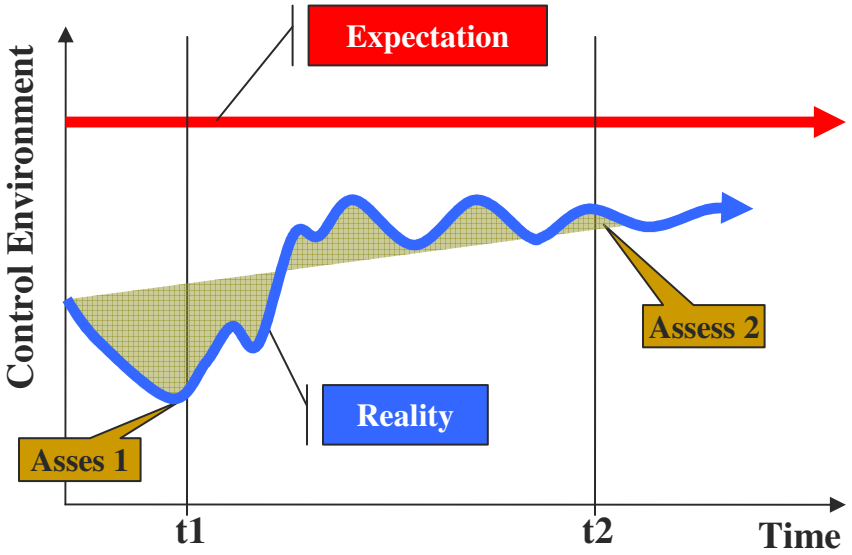


Continuous Monitoring / Auditing

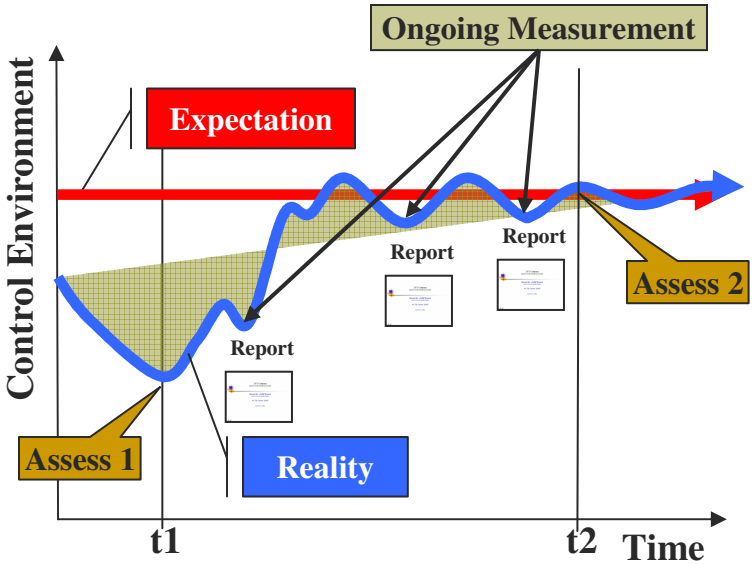
Ongoing Measurement / Ongoing Dialogue

Auditors monitor key indicators for mission critical technology functions on an ongoing basis…

Traditional Audit Approach



Ongoing Monitoring Of Indicators

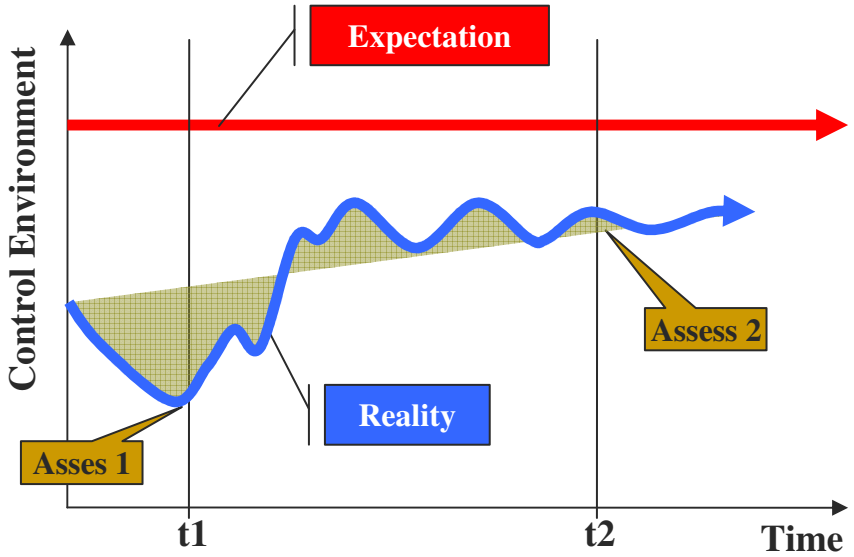


Continuous Monitoring / Auditing

Ongoing Measurement / Ongoing Dialogue

Traditional Audit Approach

(Audit rotation schedule based on annual risk assessment of function)

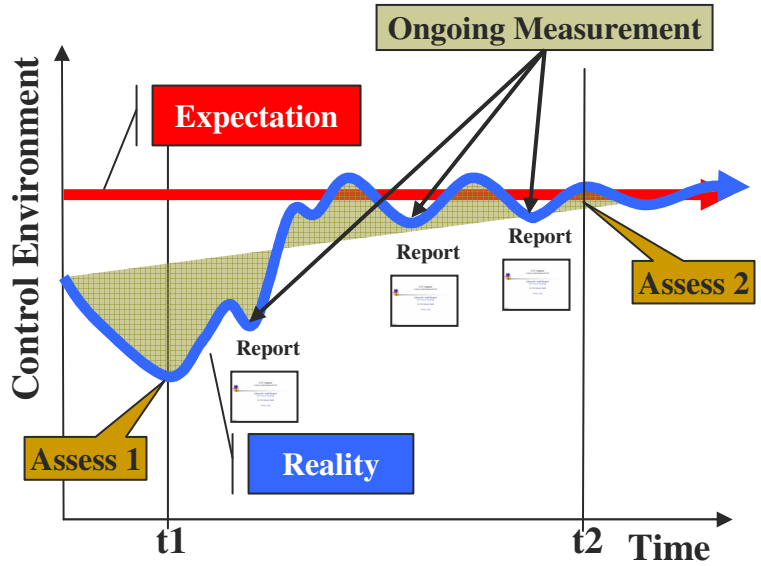


"Point-In-Time" Audit – Challenges

- Evaluation of risk and control is as of a point in time.
- Audit reporting is reflective of results as of a point in time.
- Audit scope may be influenced by prior results.
- If an audit of the function has not been completed for a long time, there may be a learning curve.

Continuous Monitoring / Auditing
Ongoing Measurement / Ongoing Dialogue

Ongoing Monitoring Of Risk Indicators
(Gaining Efficiencies Through Focus On High Risk Indicators)

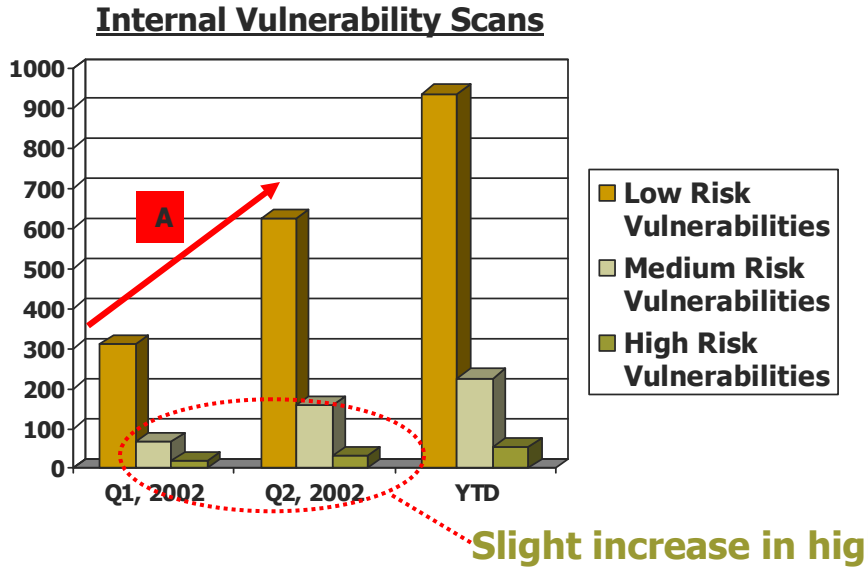


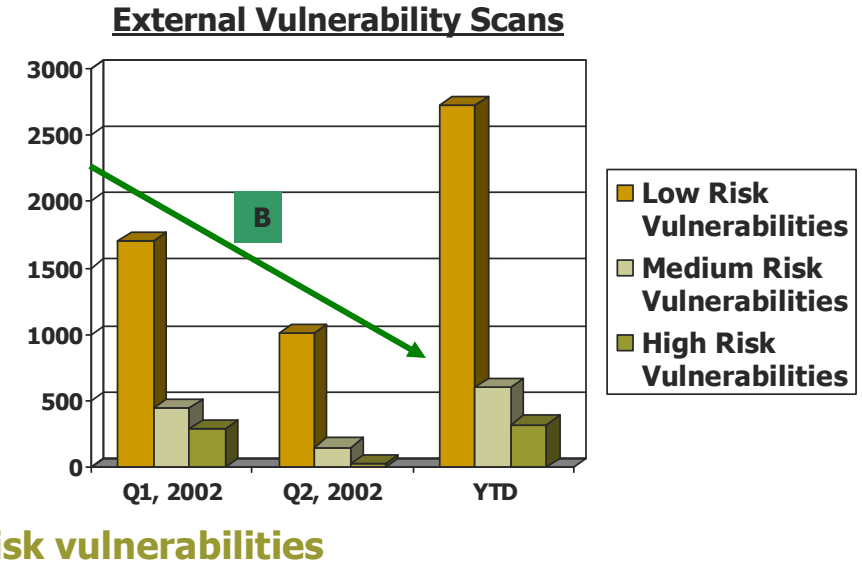
Benefits of Ongoing Monitoring

- Periodic (e.g., quarterly) readout of assessment results for technology management.
- Ongoing dialogue regarding areas of significant or increasing risk.
- IAD focuses the scope of individual audits on known risk factors ultimately leading to audit efficiencies which may result in less time impact on client personnel.

Information Security:
Measuring Performance *(illustration only)*

The Security Officer consistently performs both internal and external vulnerability scans on a monthly basis. The majority of vulnerabilities identified are low risk…





Slight increase in high risk vulnerabilities

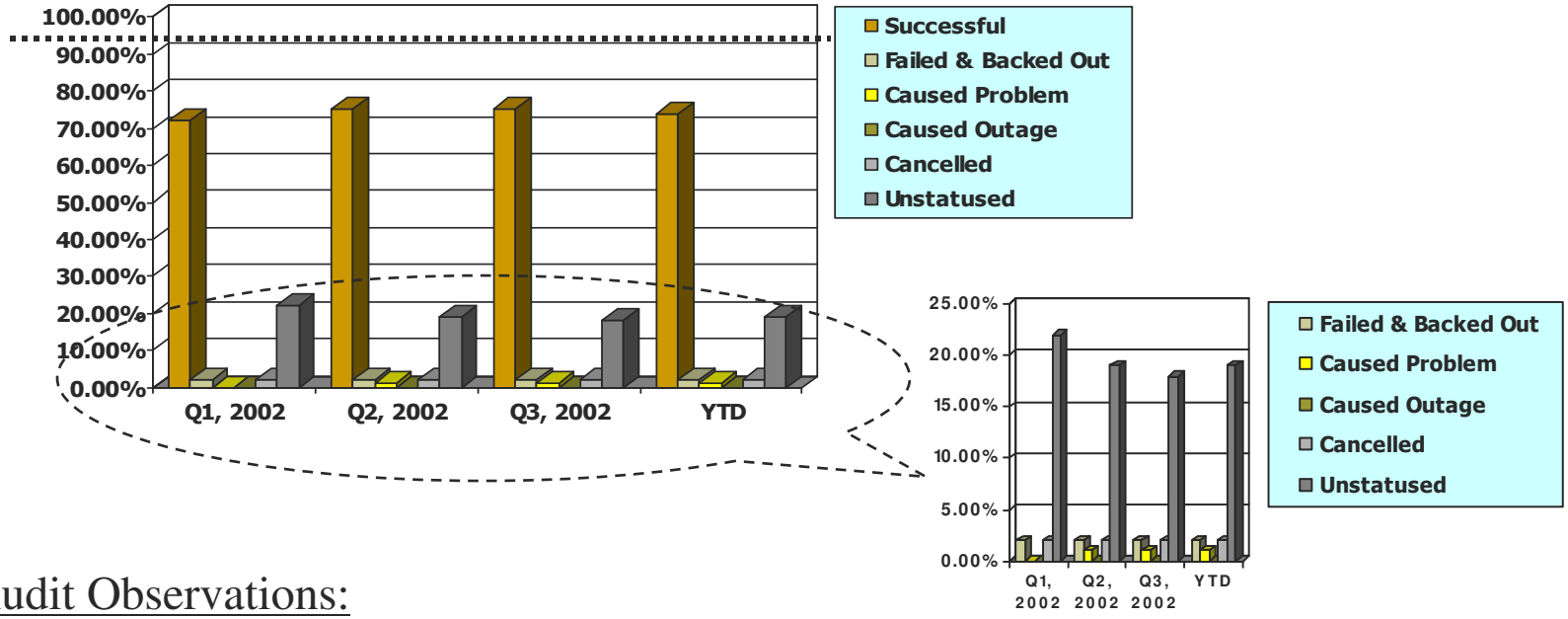
Observations:

- **A** An increase in *internal* vulnerabilities occurred from Q1 to Q2. The increase is explained due to new system patches checked for by the vulnerability scanner that have not been applied to the XYZ company servers. Technology management appropriately applies patches only after the patches have been tested and certified.
- **B** A decrease in *external* vulnerabilities was noted from Q1 to Q2. These results demonstrate that a significant number of Q1 vulnerabilities have been resolved.

Change Management:
Measuring Performance (illustration only)

Although target rates have not been achieved, change management processes are successful on average 75% of the time. Less then 1% of appropriately recorded changes resulted in problems or outages…

Target Rate 97%
(Source: Technology Management Balanced Scorecard)



Internal Audit Observations:

- Change management processes appear to be consistently applied with only minor variances in volume.
- Large percentage (~20%) of "*unstatused*" tickets indicates process adherence issues. True results cannot accurately be determined; therefore, additional management scrutiny is appropriate for the "*unstatused" items*.
- Trend for tickets with implementation problems is increasing - additional analysis to ascertain root cause of the increase in this activity would be appropriate. Root cause may rest with testing and validation processes.

ISACA®
Serving IT Governance Professionals

COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

Summary & Wrap-Up

Benefits Realized…

- IT management partners with Internal Audit throughout the audit life cycle, including input into the audit schedule and scope.
- IT management becomes conversant in risk, control, and audit concepts.
- Relationships transformed into partnerships by jointly assessing control procedures.
- Audit Report streamlined…concise report supported by detailed questionnaire.
- Audit approach is methodical and is consistent with industry standards / best practices as well as IT Governance practices implemented throughout the company's technology organization.
- Meaningful reporting for senior IT management.

Templates & Additional Resources

- Templates (www.sfisaca.org/resources/downloads.htm)
- IT Governance Implementation Guide (www.isaca.org)
- IT Control Practice Statements (www.isaca.org)
- Questionnaire for IT Control Practice Statements (www.isaca.org)
- IT Control Objectives for Sarbanes-Oxley (www.isaca.org)
- COBIT Security Baseline (www.isaca.org)
- ITIL (www.itil.co.uk)
- ISO (www.iso.org)
- ISO 17799 Related Information (www.iso-17799.com/)
- COBIT Case Studies
  (available at www.itgi.org/ and www.isaca.org)

Questions / Thank You!

Lance M. Turcato, CISA, CISM, CPA

Deputy City Auditor – Information Technology
City of Phoenix
Email: lance.turcato@phoenix.gov
Phone: 602-262-4714

City of Phoenix