ISACA®

Trust in, and value from, information systems

San Francisco Chapter

S11 – Introduction to COBIT

Integrating COBIT into the IT Audit Lifecycle

&

Update on COBIT 5.0 Development

Back to Business
COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

Audience Poll

COBIT® Knowledge

- First exposure?
- General understanding?
- Strong knowledge of COBIT® framework?

Current Users of COBIT®

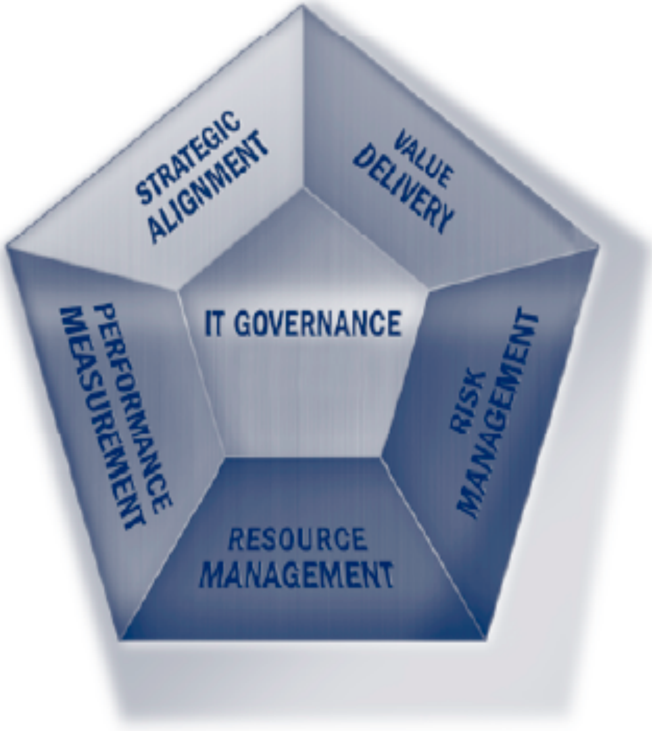
- Incorporated Into Audit Process?
- Adopted by IT Management for IT Governance?
- Users of a framework other than COBIT®?

AGENDA

- Overview of COBIT®
- Integrating COBIT® Domains into IT Audit Planning & Scope Development
- Integrating COBIT® into the IT Audit Lifecycle
- COBIT 5 Update
- Summary & Wrap-up

Control
OBjectives
for **I**nformation
and Related **T**echnology

IT Governance Focus Areas



- Strategic Alignment
- Value Delivery
- Risk Management
- Resource Management
- Performance Measurement

More information: ***Board Briefing on IT Governance*, 2nd *Edition*** (**www.itgi.org/**)

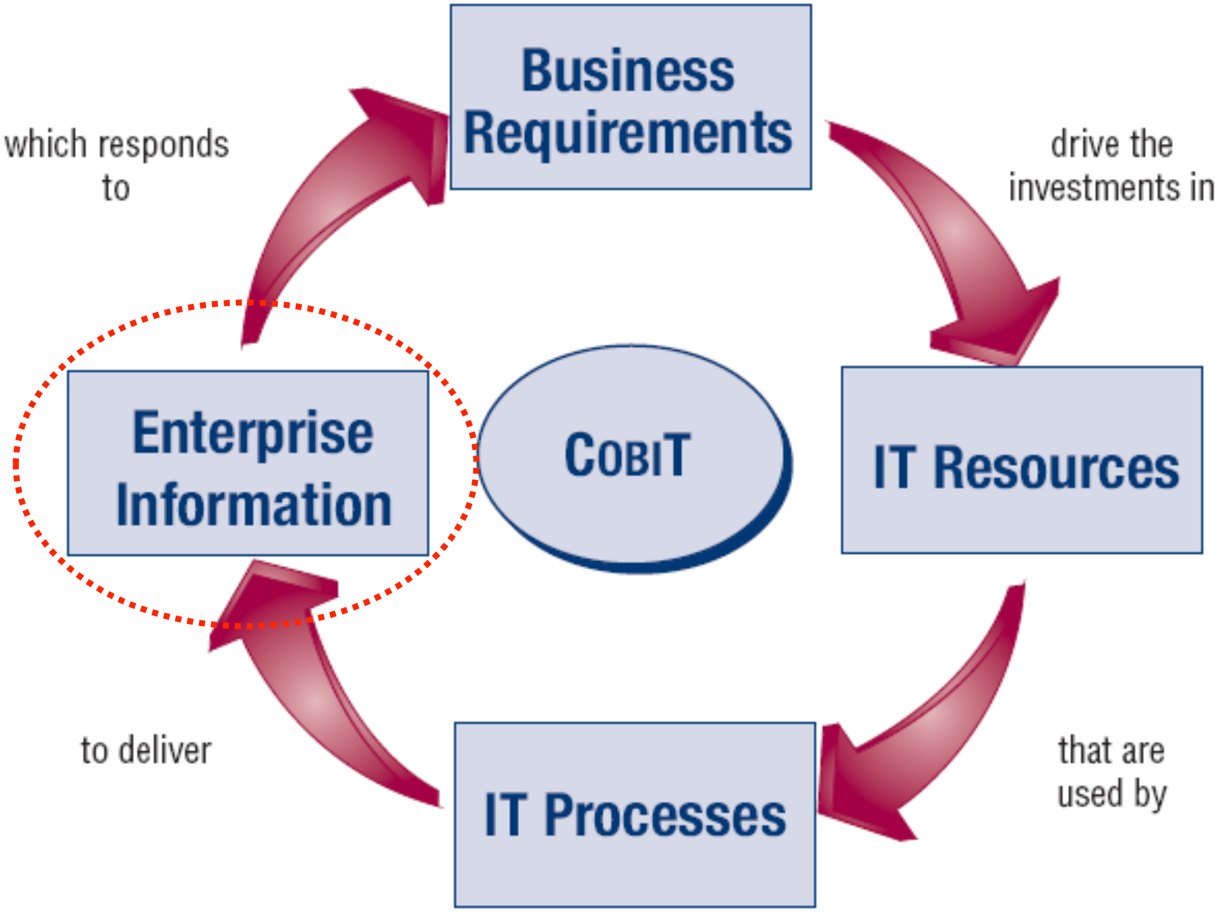
COBIT' s Scope & Objectives
IT Governance Framework

- **Business-Focused:** Linkage with business requirements (bridges the gap between control requirements, technical issues, and business risks). Management and process owner orientation to ensure accountability.
- **Process-Oriented:** Identifies the major IT resources to be leveraged and organizes IT activities into a generally accepted process model (in alignment with ITIL, ISO, and other relevant 'good practices' and industry standards).
- **Controls-Based:** Defines control objectives and associated assurance guidelines and provides a toolkit of "best practices" for IT control representing the consensus of experts.
- **Measurement-Driven:** Provides tools for performance measurement and maturity assessment.
- **Generic-Oriented:** applicable to multiple environments.

COBIT® Structure

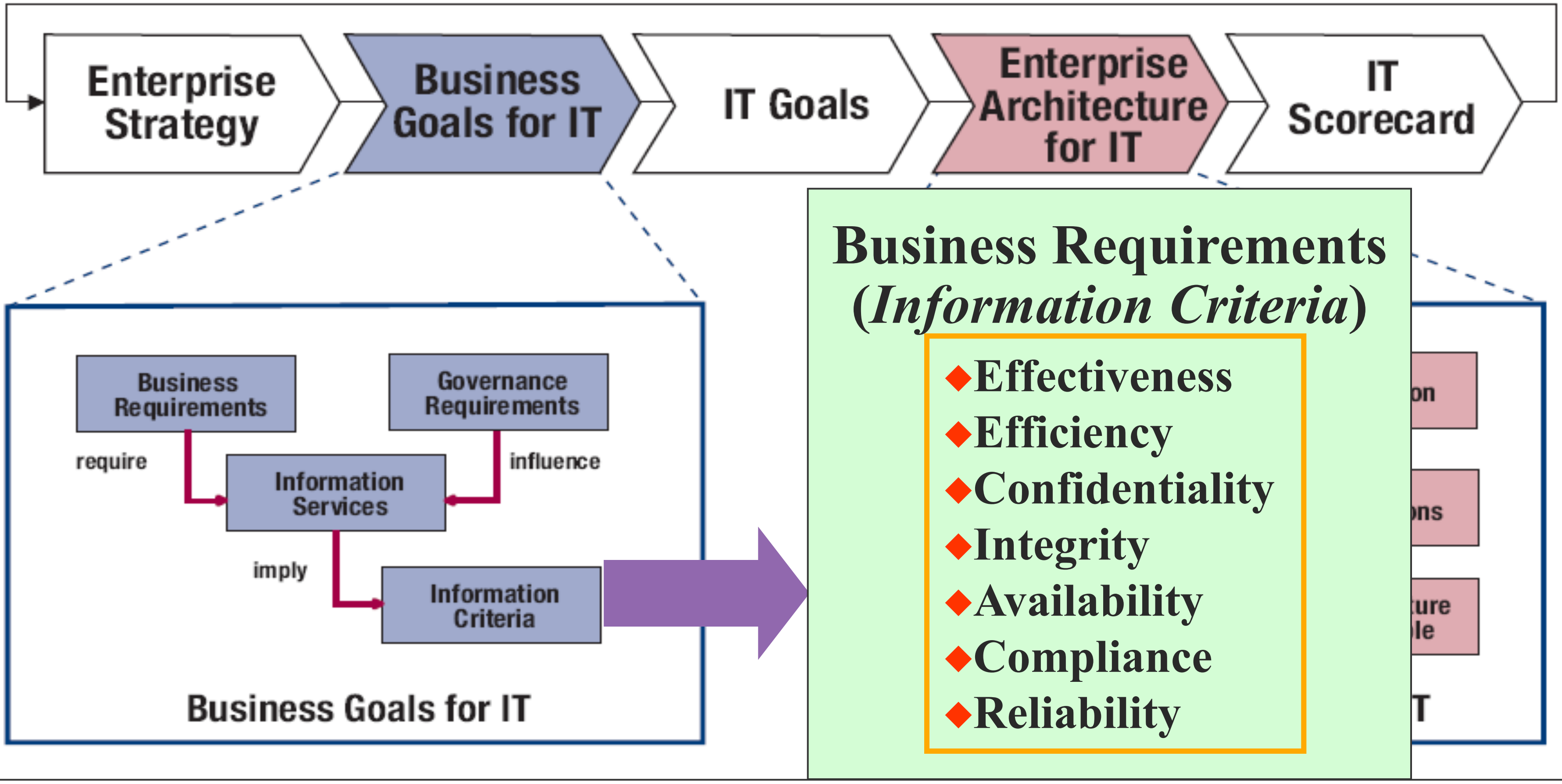
Overview

Starts from the premise that IT needs to <u>deliver the information</u> that the enterprise needs to achieve its objectives.



COBIT® Structure
Information Criteria (7)

Highlights typical business requirements of enterprises by providing seven ***information criteria*** for use in generically defining what the business requires from IT.

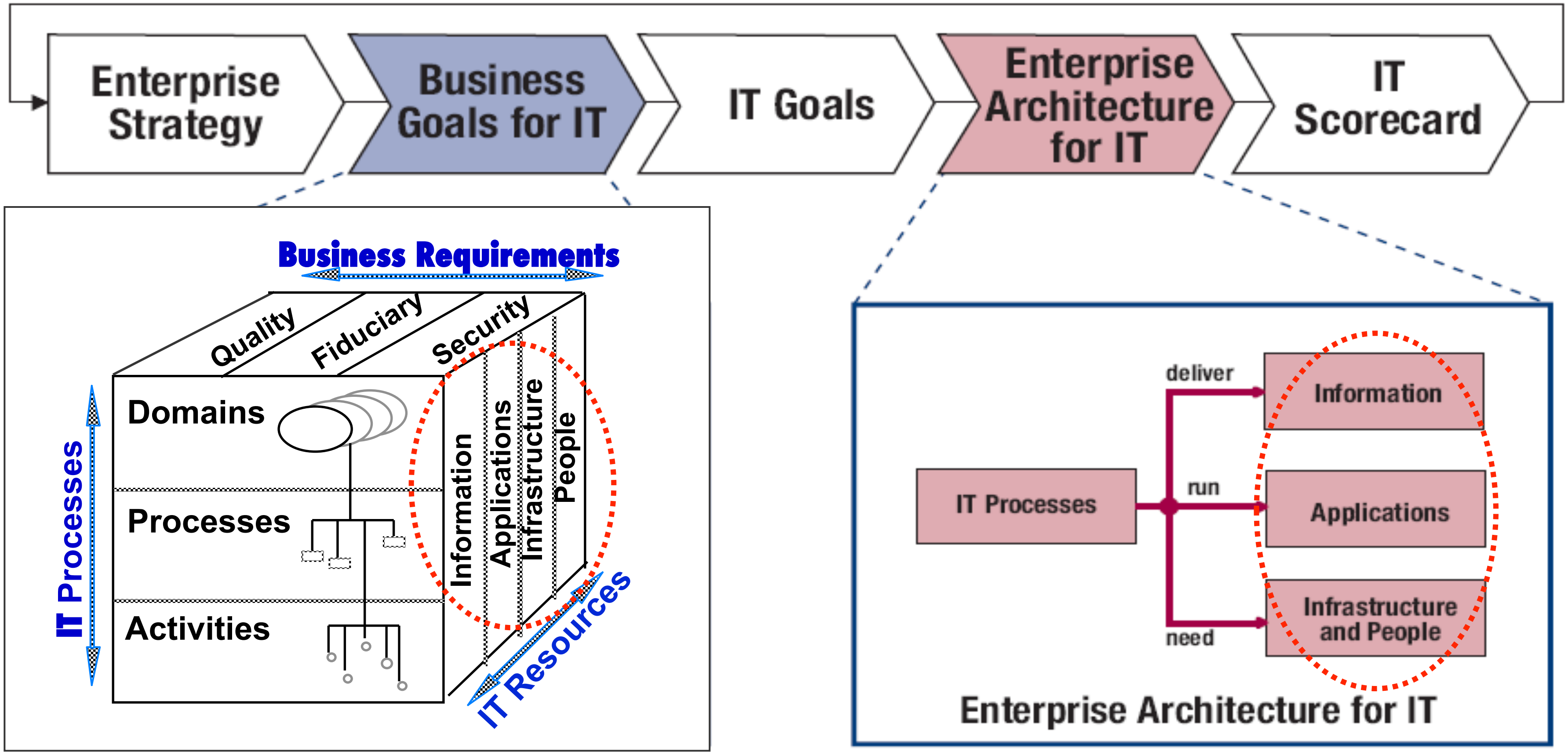


Business Requirements (*Information Criteria*)

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

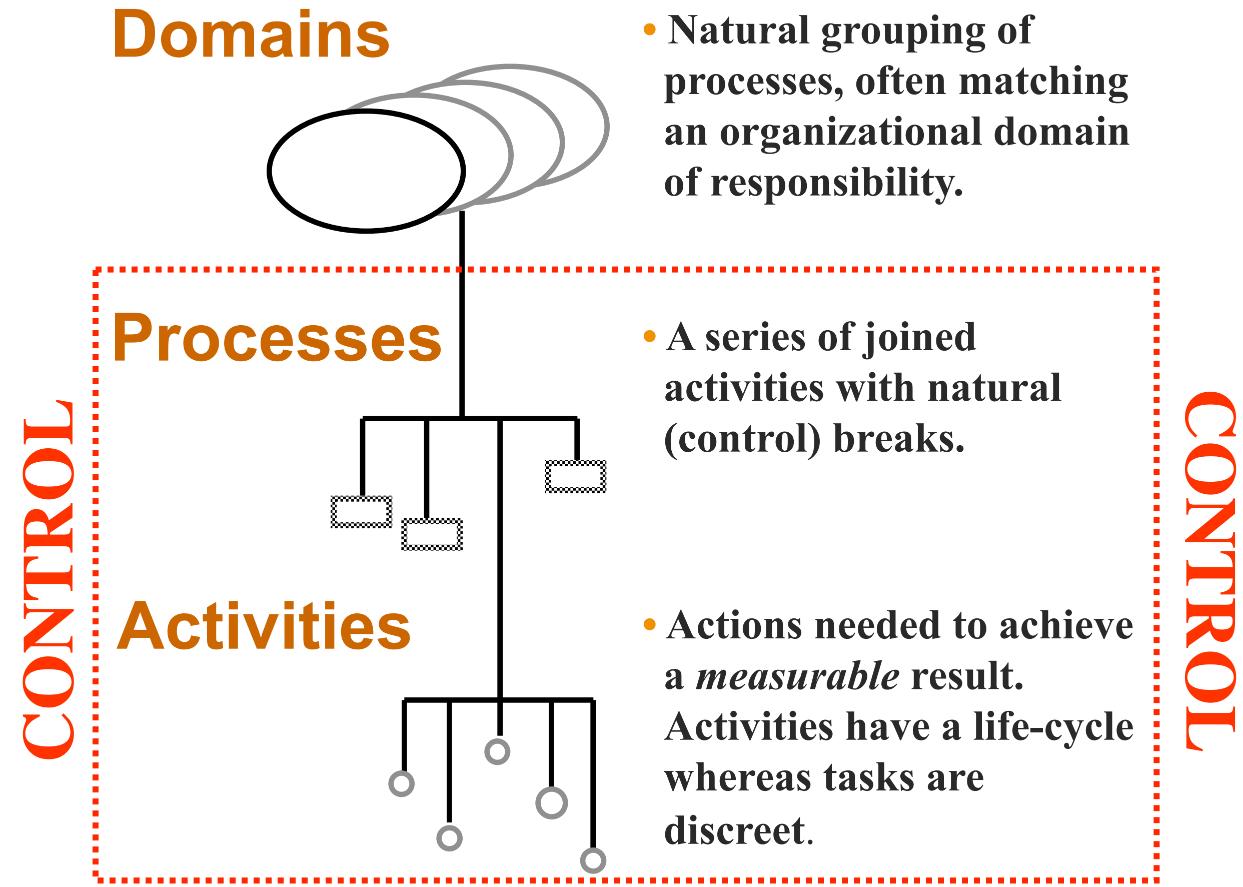
CobiT® Structure
IT Resources (4)

Maps ***IT resources*** to domains and processes to highlight resource requirements and promotes process ownership by providing RACI charts for use in defining roles and responsibilities.



COBIT® Structure
Control Objectives (>200)

Emphasizes process control by providing a ***high-level control objective*** and a set of ***detailed control objectives*** for each process.



Domains

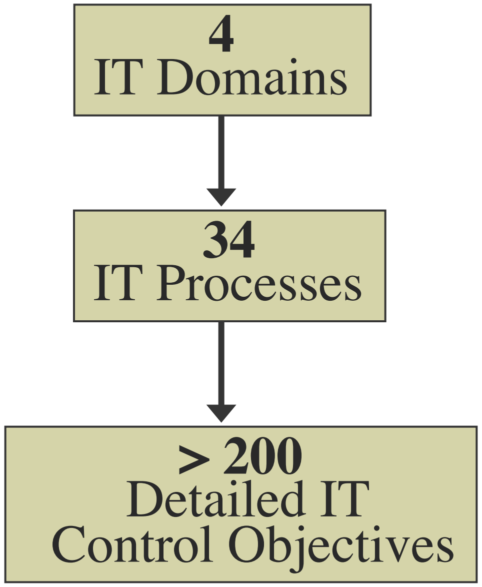
- **Natural grouping of processes, often matching an organizational domain of responsibility.**

Processes

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

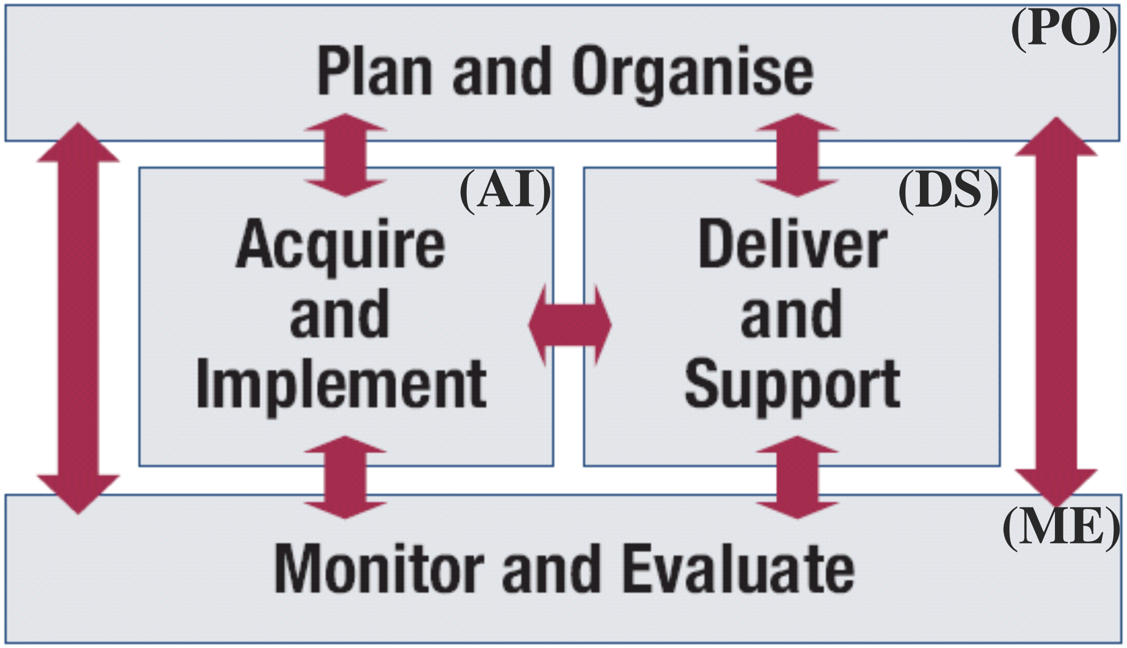
Activities

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



COBIT® Structure
Overview of 4 Domains

The primary focus of the domains is on delivering the technology capabilities, services, assets and other resources that the business functions need to implement and sustain business change.



COBIT® Structure

Overview of 34 IT Processes

Strategic & Planning Focus

Plan & Organize (PO)

- •PO1 – Define a Strategic Plan
- •PO2 – Define the Information Architecture
- •PO3 – Determine Technological Direction
- •PO4 – Define the IT Processes, Organization & Relationships
- •PO5 – Manage the IT Investment
- •PO6 – Communicate Management Aim & Direction
- •PO7 – Manage IT Human Resources
- •PO8 – Manage Quality
- •PO9 – Assess and Manage IT Risks
- •PO10 – Manage Projects

SDLC

Acquire & Implement (AI)

- •AI1 – Identify Automated Solutions
- •AI2 – Acquire & Maintain Application Software
- •AI3 – Acquire & Maintain Technology Infrastructure
- •AI4 – Enable Operation and Use
- •AI5 – Procure IT Resources
- •AI6 – Manage Changes
- •AI7 – Install & Accredit Solutions and Changes

Day to Day Ops & Service Delivery

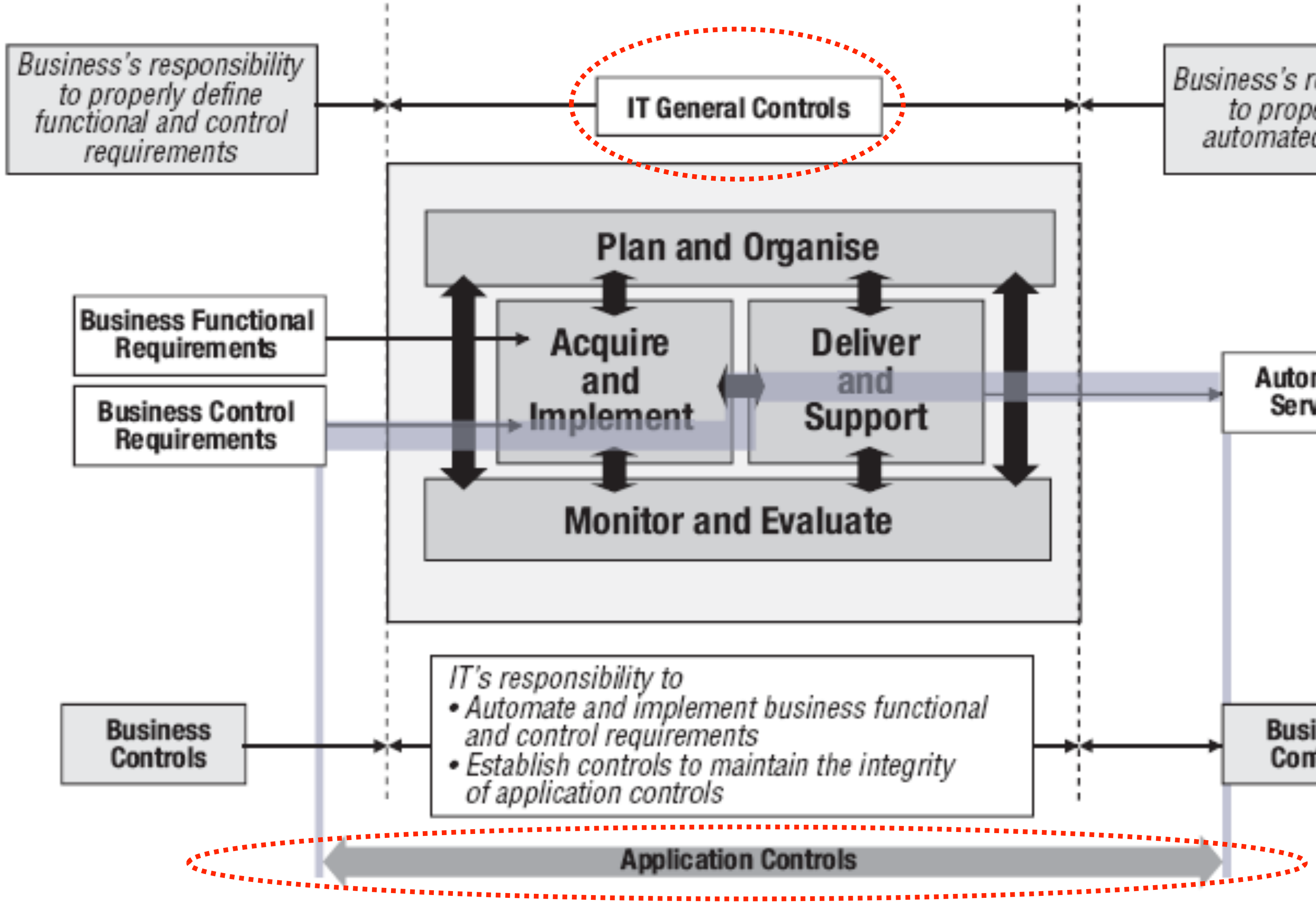
Deliver & Support (DS)

- •DS1 – Define & Manage Service Levels
- •DS2 – Manage 3rd Party Services
- •DS3 – Manage Performance & Capacity
- •DS4 – Ensure Continuous Service
- •DS5 – Ensure Systems Security
- •DS6 – Identify & Allocate Costs
- •DS7 – Educate & Train Users
- •DS8 – Manage Service Desk & Incidents
- •DS9 – Manage the Configuration
- •DS10 – Manage Problems
- •DS11 – Manage Data
- •DS12 – Manage the Physical Environment
- •DS13 – Manage Operations

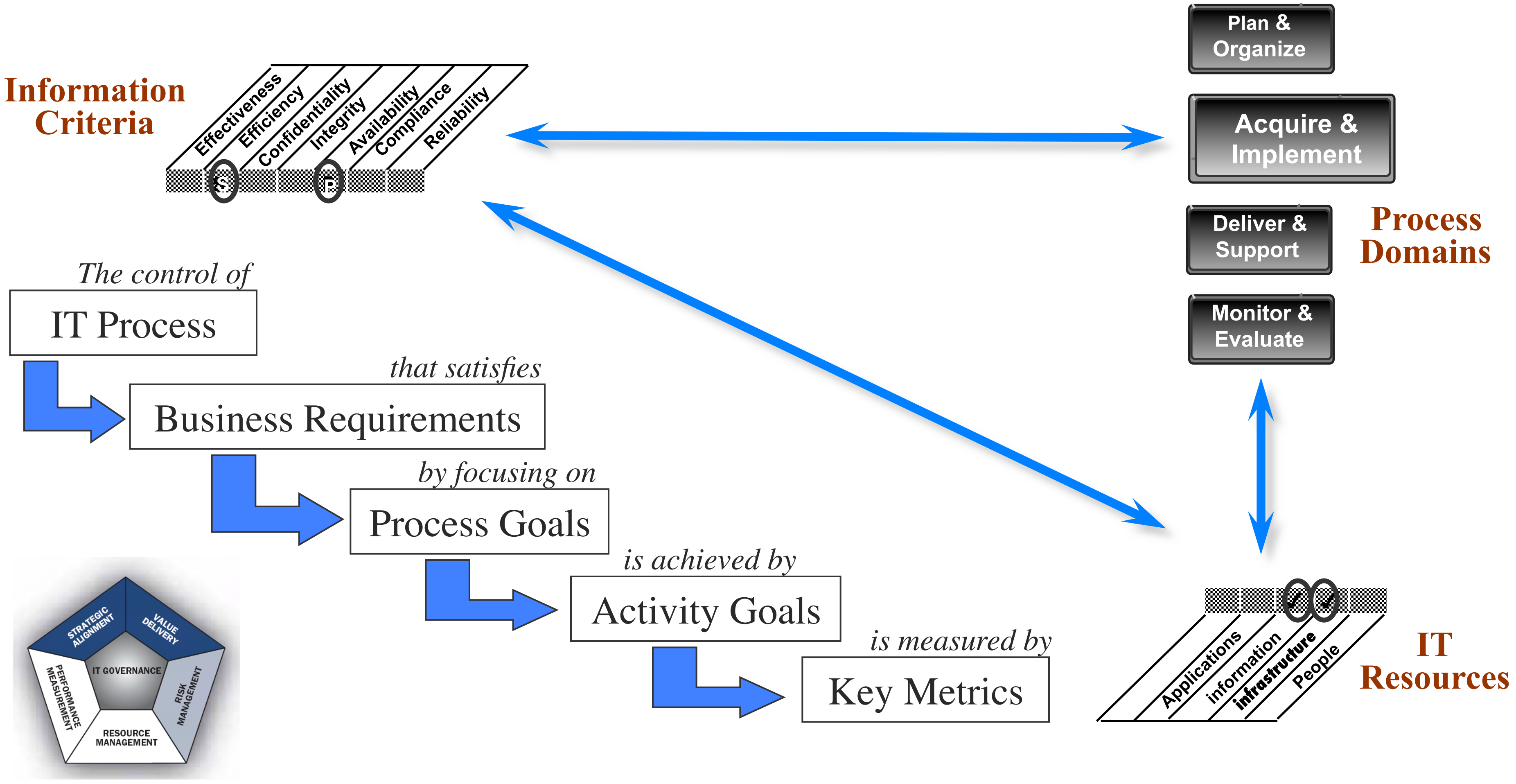
Monitor & Evaluate (ME)

- •ME1 – Monitor & Evaluate IT Performance
- •ME2 – Monitor & Evaluate Internal Control
- •ME3 – Ensure Compliance With External Requirements
- •ME4 – Provide IT Governance

COBIT® Structure
Control Objectives (Application versus General)


Business's responsibility to properly define functional and control requirements
IT General Controls
Business's responsibility to properly use automated services
Plan and Organise
Business Functional Requirements
Business Control Requirements
Acquire and Implement
Deliver and Support
Automated Services
Monitor and Evaluate
Business Controls
IT's responsibility to
• Automate and implement business functional and control requirements
• Establish controls to maintain the integrity of application controls
Business Controls
Application Controls

COBIT® "Waterfall" & Navigation Aids
Linking Processes, Resources & Information Criteria



Information Criteria

Plan & Organize

Acquire & Implement

Deliver & Support

Monitor & Evaluate

Process Domains

The control of
IT Process

that satisfies
Business Requirements

by focusing on
Process Goals

is achieved by
Activity Goals

is measured by
Key Metrics

IT Resources

Linking The Processes To Control Objectives

Example IT Process (High-level Control Objective)

Control over the IT process of

ENSURE SYSTEM SECURITY (DS5)

that satisfies the business requirement

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

by focusing on

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

is achieved by

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

and is measured by

- Number of incidents damaging the organization’ s reputation
- Number of systems where security requirements are not met
- Number of violations in segregation of duties

Example
(Domain → Process → Control Objective)

DOMAIN: Deliver and Support (**DS**)

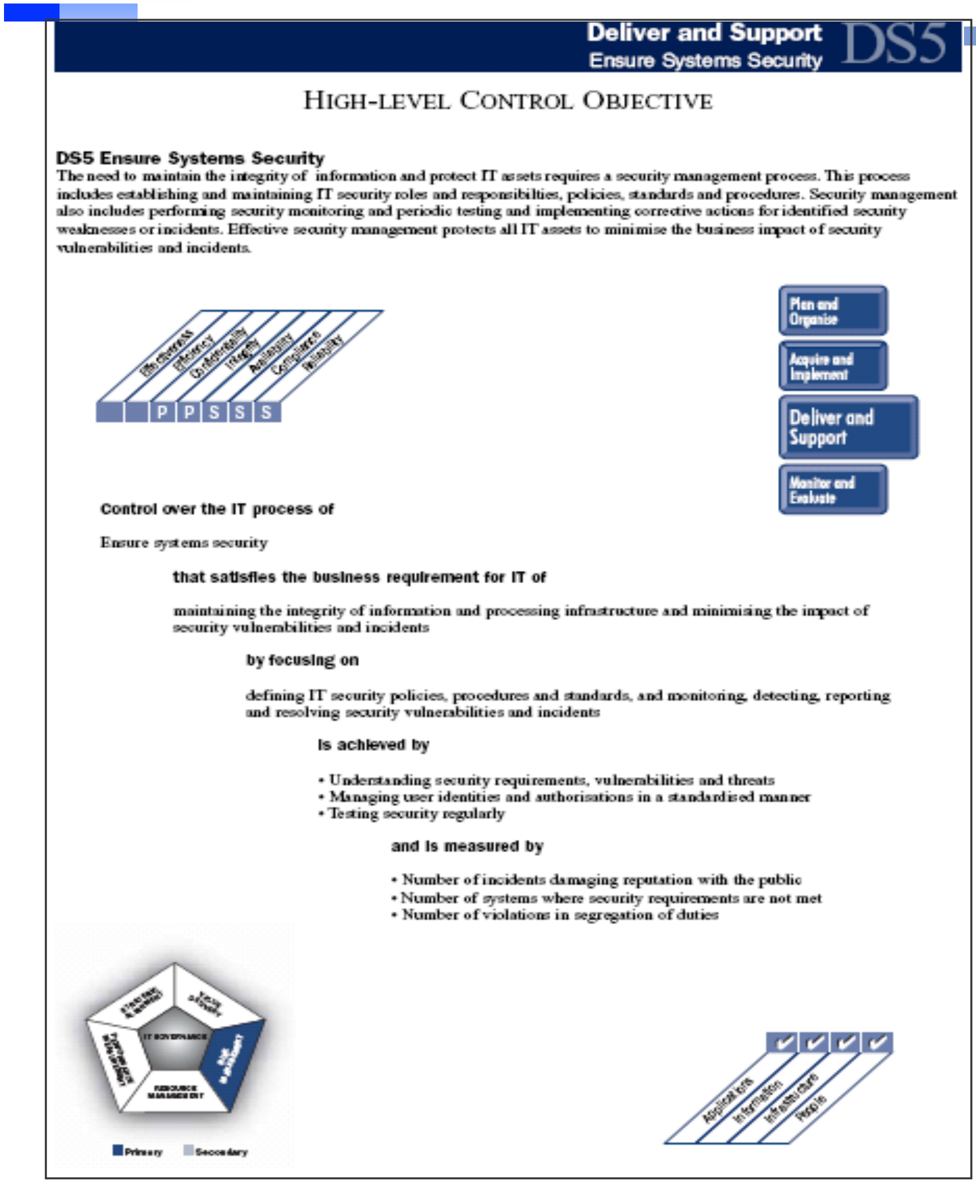
PROCESS (High-level Control Objective):

Ensure Systems Security (**DS5**)

DETAILED CONTROL OBJECTIVES:

DS 5.1	Management of IT Security
DS 5.2	IT Security Plan
DS 5.3	Identity Management
DS 5.4	User Account Management
DS 5.5	Security Testing, Surveillance and Monitoring
…	
DS 5.11	Exchange of Sensitive Data

Example of COBIT® DS5 (page 1)



Deliver and Support
Ensure Systems Security DS5

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 responsibilties, 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.

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

Process Description

IT Domains & Information Indicators

IT Goals

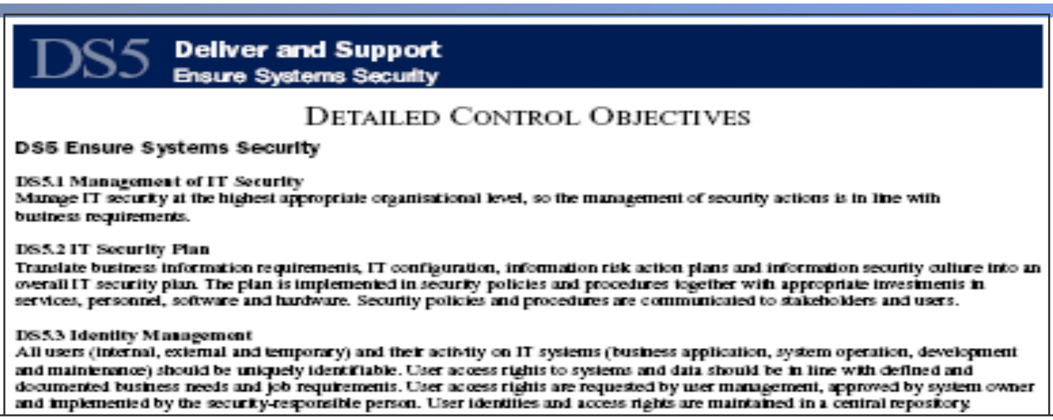
Process Goals

Key Practices/Activities

Key Metrics

IT Governance & IT Resource Indicators

Example of COBIT® 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.

Detailed Control Objectives

DS5.3 Identity Management
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

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

COBIT® Management Guidelines

COBIT 3rd Edition introduced the *Management* and *Governance* layer, providing management tools…

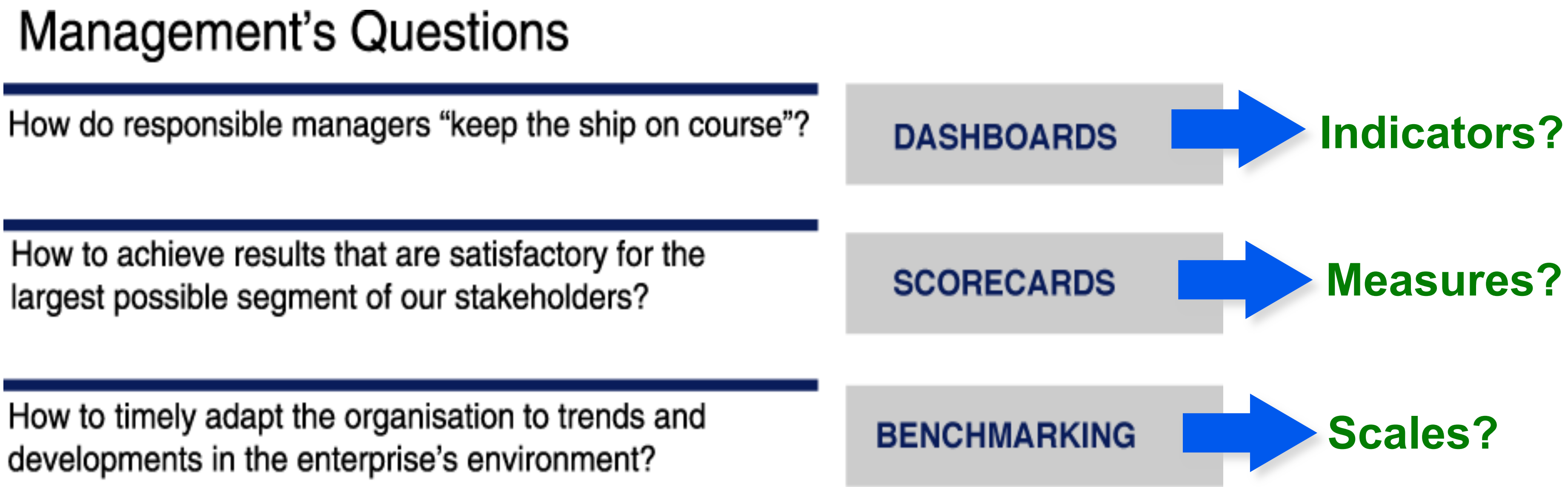
Maturity Models

RACI Charts

Process I/Os

Metrics

Goals



Management's Questions

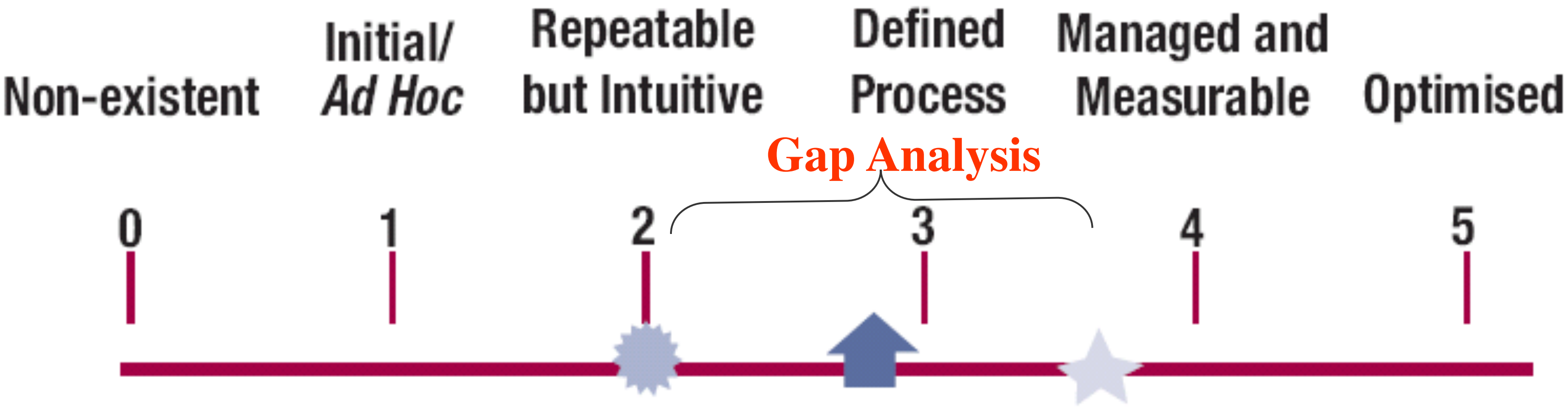
How do responsible managers "keep the ship on course"?	DASHBOARDS	Indicators?
How to achieve results that are satisfactory for the largest possible segment of our stakeholders?	SCORECARDS	Measures?
How to timely adapt the organisation to trends and developments in the enterprise's environment?	BENCHMARKING	Scales?

Monitor & Measure To Achieve Business Objectives

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

COBIT® Maturity Models

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



Non-existent
Initial/ *Ad Hoc*
Repeatable but Intuitive
Defined Process
Managed and Measurable
Optimised

Gap Analysis

LEGEND FOR SYMBOLS USED

✹ Enterprise current status

⬆ Industry average

★ Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.

1—Processes are *ad hoc* and disorganised.

2—Processes follow a regular pattern.

3—Processes are documented and communicated.

4—Processes are monitored and measured.

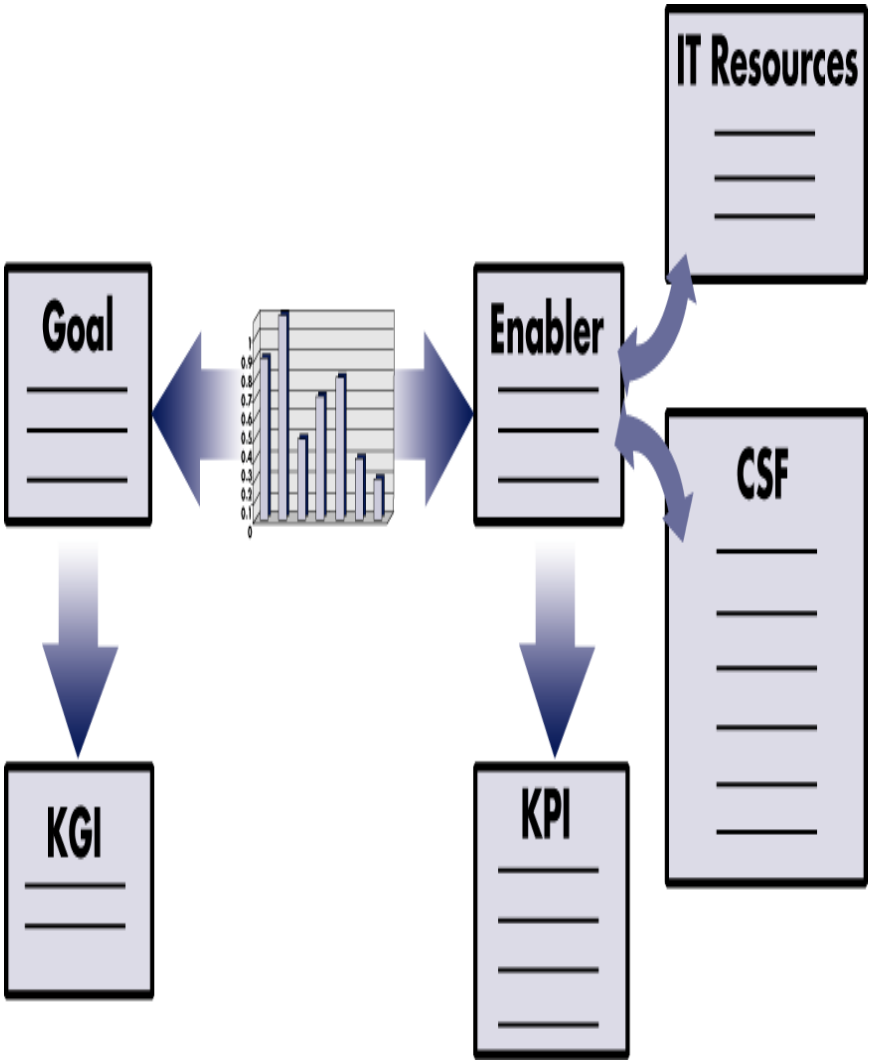
5—Good practices are followed and automated.

Metrics

Performance Indicators & Outcome Measures

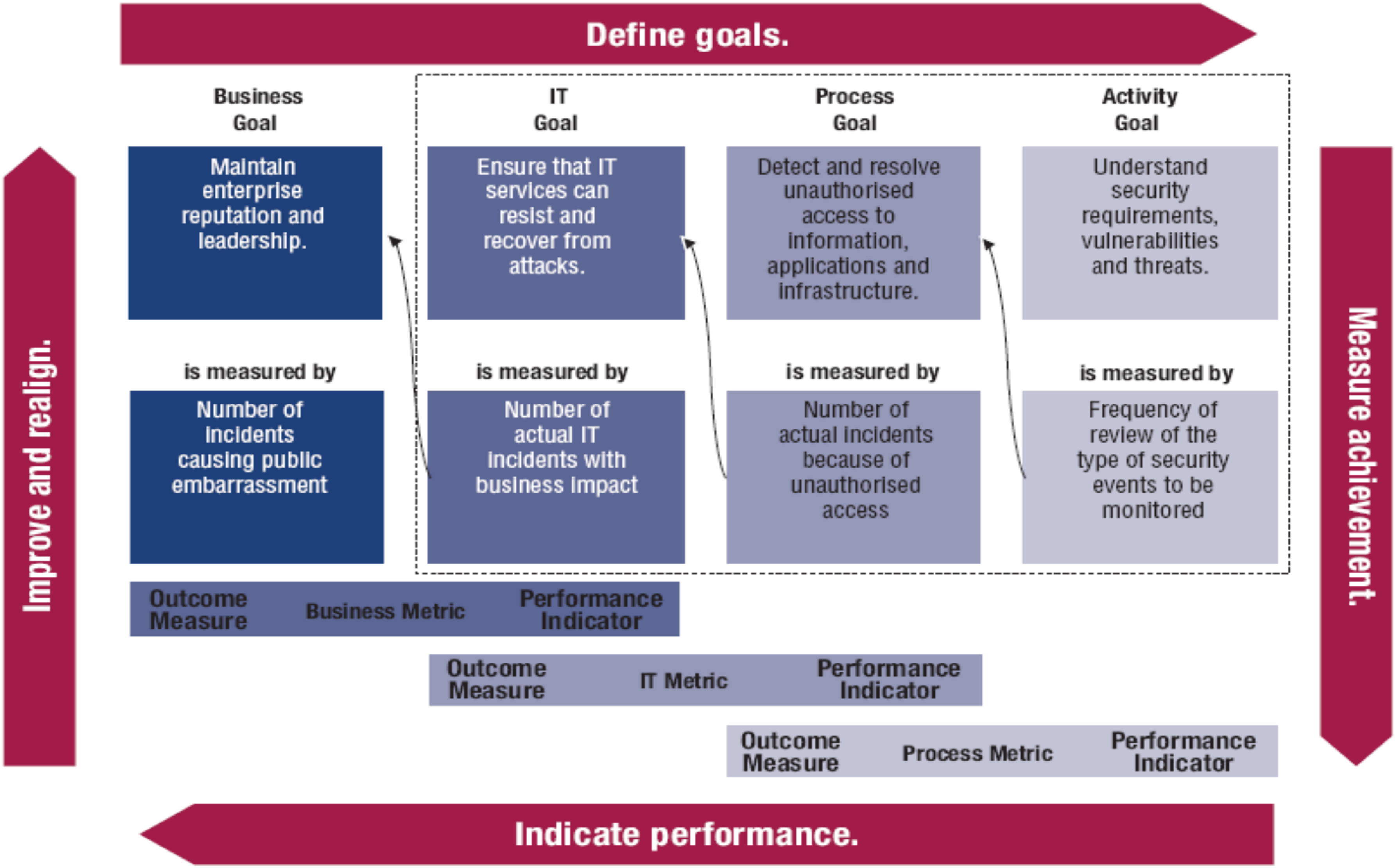
- **Performance Indicators**
  (formerly Key Performance Indicators - KPI)
  Measure how well a process is performing.

- **Outcome Measures**
  (formerly Key Goal Indicators - KGI)
  Measure whether a process achieved its business requirements.



Measuring Success

Metric & Goal Relationships



Define goals.

Business Goal	IT Goal	Process Goal	Activity Goal
Maintain enterprise reputation and leadership.	Ensure that IT services can resist and recover from attacks.	Detect and resolve unauthorised access to information, applications and infrastructure.	Understand security requirements, vulnerabilities and threats.
is measured by	is measured by	is measured by	is measured by
Number of incidents causing public embarrassment	Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored

Outcome Measure — Business Metric — Performance Indicator

Outcome Measure — IT Metric — Performance Indicator

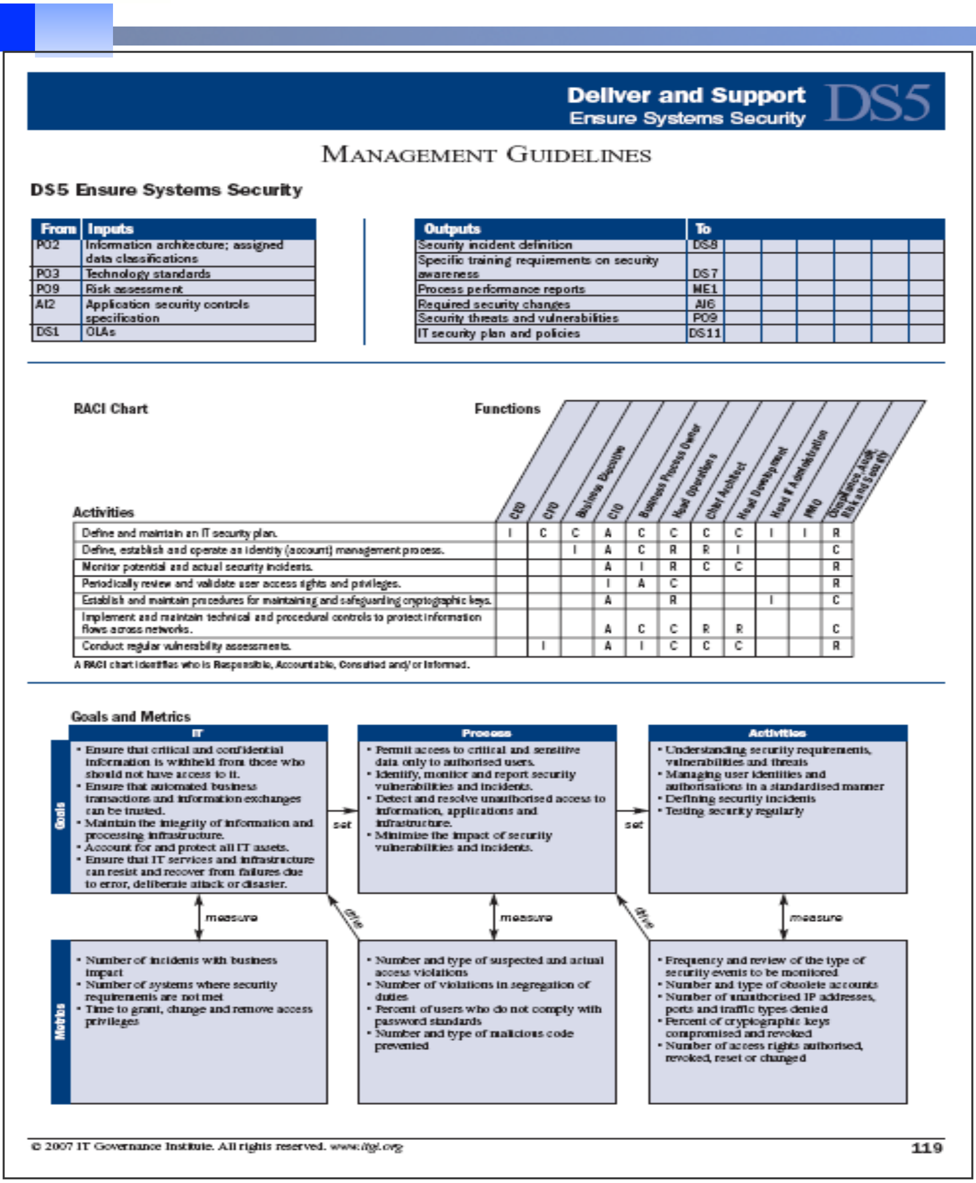
Outcome Measure — Process Metric — Performance Indicator

Improve and realign.

Measure achievement.

Indicate performance.

Example of CobiT® DS5 (page 3)



Deliver and Support DS5
Ensure Systems Security

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
IT security plan and policies	DS11

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
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

Goals

IT
- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure that 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 that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.

Process
- Permit access to critical and sensitive data only to authorised users.
- Identify, monitor and report security vulnerabilities and incidents.
- Detect and resolve unauthorised access to information, applications and infrastructure.
- Minimise the impact of security vulnerabilities and incidents.

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

Metrics

- Number of incidents with business impact
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges

- Number and type of suspected and actual access violations
- Number of violations in segregation of duties
- Percent of users who do not comply with password standards
- Number and type of malicious code prevented

- Frequency and review of the type of security events to be monitored
- Number and type of obsolete accounts
- Number of unauthorised IP addresses, ports and traffic types denied
- Percent of cryptographic keys compromised and revoked
- Number of access rights authorised, revoked, reset or changed

Management Guidelines

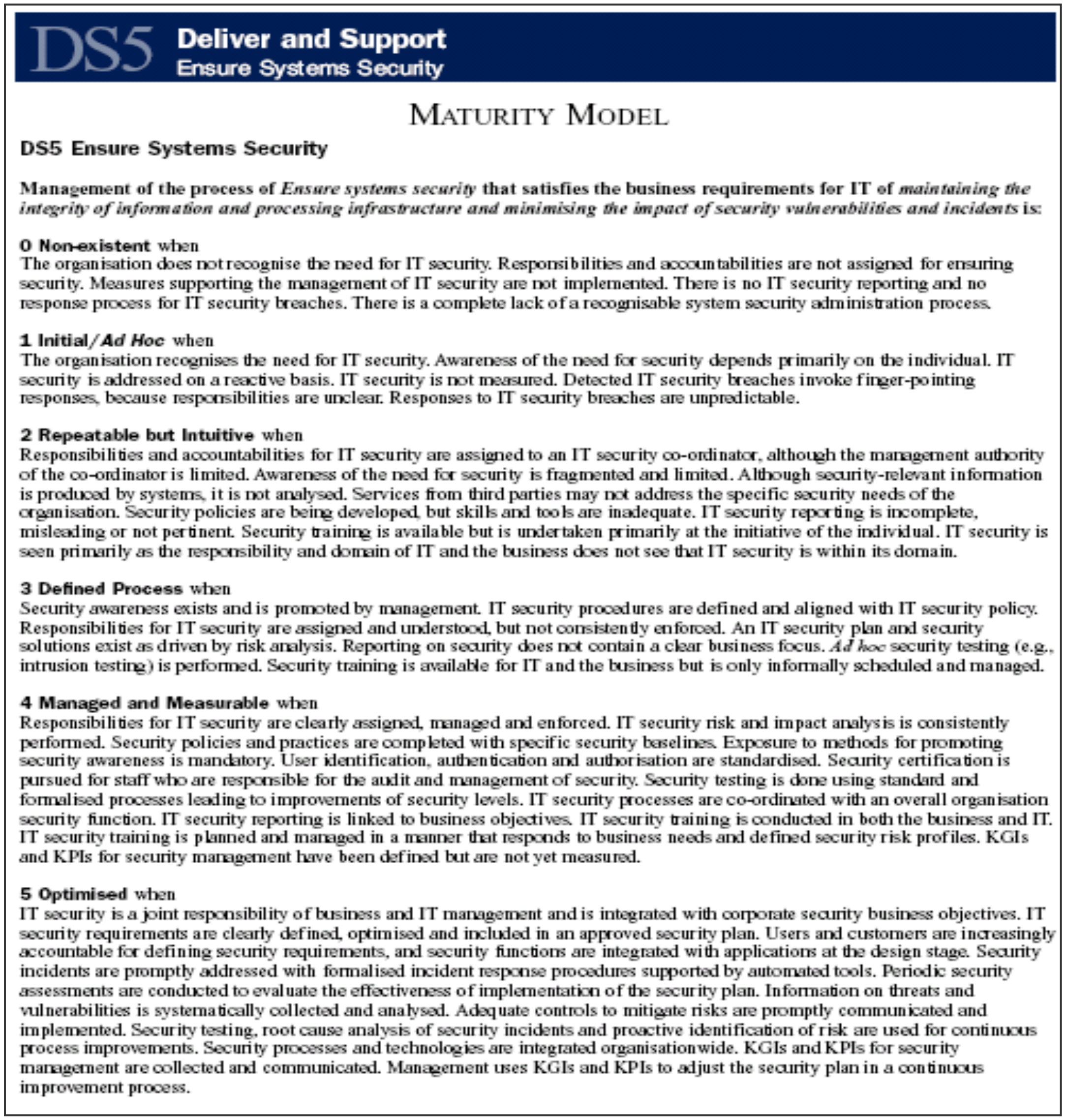
Process Relationships

RACI Chart
(Major activities and associated responsibilities)

IT Goals

Performance Metrics

Example of COBIT® 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.

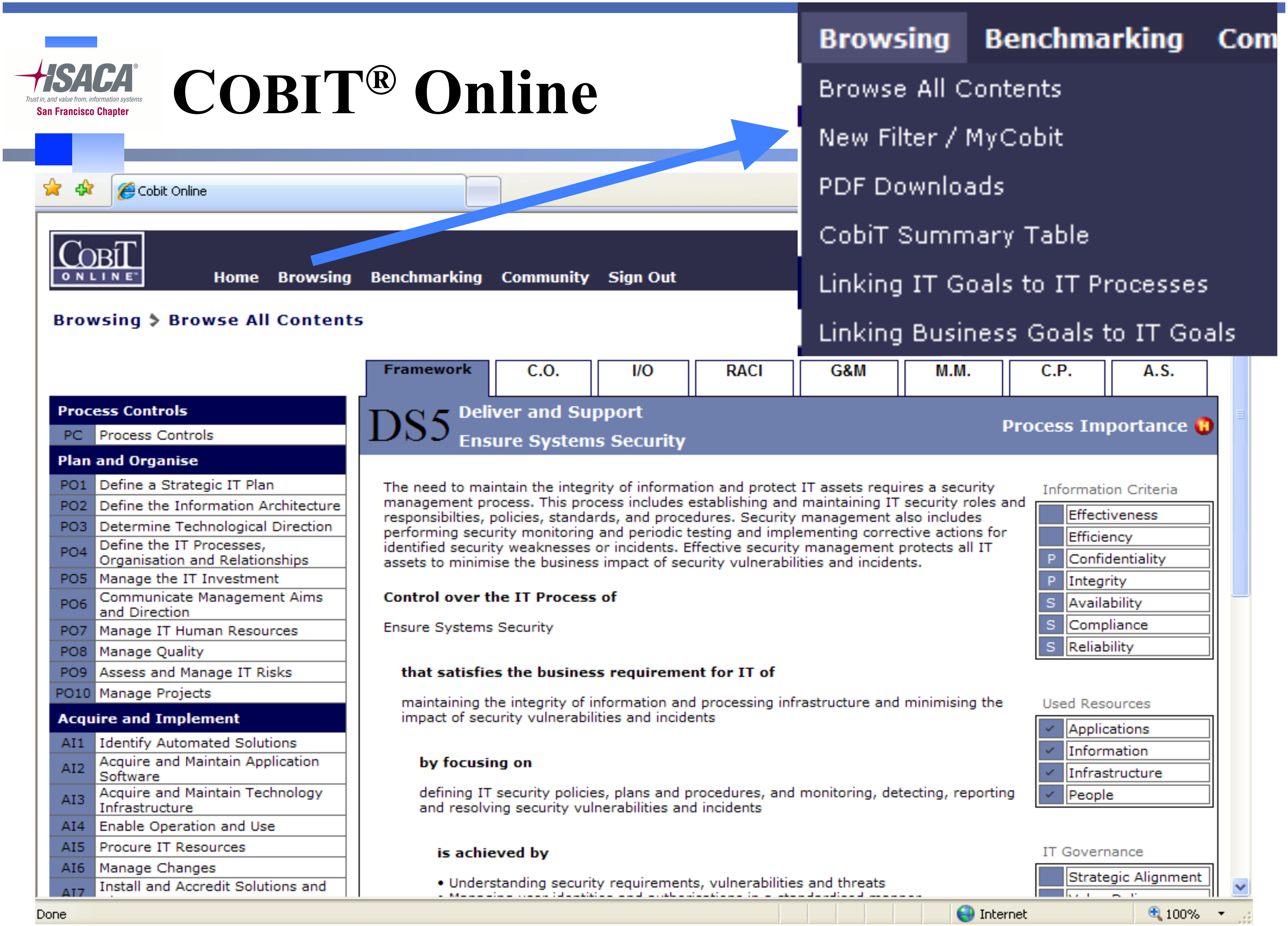
5 Optimised when
IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining 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

COBIT® 4.1 Additions

- **COBIT® IT Control Practices**
  - *Non-prescriptive control designs* for achieving the control objectives
  - Describing the necessary and sufficient steps to *achieve* control objectives
  - *Action-oriented*, enabling timely execution
  - *Measurable* and *relevant* to the purpose of each control objective
  - Cover all *inputs, activities*, and *outputs* of the processes
  - Support clear *roles* and *responsibilities* (including segregation of duties)
  - Generic and specific practices
- **IT Assurance Guide Using COBIT®**
  - Testing of control approaches covering 4 assurance objectives
    - 1) Existence, 2) Design Effectiveness, 3) Operating Effectiveness, 4) Design & Operating Efficiency
  - Provide 3 types of assurance guidance
    - 1) Testing suggested control design, 2)Testing control objective achievement, 3) Documenting impact of control weakness
  - Tests based on a documented taxonomy of relevant assurance methods
    - Inquire and confirm, inspect, observe, re-perform or re-calculate, automated evidence collection and analysis

COBIT® Online



Browsing > Browse All Contents

Process Controls	
PC	Process Controls
Plan and Organise	
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and

DS5 Deliver and Support
Ensure Systems Security

Process Importance H

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 responsibilties, 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.

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, plans and procedures, 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

Information Criteria

	Effectiveness
	Efficiency
P	Confidentiality
P	Integrity
S	Availability
S	Compliance
S	Reliability

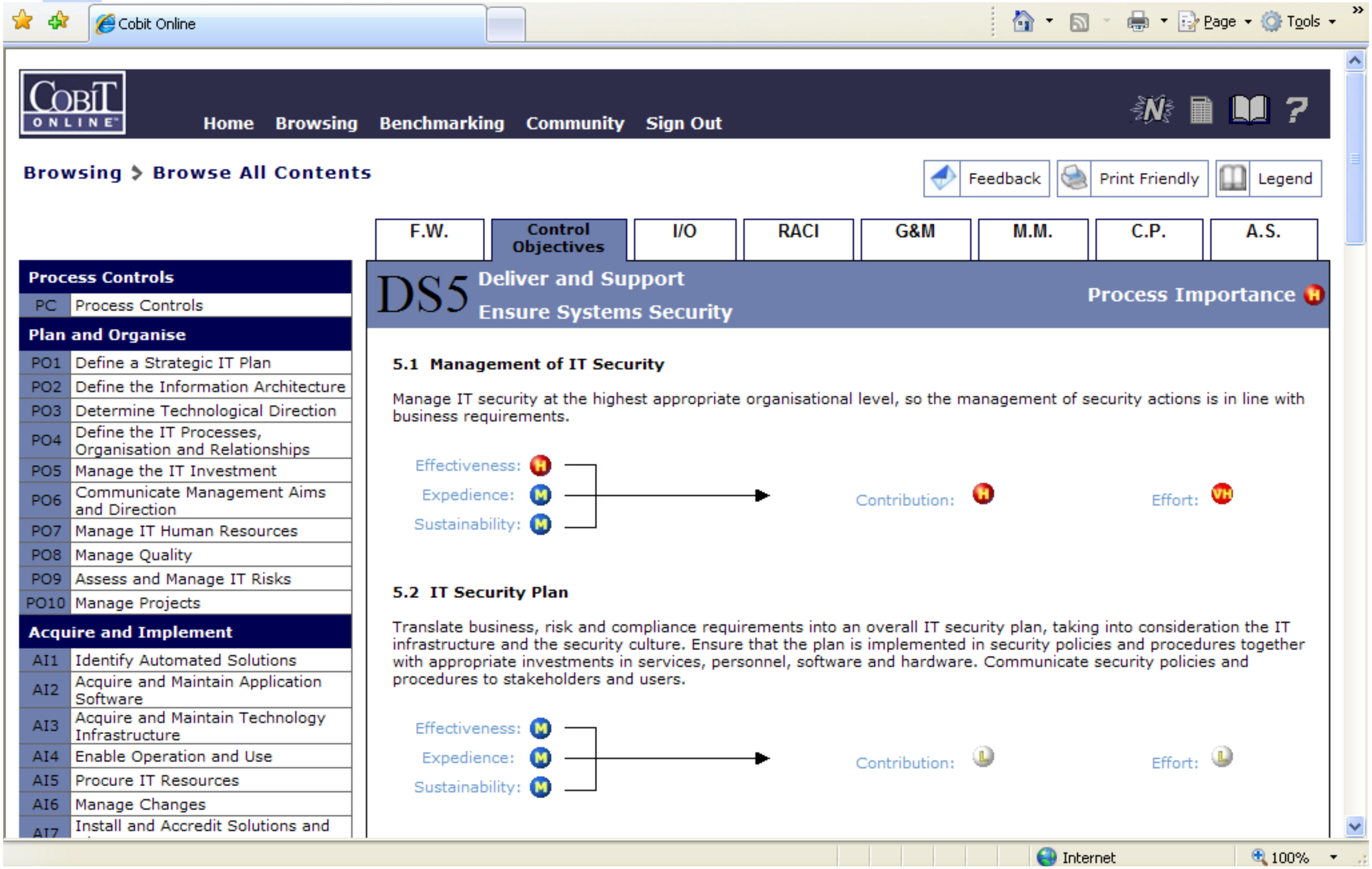
Used Resources

✓	Applications
✓	Information
✓	Infrastructure
✓	People

IT Governance

	Strategic Alignment
	Value Delivery

COBIT® Online



Browsing > Browse All Contents

Process Controls	
PC	Process Controls
Plan and Organise	
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and

DS5 Deliver and Support
Ensure Systems Security

Process Importance H

5.1 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.

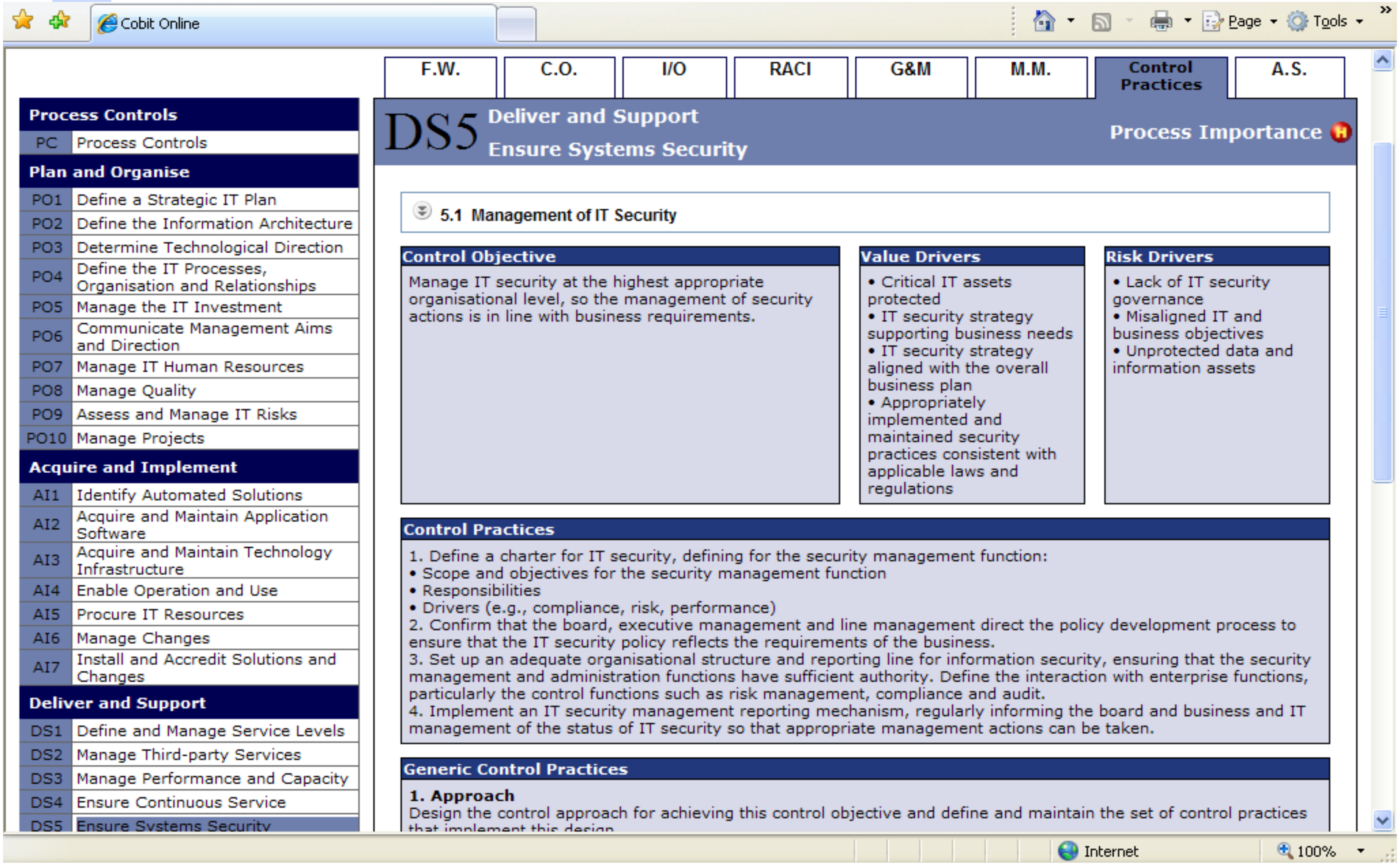
Effectiveness: H
Expedience: M
Sustainability: M
Contribution: H
Effort: VH

5.2 IT Security Plan

Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

Effectiveness: M
Expedience: M
Sustainability: M
Contribution: L
Effort: L

COBIT® Online



Process Controls	
PC	Process Controls
Plan and Organise	
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes
Deliver and Support	
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security

DS5 Deliver and Support
Ensure Systems Security

Process Importance H

5.1 Management of IT Security

Control Objective

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

Value Drivers

- Critical IT assets protected
- IT security strategy supporting business needs
- IT security strategy aligned with the overall business plan
- Appropriately implemented and maintained security practices consistent with applicable laws and regulations

Risk Drivers

- Lack of IT security governance
- Misaligned IT and business objectives
- Unprotected data and information assets

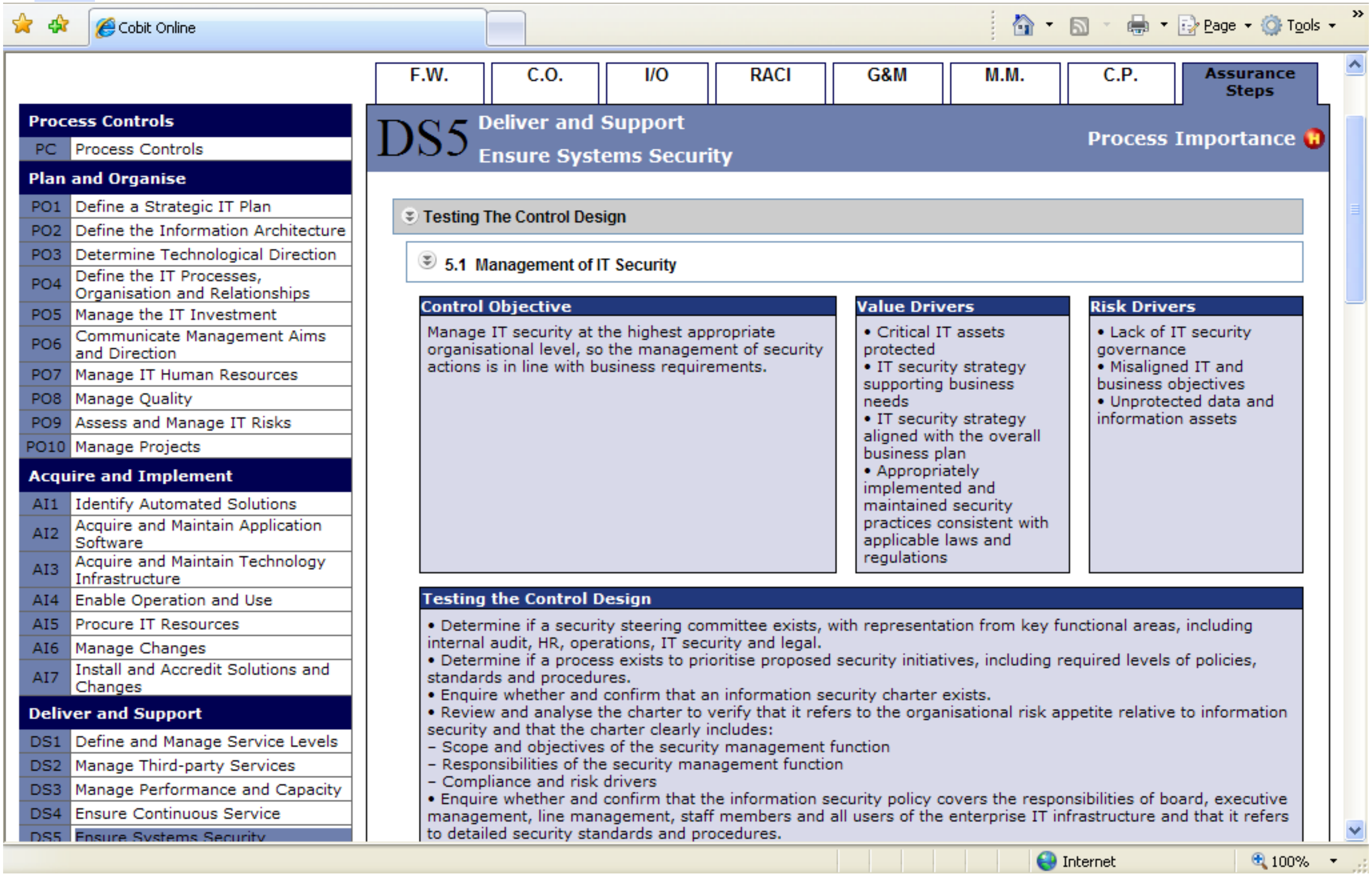
Control Practices

1. Define a charter for IT security, defining for the security management function:
- Scope and objectives for the security management function
- Responsibilities
- Drivers (e.g., compliance, risk, performance)
2. Confirm that the board, executive management and line management direct the policy development process to ensure that the IT security policy reflects the requirements of the business.
3. Set up an adequate organisational structure and reporting line for information security, ensuring that the security management and administration functions have sufficient authority. Define the interaction with enterprise functions, particularly the control functions such as risk management, compliance and audit.
4. Implement an IT security management reporting mechanism, regularly informing the board and business and IT management of the status of IT security so that appropriate management actions can be taken.

Generic Control Practices

1. Approach
Design the control approach for achieving this control objective and define and maintain the set of control practices that implement this design

COBIT® Online



Process Controls	
PC	Process Controls
Plan and Organise	
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes
Deliver and Support	
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security

DS5 Deliver and Support — Ensure Systems Security

Process Importance H

Testing The Control Design

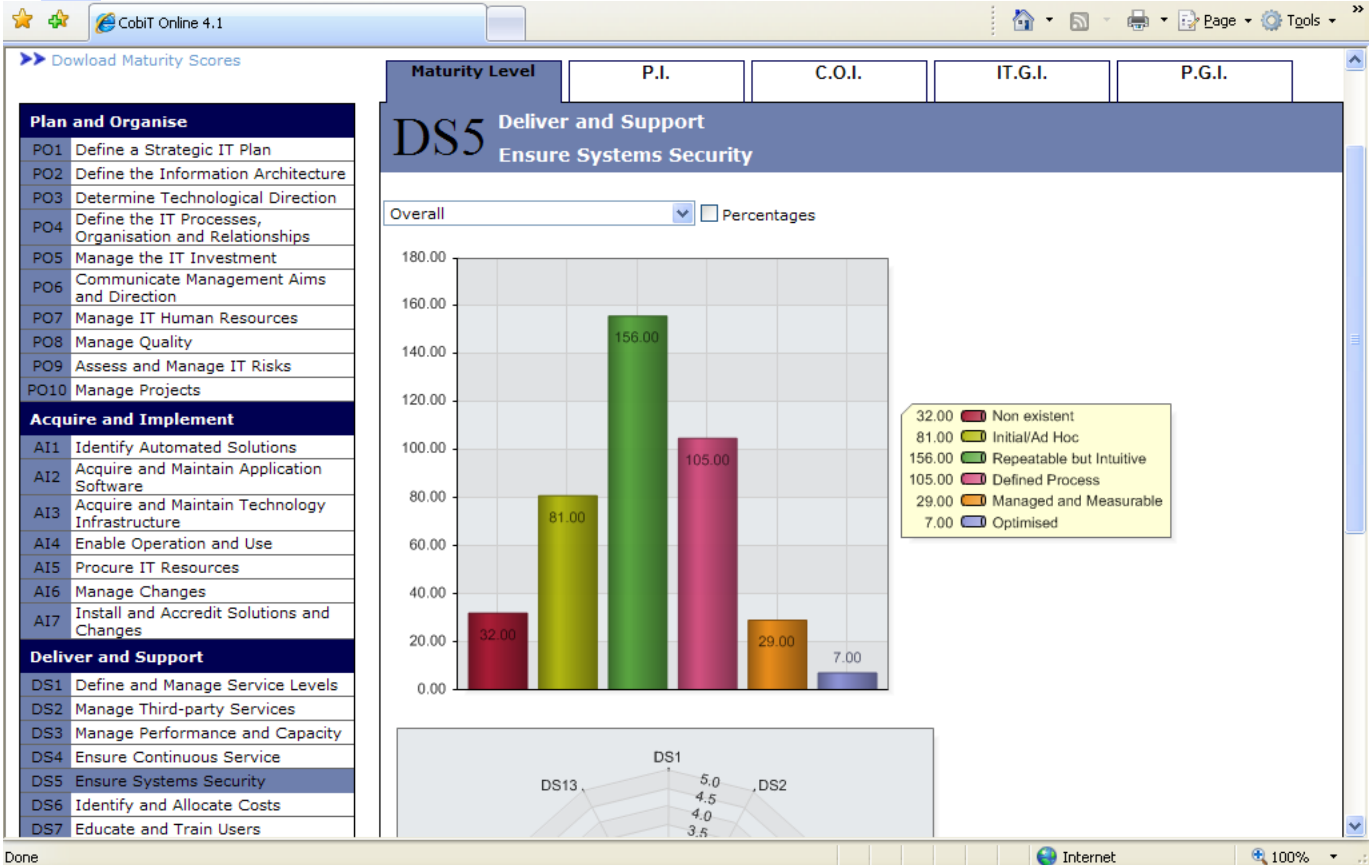
5.1 Management of IT Security

Control Objective	Value Drivers	Risk Drivers
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.	• Critical IT assets protected • IT security strategy supporting business needs • IT security strategy aligned with the overall business plan • Appropriately implemented and maintained security practices consistent with applicable laws and regulations	• Lack of IT security governance • Misaligned IT and business objectives • Unprotected data and information assets

Testing the Control Design

• Determine if a security steering committee exists, with representation from key functional areas, including internal audit, HR, operations, IT security and legal.
• Determine if a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures.
• Enquire whether and confirm that an information security charter exists.
• Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security and that the charter clearly includes:
– Scope and objectives of the security management function
– Responsibilities of the security management function
– Compliance and risk drivers
• Enquire whether and confirm that the information security policy covers the responsibilities of board, executive management, line management, staff members and all users of the enterprise IT infrastructure and that it refers to detailed security standards and procedures.

COBIT® Online



CobiT Online 4.1

Page Tools

>> Dowload Maturity Scores

Maturity Level | P.I. | C.O.I. | IT.G.I. | P.G.I.

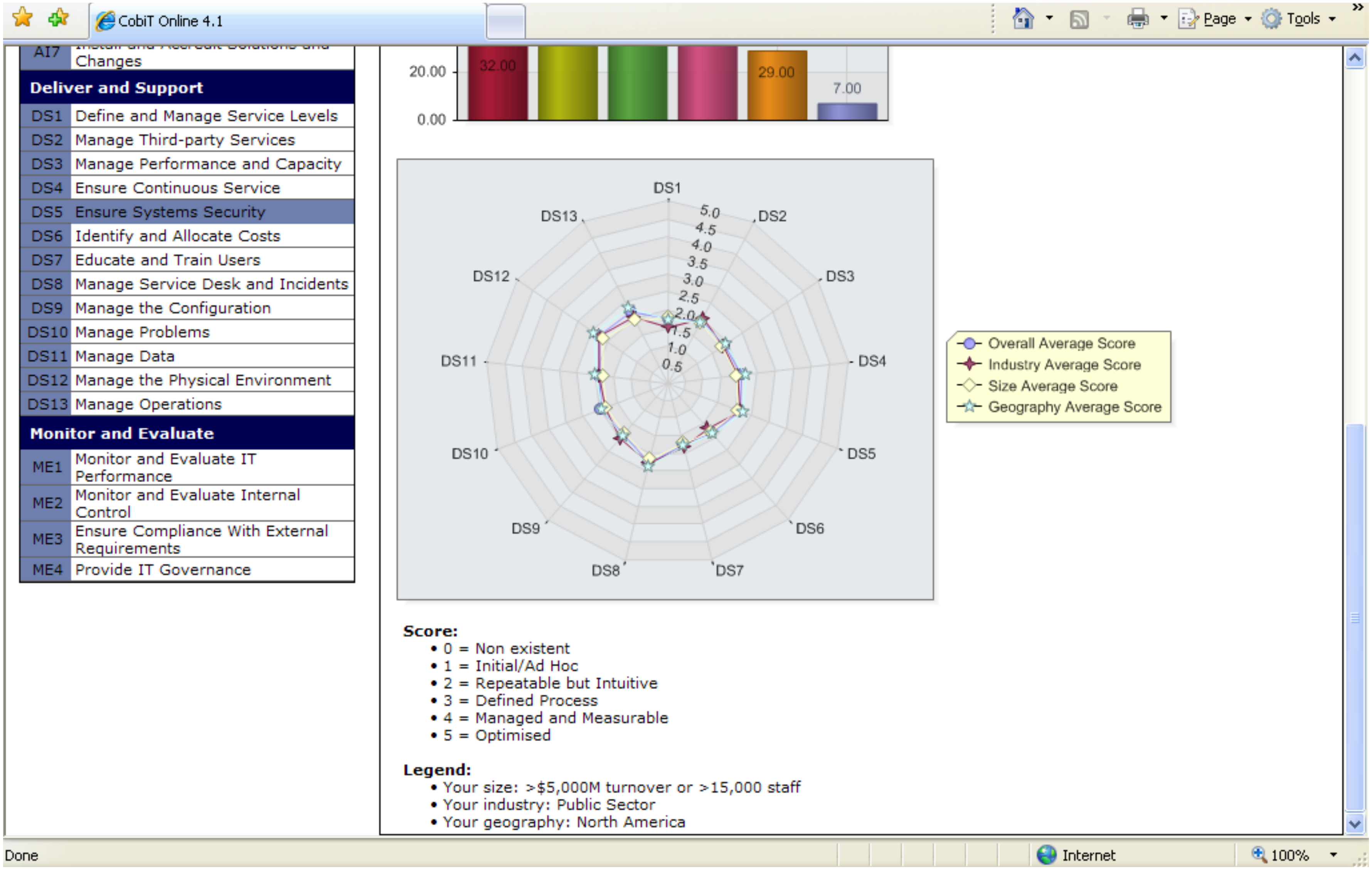
Plan and Organise	
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes
Deliver and Support	
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users

DS5 Deliver and Support
Ensure Systems Security

Overall ▾ □ Percentages

32.00	🟥	Non existent
81.00	🟨	Initial/Ad Hoc
156.00	🟩	Repeatable but Intuitive
105.00	🟥	Defined Process
29.00	🟧	Managed and Measurable
7.00	🟦	Optimised

COBIT® Online



AI7	Changes
Deliver and Support	
DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations
Monitor and Evaluate	
ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance With External Requirements
ME4	Provide IT Governance

Score:

- 0 = Non existent
- 1 = Initial/Ad Hoc
- 2 = Repeatable but Intuitive
- 3 = Defined Process
- 4 = Managed and Measurable
- 5 = Optimised

Legend:

- Your size: >$5,000M turnover or >15,000 staff
- Your industry: Public Sector
- Your geography: North America

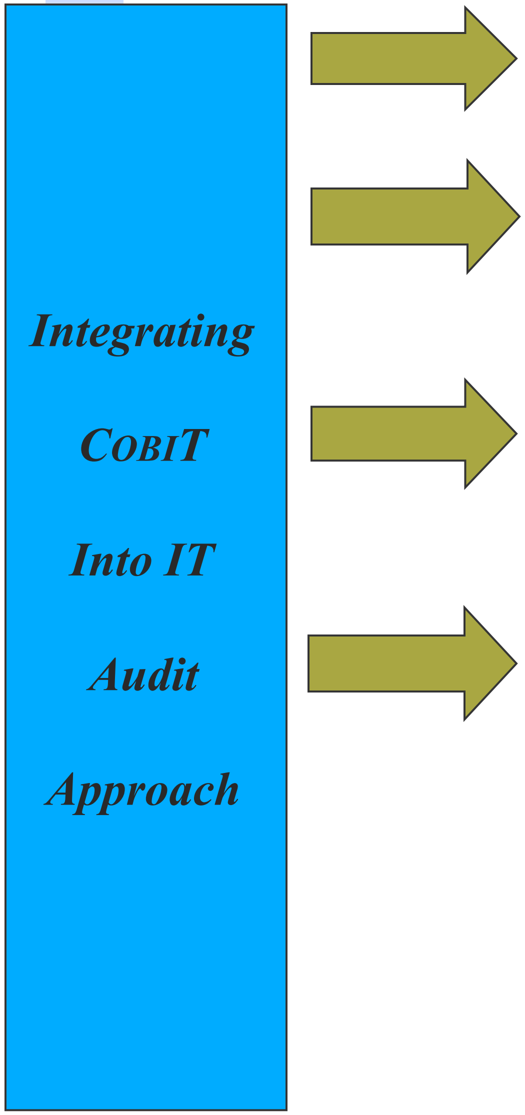
Summary
COBIT's® Value As A Framework

- Enables the **auditor** to review specific IT processes against COBIT's *Control Objectives* to determine where controls are sufficient or advise management where controls over processes need to be improved.
- Helps **process owners** answer questions - "Is what I'm doing adequate and in line with **good 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" processes and controls should be in place. An effective implementation requires that COBIT® be supplemented with other sources of industry standards and "good practice" that prescribe the "how" for controlled process execution.

AGENDA

- Overview of COBIT®
- **Integrating COBIT® Domains into IT Audit Planning & Scope Development**
- Integrating COBIT® into the IT Audit Lifecycle
- COBIT 5 Update
- Summary & Wrap-up

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*

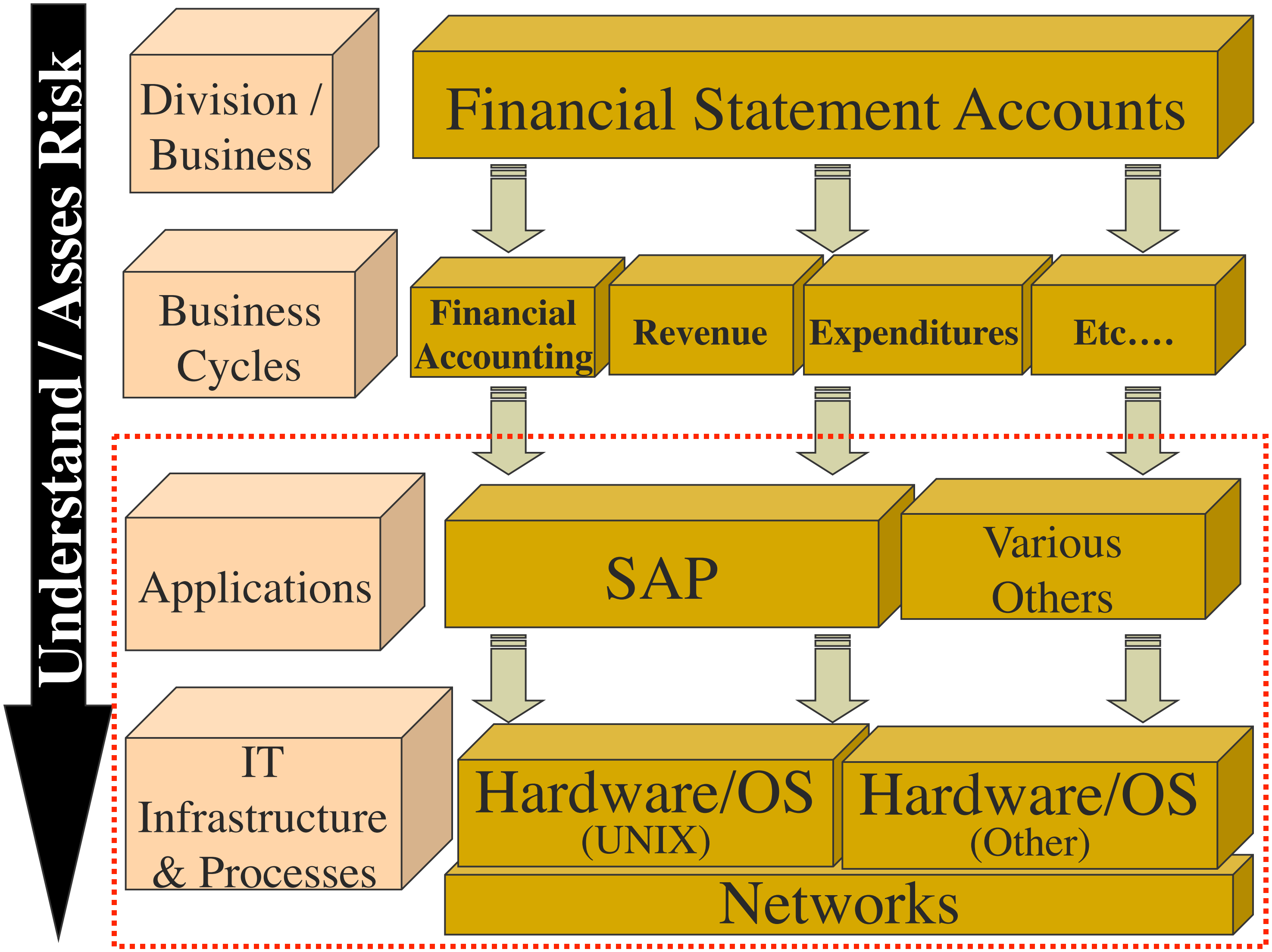
ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Mapping COBIT® to the *Technology Audit Universe*

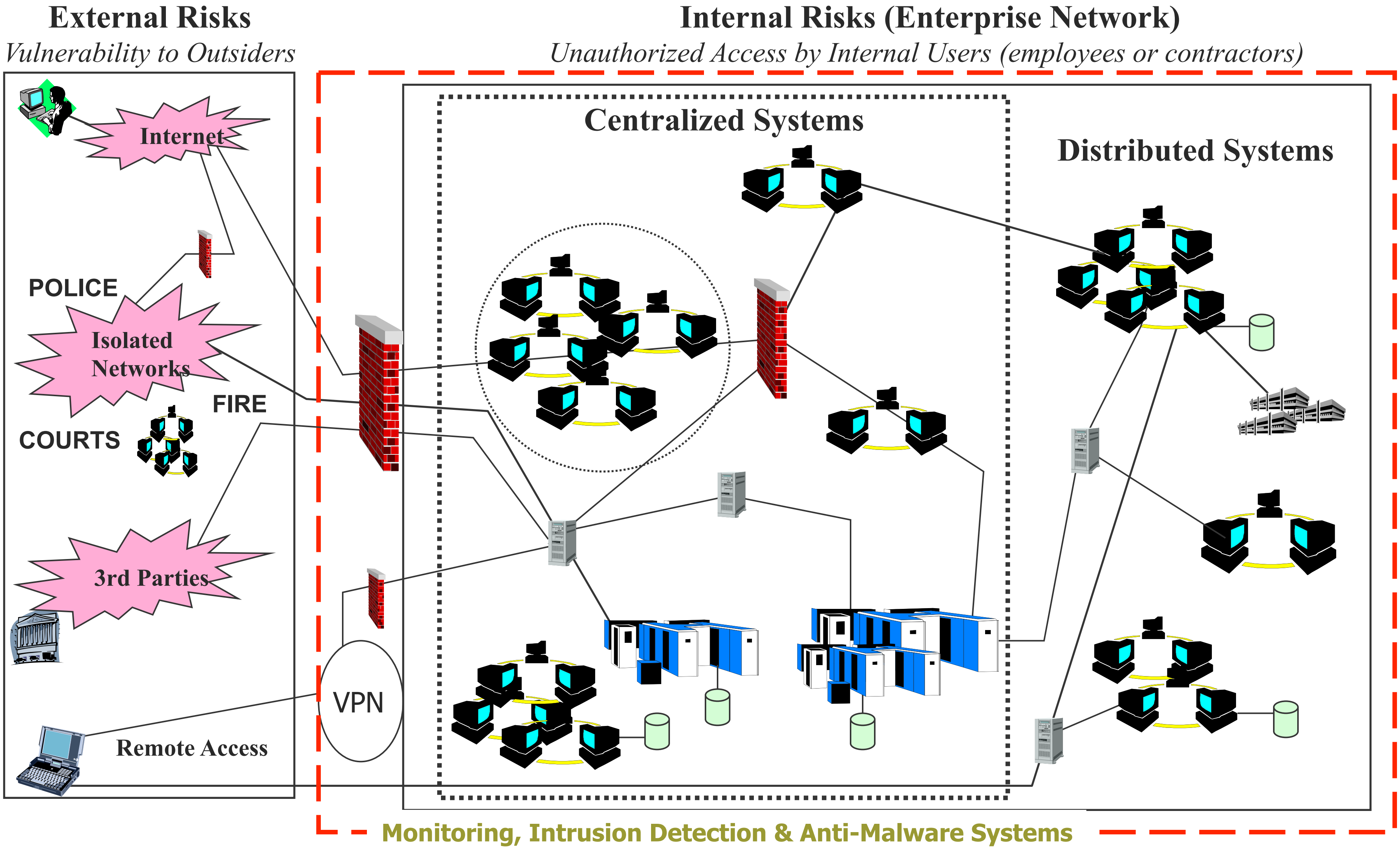
Unraveling the *Technology Audit Universe*



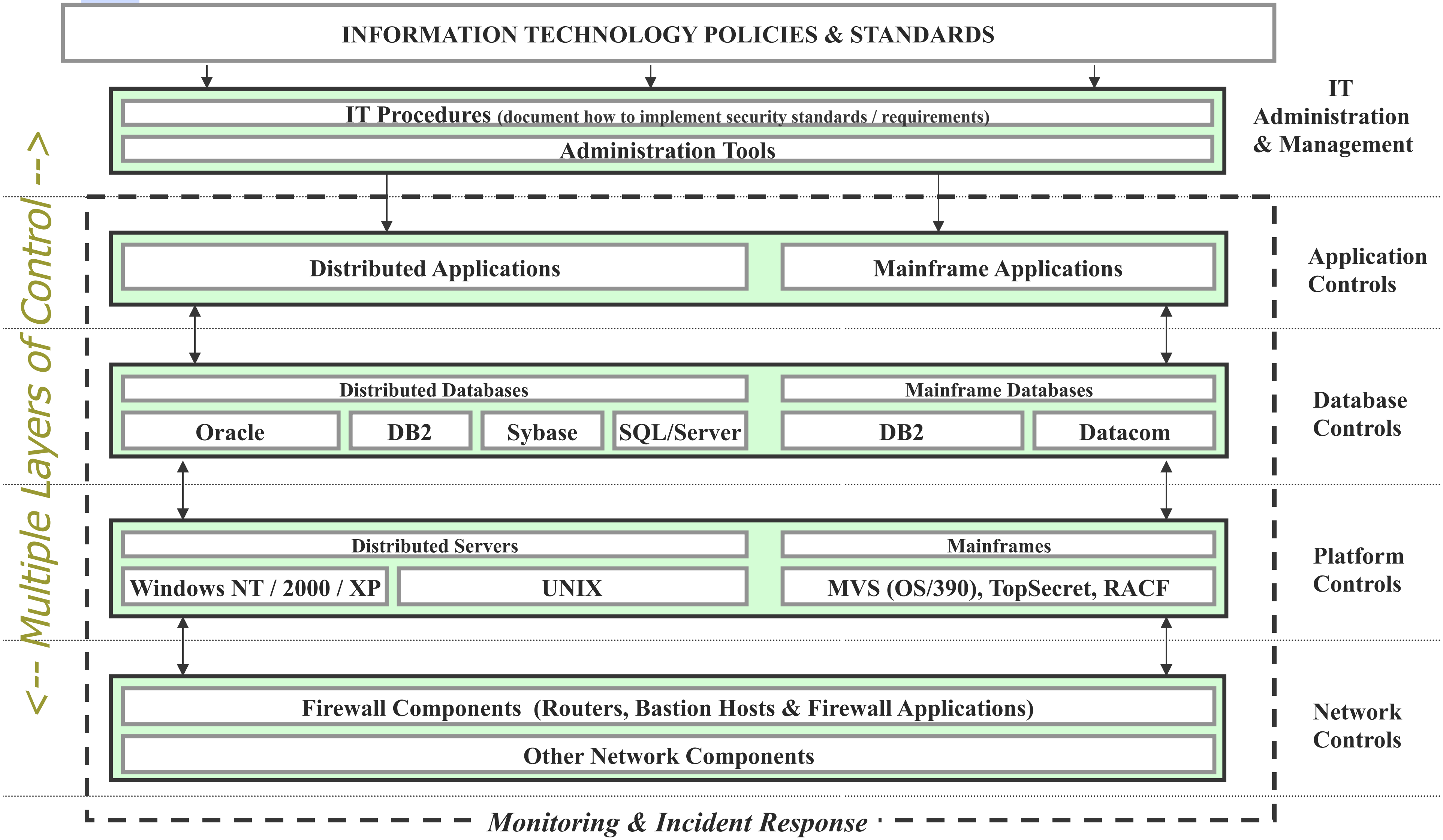
STEPS

1. Identify mission critical business cycles.
2. Identify applications supporting those cycles.
3. Identify technology and infrastructure components.
4. Identify IT process universe.
5. Identify and assess risk.

Understanding the Technology Infrastructure


External Risks
Vulnerability to Outsiders
Internal Risks (Enterprise Network)
Unauthorized Access by Internal Users (employees or contractors)
Internet
POLICE
Isolated Networks
FIRE
COURTS
3rd Parties
Remote Access
VPN
Centralized Systems
Distributed Systems
Monitoring, Intrusion Detection & Anti-Malware Systems

Understand Relevant Technology "Layers"



INFORMATION TECHNOLOGY POLICIES & STANDARDS

IT Procedures (document how to implement security standards / requirements)

Administration Tools

IT Administration & Management

Distributed Applications

Mainframe Applications

Application Controls

Distributed Databases

Oracle

DB2

Sybase

SQL/Server

Mainframe Databases

DB2

Datacom

Database Controls

Distributed Servers

Windows NT / 2000 / XP

UNIX

Mainframes

MVS (OS/390), TopSecret, RACF

Platform Controls

Firewall Components (Routers, Bastion Hosts & Firewall Applications)

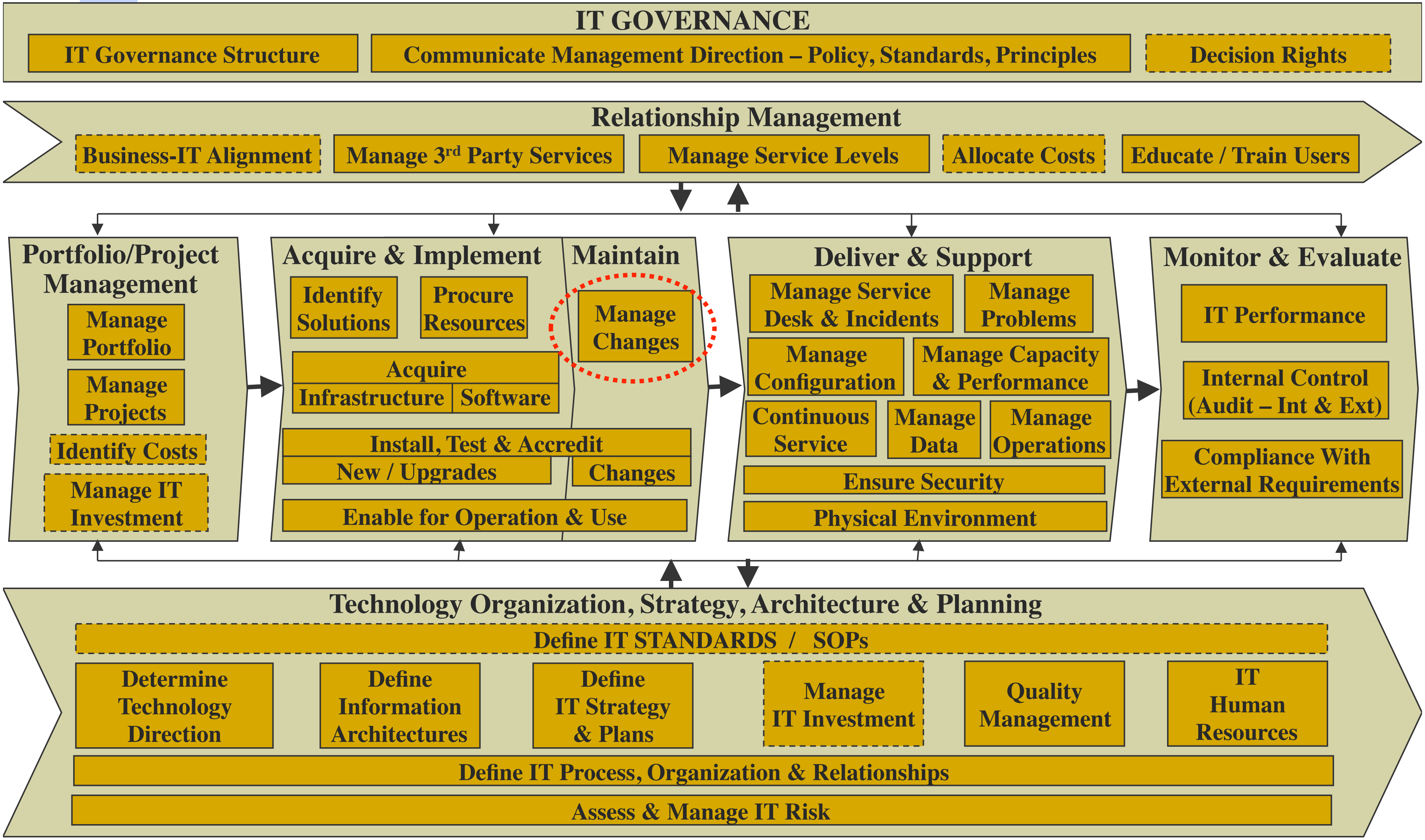
Other Network Components

Network Controls

<-- Multiple Layers of Control -->

Monitoring & Incident Response

Understanding the *Process Universe*



IT GOVERNANCE

IT Governance Structure

Communicate Management Direction – Policy, Standards, Principles

Decision Rights

Relationship Management

Business-IT Alignment

Manage 3rd Party Services

Manage Service Levels

Allocate Costs

Educate / Train Users

Portfolio/Project Management

Manage Portfolio

Manage Projects

Identify Costs

Manage IT Investment

Acquire & Implement

Identify Solutions

Procure Resources

Acquire

Infrastructure

Software

Install, Test & Accredit

New / Upgrades

Enable for Operation & Use

Maintain

Manage Changes

Changes

Deliver & Support

Manage Service Desk & Incidents

Manage Problems

Manage Configuration

Manage Capacity & Performance

Continuous Service

Manage Data

Manage Operations

Ensure Security

Physical Environment

Monitor & Evaluate

IT Performance

Internal Control (Audit – Int & Ext)

Compliance With External Requirements

Technology Organization, Strategy, Architecture & Planning

Define IT STANDARDS / SOPs

Determine Technology Direction

Define Information Architectures

Define IT Strategy & Plans

Manage IT Investment

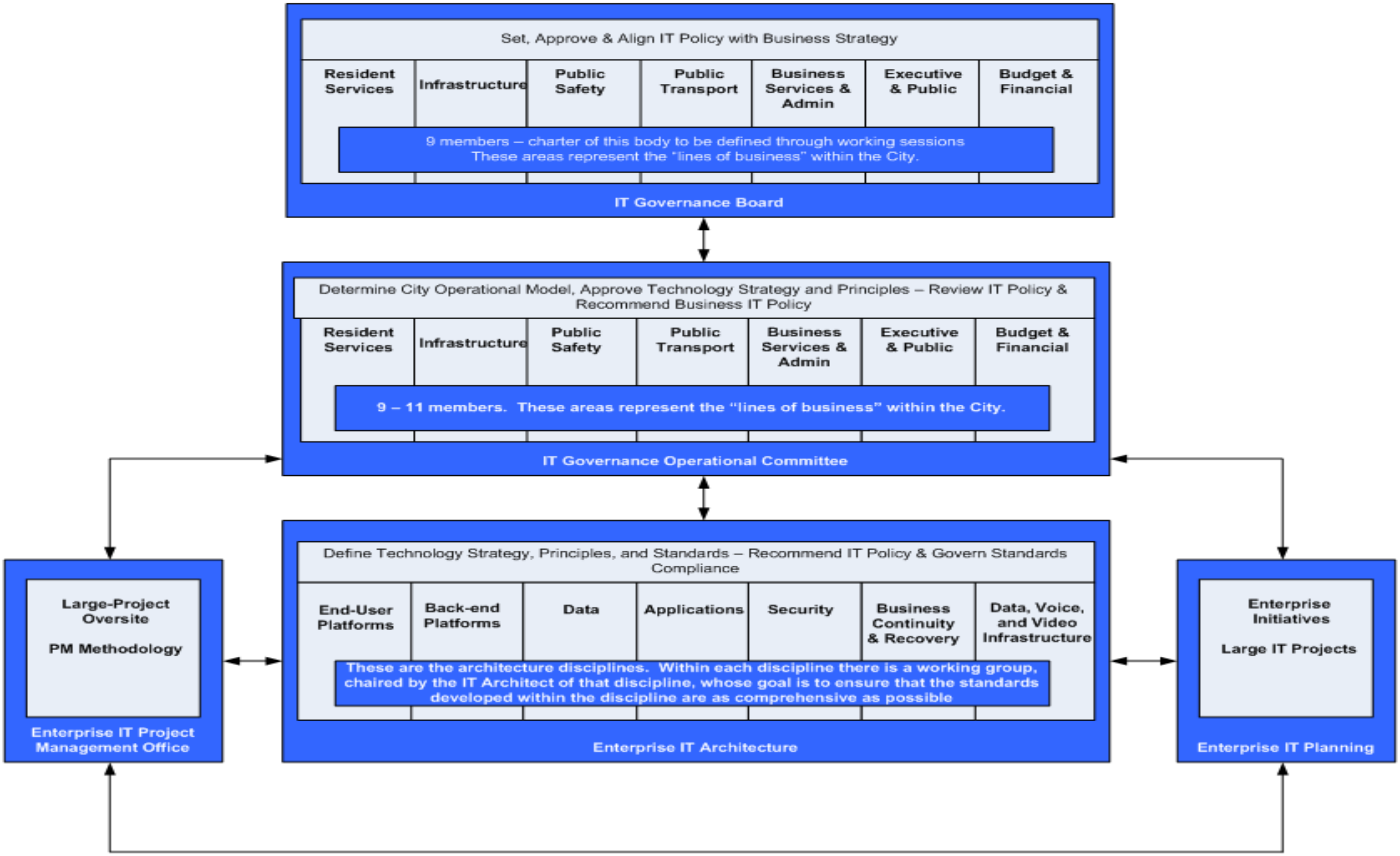
Quality Management

IT Human Resources

Define IT Process, Organization & Relationships

Assess & Manage IT Risk

Understanding the IT Governance Structure



Set, Approve & Align IT Policy with Business Strategy

Resident Services	Infrastructure	Public Safety	Public Transport	Business Services & Admin	Executive & Public	Budget & Financial

9 members – charter of this body to be defined through working sessions
These areas represent the "lines of business" within the City.

IT Governance Board

Determine City Operational Model, Approve Technology Strategy and Principles – Review IT Policy & Recommend Business IT Policy

Resident Services	Infrastructure	Public Safety	Public Transport	Business Services & Admin	Executive & Public	Budget & Financial

9 – 11 members. These areas represent the "lines of business" within the City.

IT Governance Operational Committee

Define Technology Strategy, Principles, and Standards – Recommend IT Policy & Govern Standards Compliance

End-User Platforms	Back-end Platforms	Data	Applications	Security	Business Continuity & Recovery	Data, Voice, and Video Infrastructure

These are the architecture disciplines. Within each discipline there is a working group, chaired by the IT Architect of that discipline, whose goal is to ensure that the standards developed within the discipline are as comprehensive as possible

Enterprise IT Architecture

Large-Project Oversite

PM Methodology

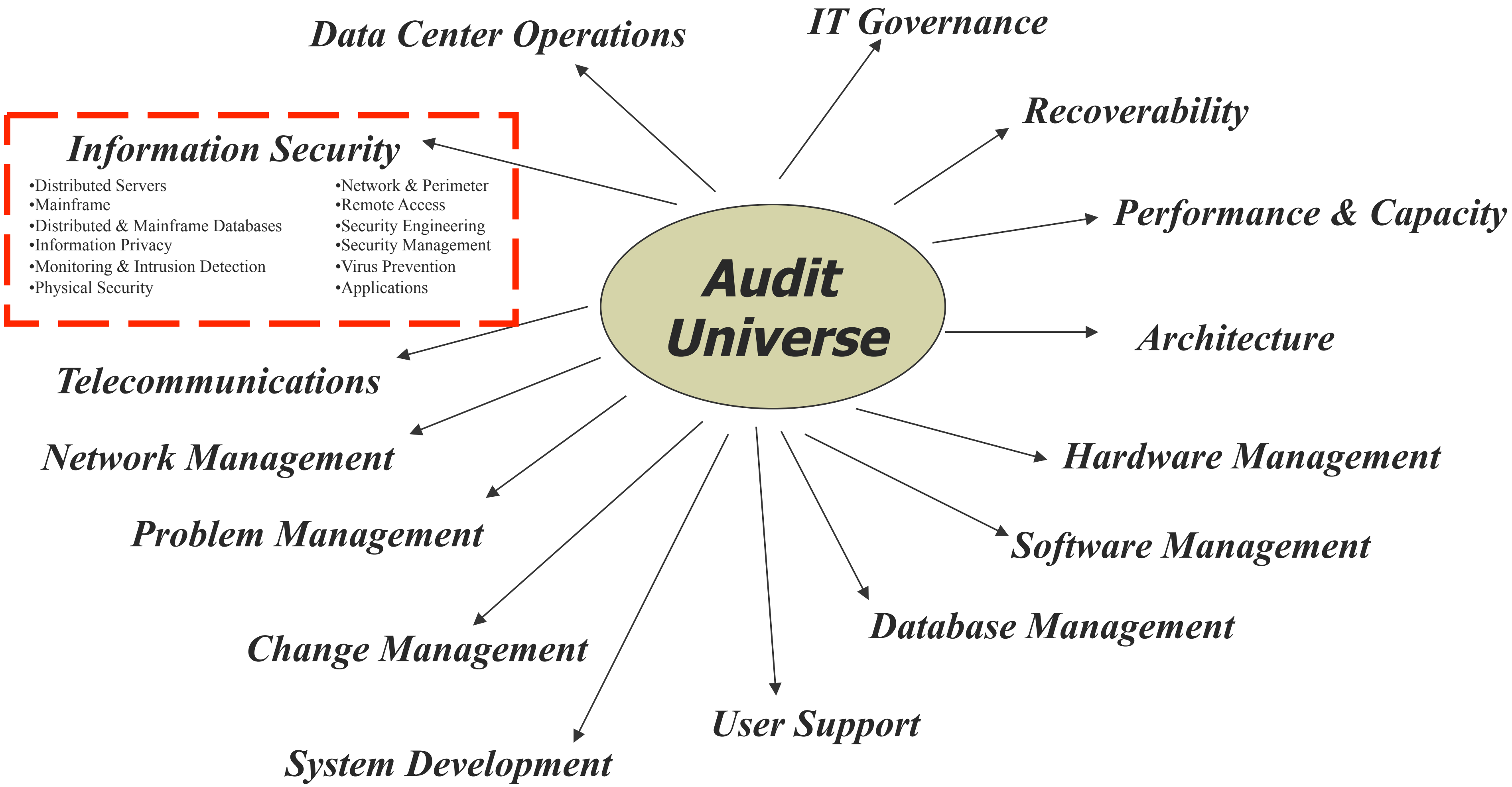
Enterprise IT Project Management Office

Enterprise Initiatives

Large IT Projects

Enterprise IT Planning

Defining the *Technology Audit Universe*



Audit Universe

Data Center Operations

IT Governance

Recoverability

Performance & Capacity

Architecture

Hardware Management

Software Management

Database Management

User Support

System Development

Change Management

Problem Management

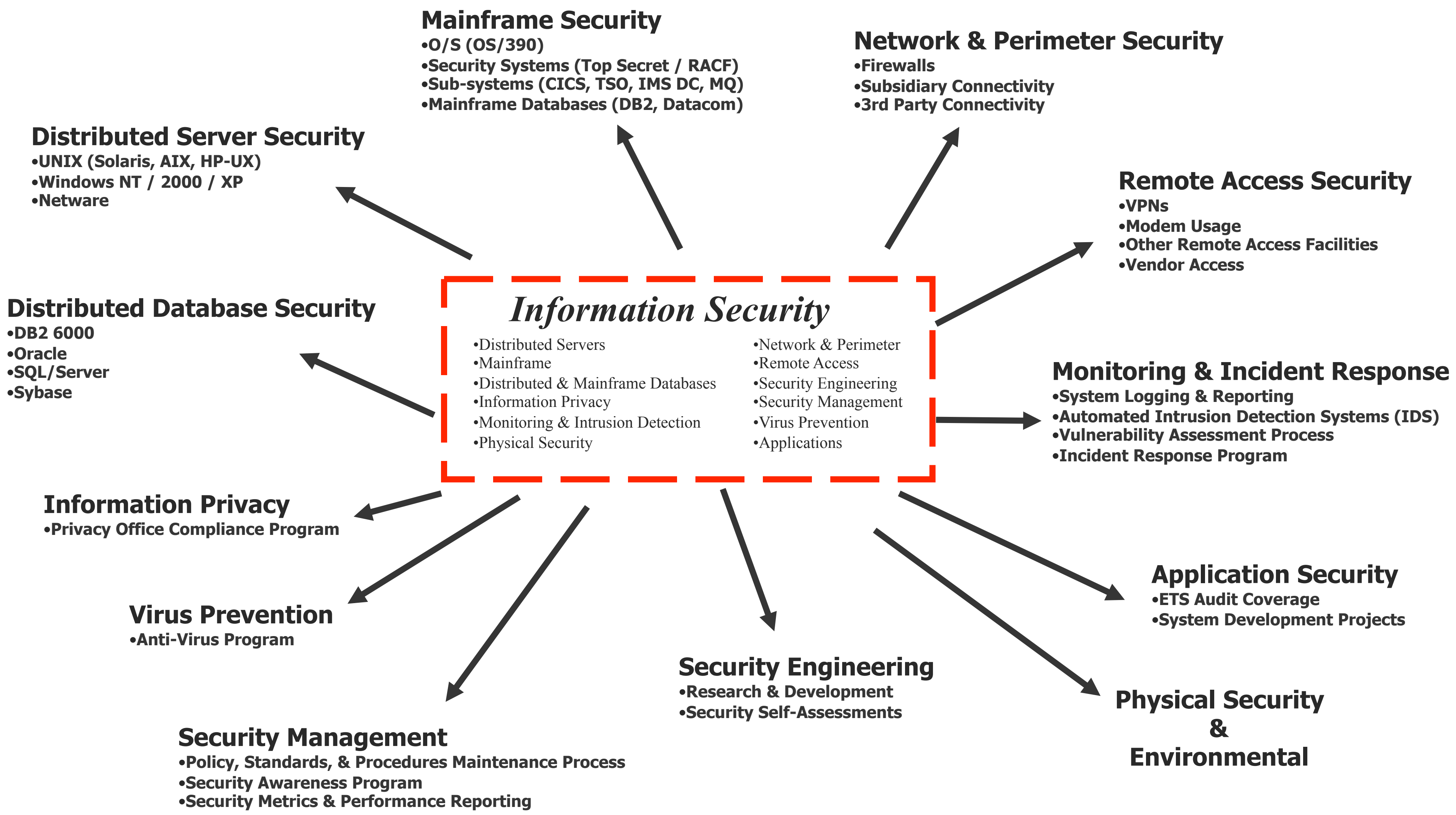
Network Management

Telecommunications

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

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)**

Network & Perimeter Security
- **Firewalls**
- **Subsidiary Connectivity**
- **3rd Party Connectivity**

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

Remote Access Security
- **VPNs**
- **Modem Usage**
- **Other Remote Access Facilities**
- **Vendor Access**

Distributed Database Security
- **DB2 6000**
- **Oracle**
- **SQL/Server**
- **Sybase**

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

Information Privacy
- **Privacy Office Compliance Program**

Virus Prevention
- **Anti-Virus Program**

Application Security
- **ETS Audit Coverage**
- **System Development Projects**

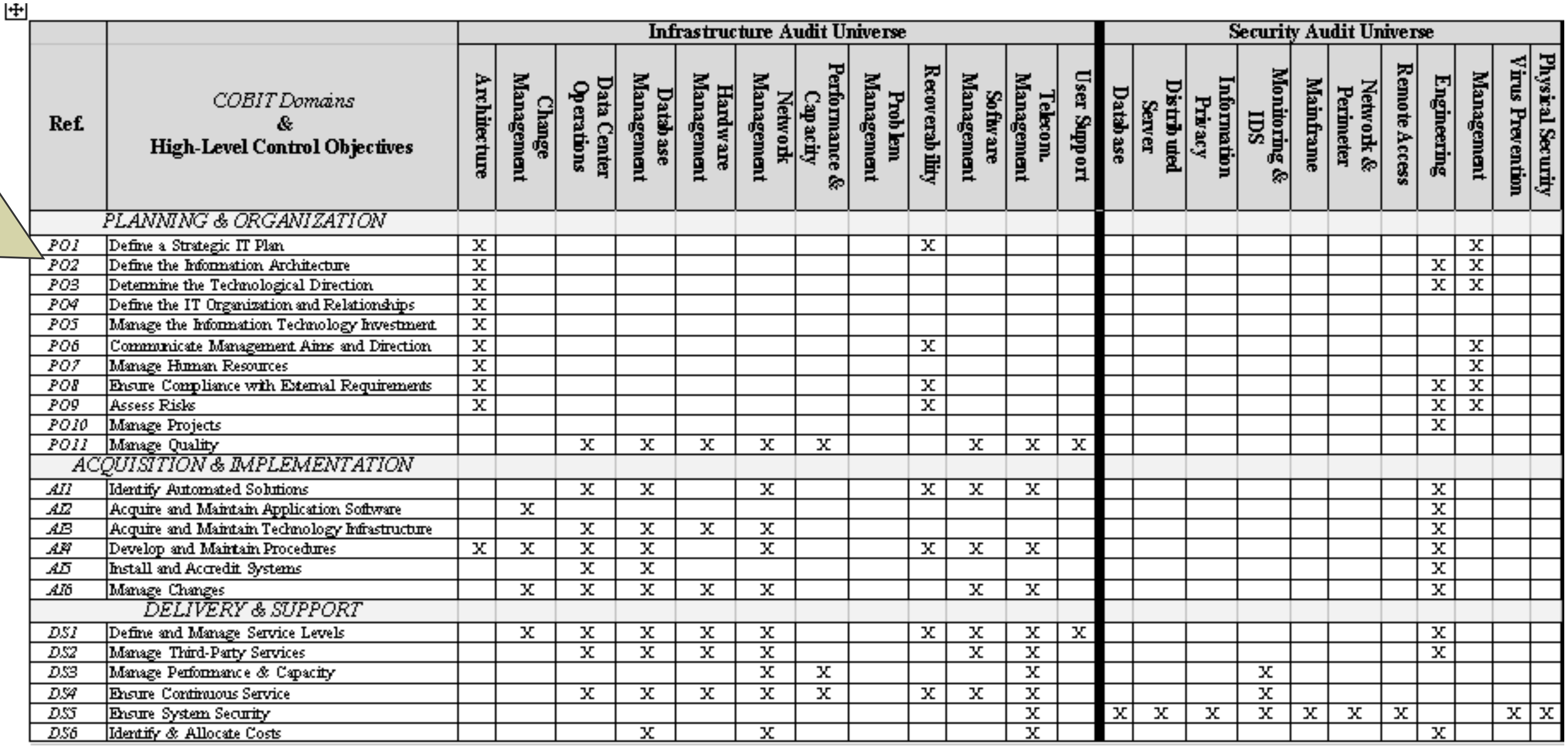
Security Engineering
- **Research & Development**
- **Security Self-Assessments**

Physical Security
&
Environmental

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

Map Audit Universe To CobiT®

Process (e.g. PO2)

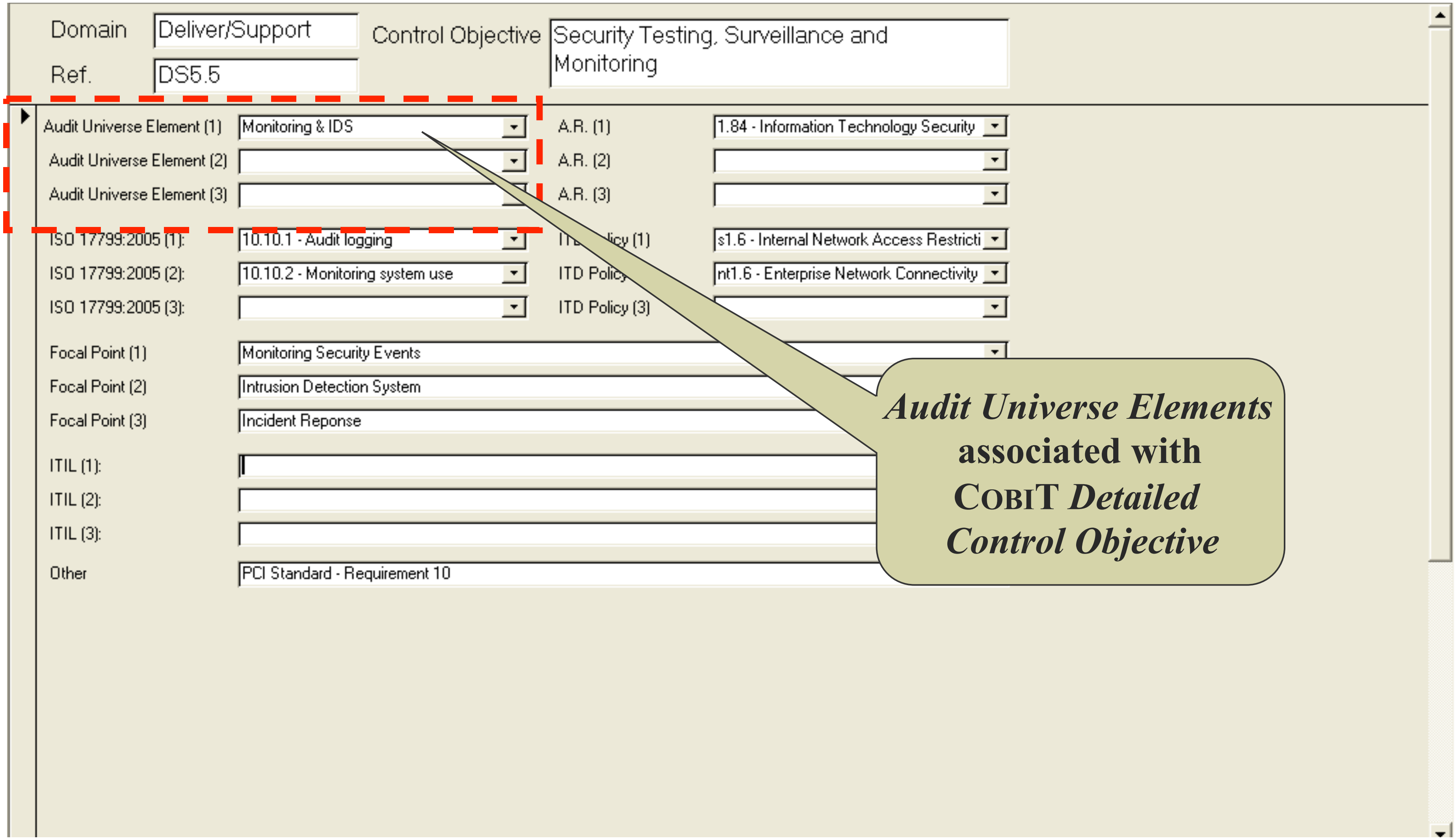


		Infrastructure Audit Universe												Security Audit Universe										
Ref.	*COBIT Domains* & High-Level Control Objectives	Architecture	Change Management	Data Center Operations	Database Management	Hardware Management	Network Management	Performance & Capacity	Problem Management	Recoverability	Software 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			

Illustration Only

Applicable Processes Noted With 'X'

Map Audit Universe To COBIT®
Mapping Database



Domain	Deliver/Support	Control Objective	Security Testing, Surveillance and Monitoring
Ref.	DS5.5		
Audit Universe Element (1)	Monitoring & IDS	A.R. (1)	1.84 - Information Technology Security
Audit Universe Element (2)		A.R. (2)	
Audit Universe Element (3)		A.R. (3)	
ISO 17799:2005 (1):	10.10.1 - Audit logging	ITD Policy (1)	s1.6 - Internal Network Access Restricti
ISO 17799:2005 (2):	10.10.2 - Monitoring system use	ITD Policy (2)	nt1.6 - Enterprise Network Connectivity
ISO 17799:2005 (3):		ITD Policy (3)	
Focal Point (1)	Monitoring Security Events		
Focal Point (2)	Intrusion Detection System		
Focal Point (3)	Incident Reponse		
ITIL (1):			
ITIL (2):			
ITIL (3):			
Other	PCI Standard - Requirement 10		

Audit Universe Elements* associated with COBIT *Detailed Control Objective

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.

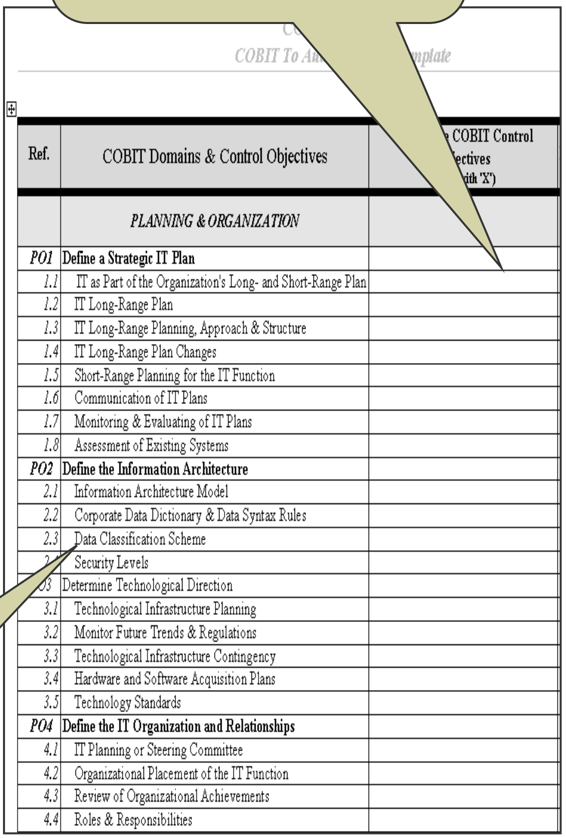
Remote Access
Appropriate mechanisms are in place to control and monitor remote user access to Schwab's internal network.

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.).

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

Record Applicable Focal Points & Areas of Emphasis

Detailed Control Objectives

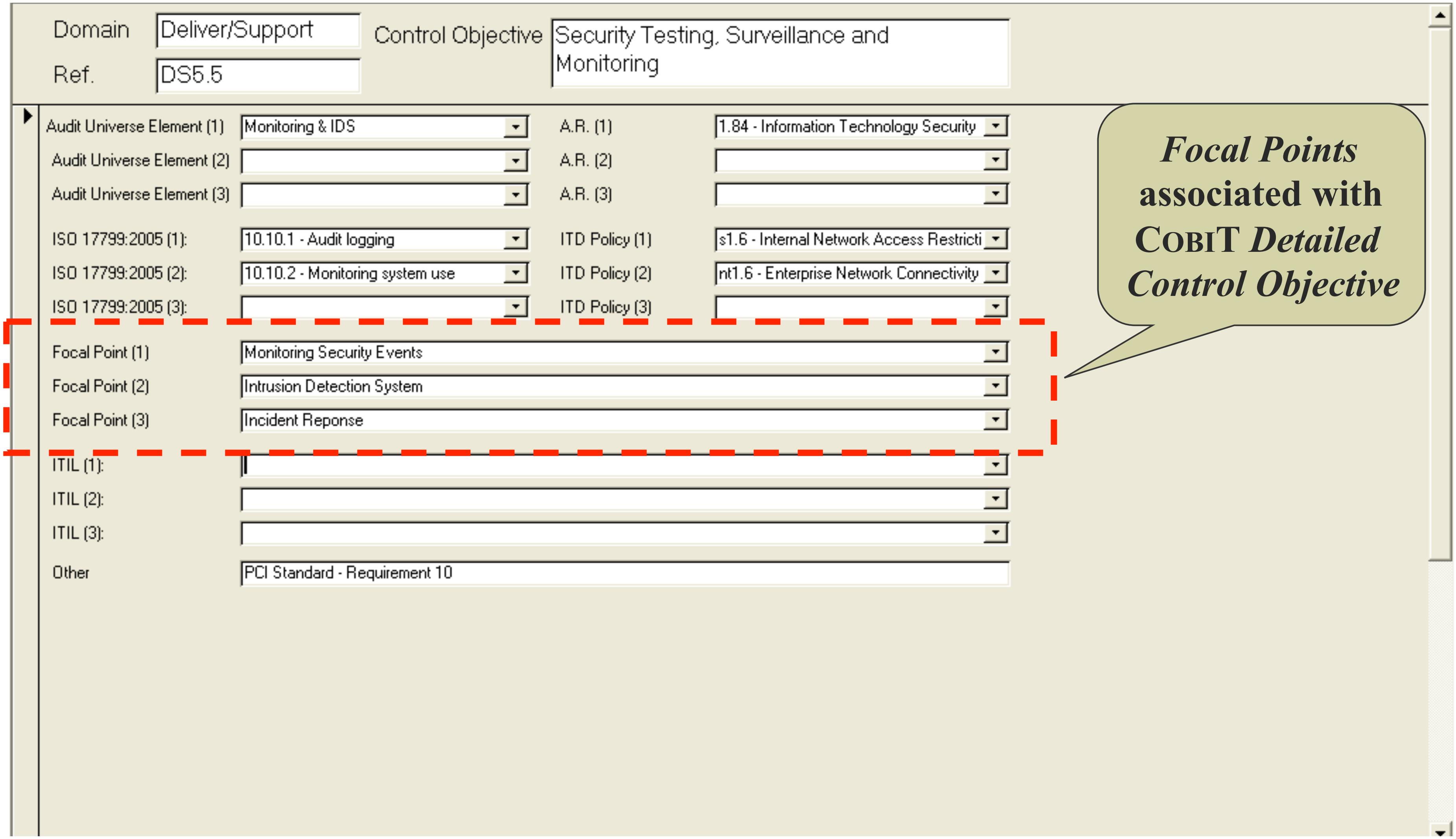


C

COBIT To Au mplate

Ref.	COBIT Domains & Control Objectives	e COBIT Control ectives ith '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	
O3	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	

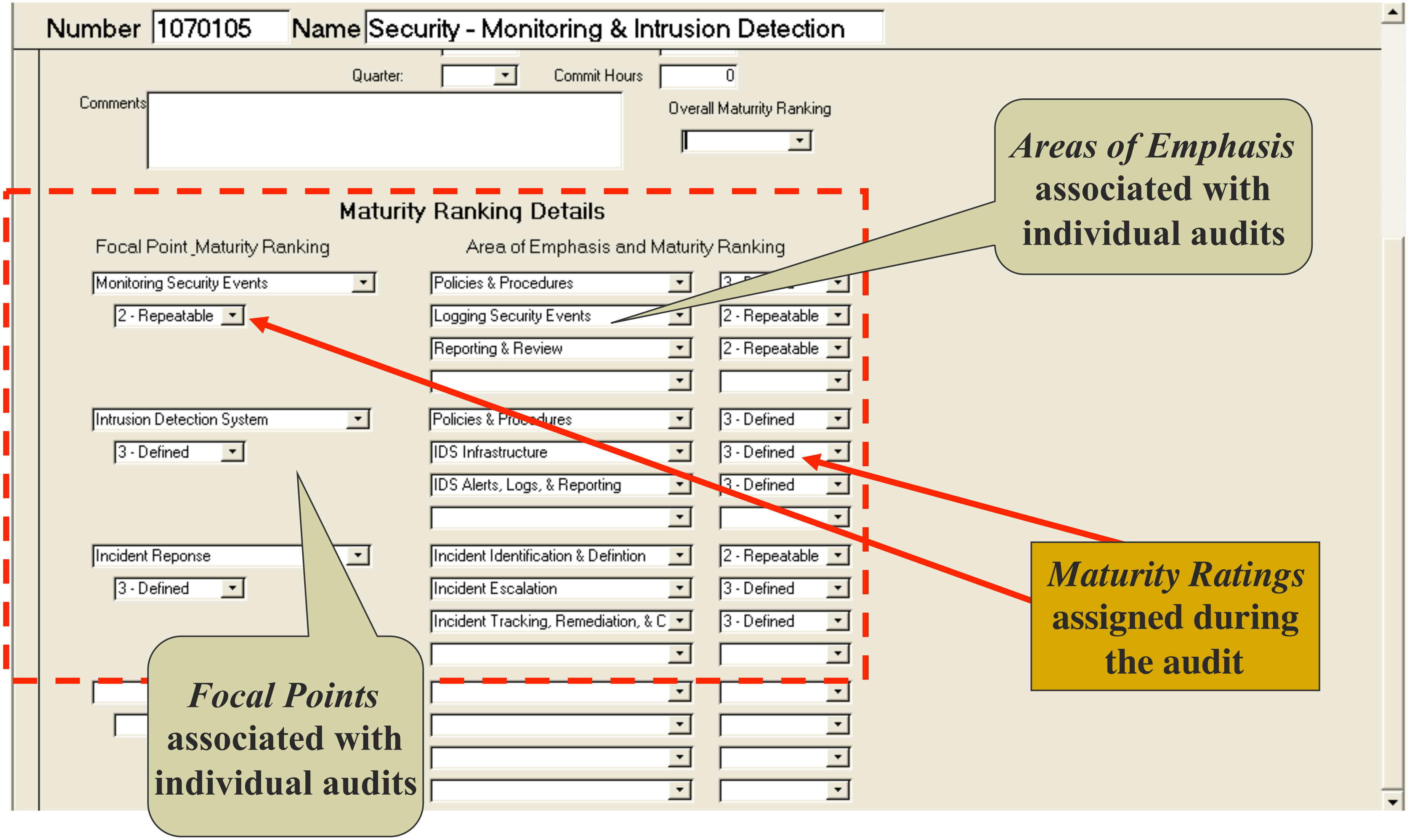
Map Audit Focal Points To COBIT®
Mapping Database



Domain	Deliver/Support	Control Objective	Security Testing, Surveillance and Monitoring
Ref.	DS5.5		
Audit Universe Element (1)	Monitoring & IDS	A.R. (1)	1.84 - Information Technology Security
Audit Universe Element (2)		A.R. (2)	
Audit Universe Element (3)		A.R. (3)	
ISO 17799:2005 (1):	10.10.1 - Audit logging	ITD Policy (1)	s1.6 - Internal Network Access Restricti
ISO 17799:2005 (2):	10.10.2 - Monitoring system use	ITD Policy (2)	nt1.6 - Enterprise Network Connectivity
ISO 17799:2005 (3):		ITD Policy (3)	
Focal Point (1)	Monitoring Security Events		
Focal Point (2)	Intrusion Detection System		
Focal Point (3)	Incident Reponse		
ITIL (1):			
ITIL (2):			
ITIL (3):			
Other	PCI Standard - Requirement 10		

Focal Points* associated with COBIT *Detailed Control Objective

Map Focal Points / Areas of Emphasis To Individual Audit
Project Tracking / Measurement Database



Number 1070105 Name Security - Monitoring & Intrusion Detection

Quarter: Commit Hours 0

Comments

Overall Maturity Ranking

Maturity Ranking Details

Focal Point Maturity Ranking	Area of Emphasis and Maturity Ranking	
Monitoring Security Events	Policies & Procedures	3 - D
2 - Repeatable	Logging Security Events	2 - Repeatable
	Reporting & Review	2 - Repeatable
Intrusion Detection System	Policies & Procedures	3 - Defined
3 - Defined	IDS Infrastructure	3 - Defined
	IDS Alerts, Logs, & Reporting	3 - Defined
Incident Reponse	Incident Identification & Defintion	2 - Repeatable
3 - Defined	Incident Escalation	3 - Defined
	Incident Tracking, Remediation, & C	3 - Defined

***Areas of Emphasis* associated with individual audits**

***Maturity Ratings* assigned during the audit**

***Focal Points* associated with individual audits**

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

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

ITIL®

IT Service Management

COBIT®

GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

ISO

NIST

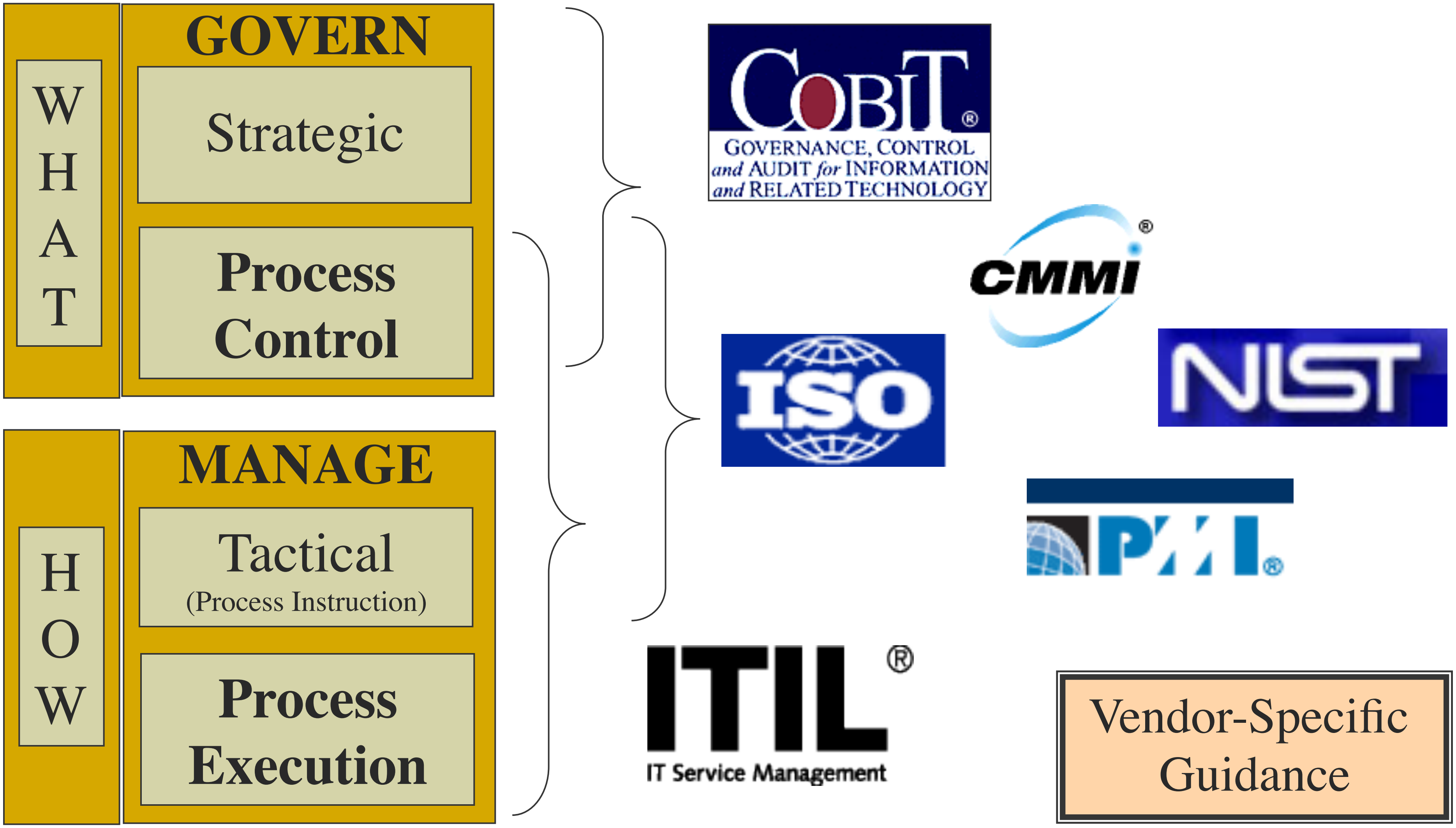
Vendor-Specific Guidance

PMI®

CMMI®

Classification of Industry Standards

“What” versus “How”



WHAT

GOVERN

Strategic

Process Control

HOW

MANAGE

Tactical (Process Instruction)

Process Execution

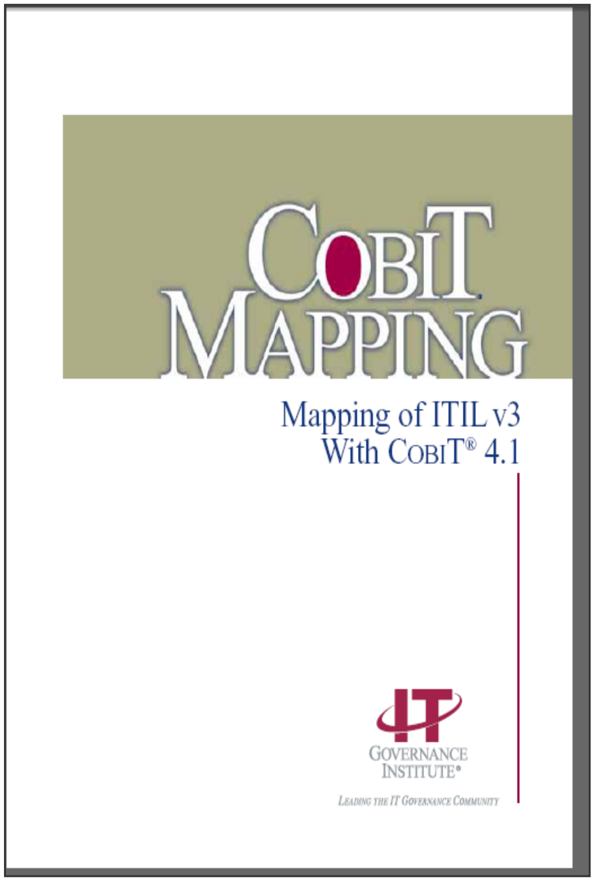
Vendor-Specific Guidance

COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY
CMMI®
ISO
NIST
PMI®
ITIL®
IT Service Management

Available COBIT® Mappings

Currently available at *ISACA.ORG* or *ITGI.ORG*

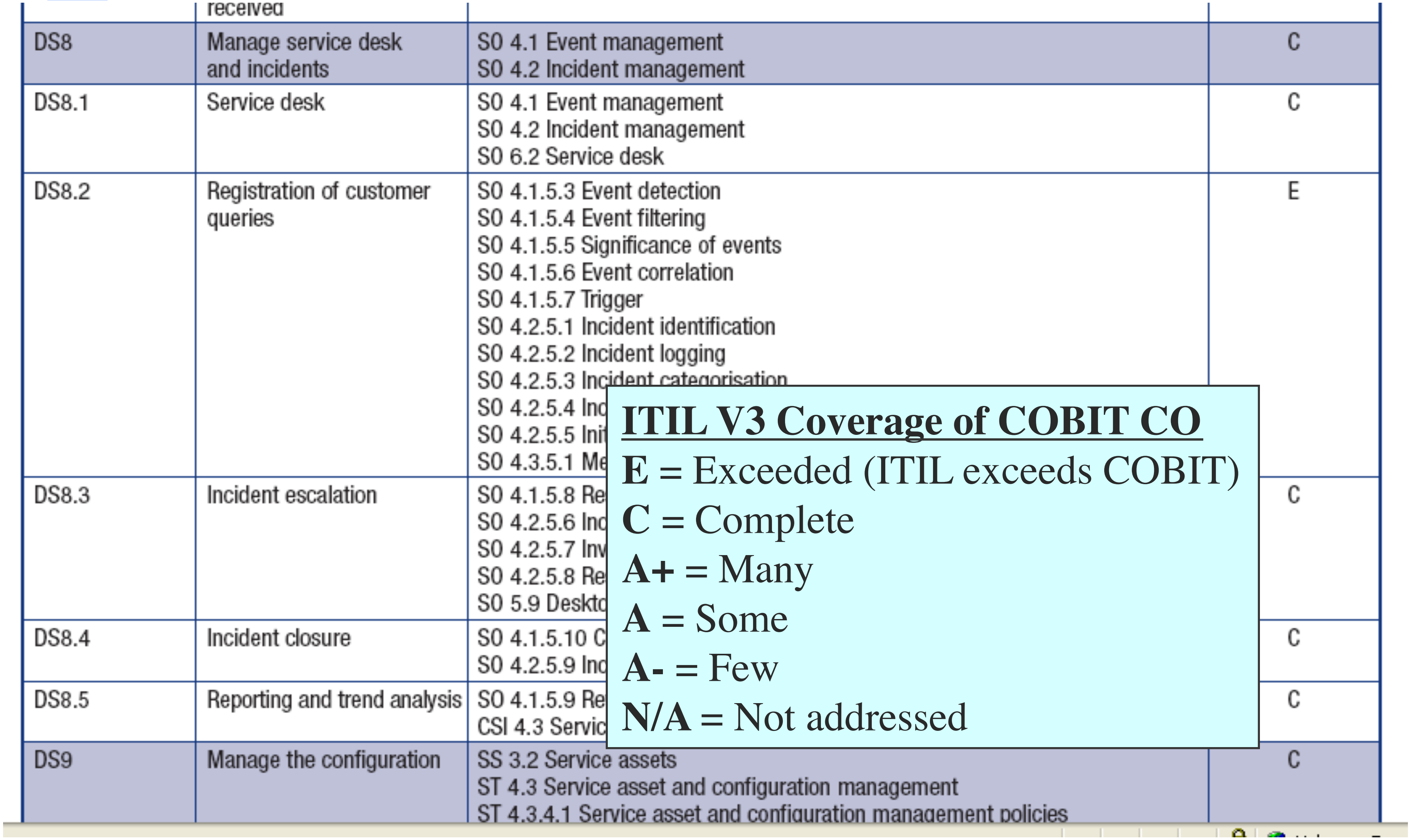
- Go to *COBIT* link



- **ITIL V3** (IT Infrastructure Library)
- **ISO ISO27002(17799:2005)** (Security Code of Practice)
- **NIST SP800-53 Rev 1** (Security – Federal IS)
- **CMMI for Development V1.2** (Capability Maturity Model Integration)
- **SEI's CMM for Software** (Capability Maturity Model For Software – retired)
- **TOGAF 8.1** (Open Group Architecture Framework)
- **PMBOK** (Project Management BOK – ANSI Standard)
- **PRINCE2** (Projects in Controlled Environments)
- Others under development

Mapping

Detailed: By Control Objective



	received		
DS8	Manage service desk and incidents	SO 4.1 Event management SO 4.2 Incident management	C
DS8.1	Service desk	SO 4.1 Event management SO 4.2 Incident management SO 6.2 Service desk	C
DS8.2	Registration of customer queries	SO 4.1.5.3 Event detection SO 4.1.5.4 Event filtering SO 4.1.5.5 Significance of events SO 4.1.5.6 Event correlation SO 4.1.5.7 Trigger SO 4.2.5.1 Incident identification SO 4.2.5.2 Incident logging SO 4.2.5.3 Incident categorisation SO 4.2.5.4 Inc SO 4.2.5.5 Ini SO 4.3.5.1 Me	E
DS8.3	Incident escalation	SO 4.1.5.8 Re SO 4.2.5.6 Inc SO 4.2.5.7 Inv SO 4.2.5.8 Re SO 5.9 Deskto	C
DS8.4	Incident closure	SO 4.1.5.10 C SO 4.2.5.9 Inc	C
DS8.5	Reporting and trend analysis	SO 4.1.5.9 Re CSI 4.3 Servic	C
DS9	Manage the configuration	SS 3.2 Service assets ST 4.3 Service asset and configuration management ST 4.3.4.1 Service asset and configuration management policies	C

ITIL V3 Coverage of COBIT CO

E = Exceeded (ITIL exceeds COBIT)

C = Complete

A+ = Many

A = Some

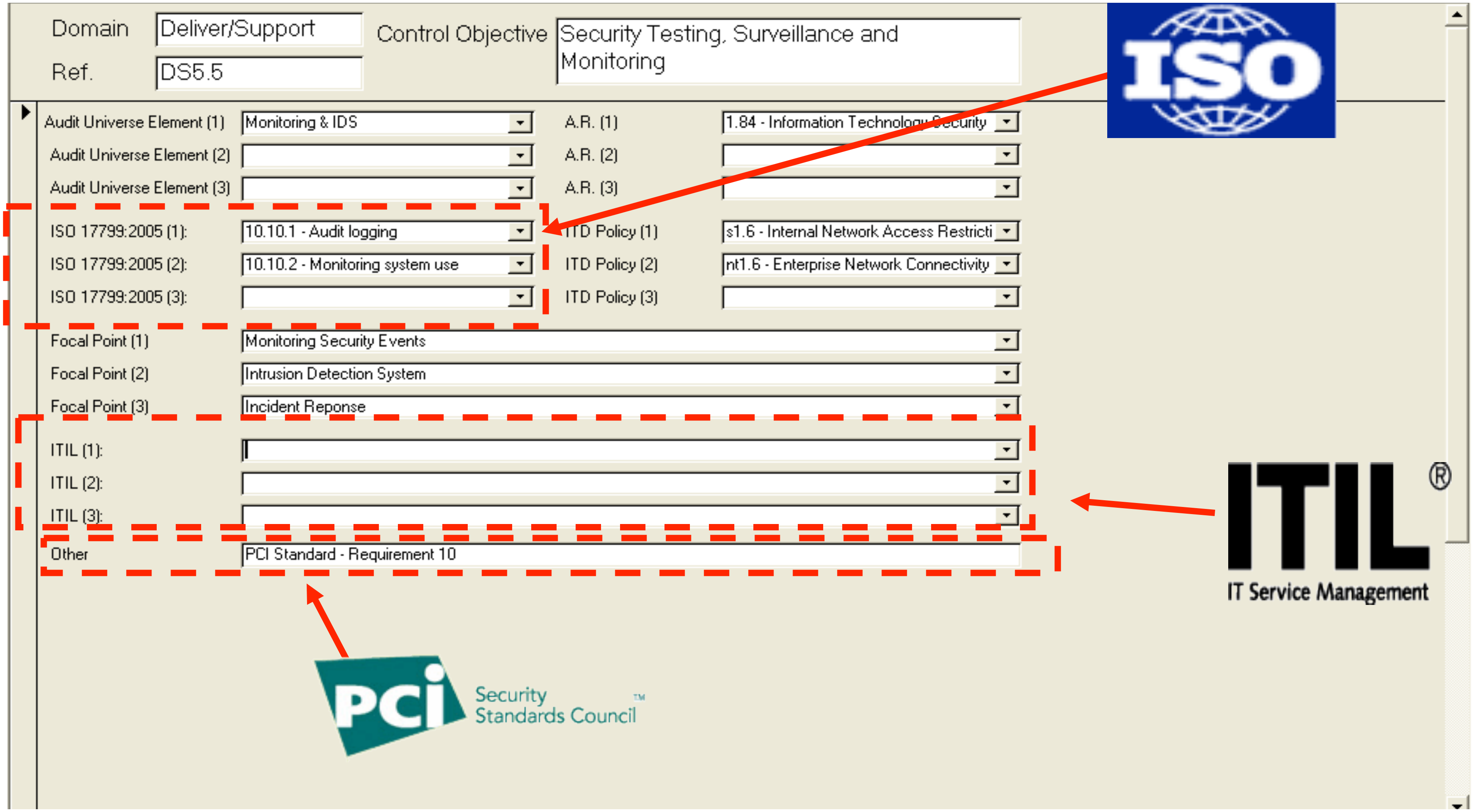
A- = Few

N/A = Not addressed

Source: **IT Governance Institute - COBIT® Mapping: Mapping of ITIL V3 with COBIT® 4.1**

Map Relevant Standards To COBIT®

Mapping Database



Domain	Deliver/Support	Control Objective	Security Testing, Surveillance and Monitoring
Ref.	DS5.5		

Audit Universe Element (1)	Monitoring & IDS	A.R. (1)	1.84 - Information Technology Security
Audit Universe Element (2)		A.R. (2)	
Audit Universe Element (3)		A.R. (3)	
ISO 17799:2005 (1):	10.10.1 - Audit logging	ITD Policy (1)	s1.6 - Internal Network Access Restricti
ISO 17799:2005 (2):	10.10.2 - Monitoring system use	ITD Policy (2)	nt1.6 - Enterprise Network Connectivity
ISO 17799:2005 (3):		ITD Policy (3)	
Focal Point (1)	Monitoring Security Events		
Focal Point (2)	Intrusion Detection System		
Focal Point (3)	Incident Reponse		
ITIL (1):			
ITIL (2):			
ITIL (3):			
Other	PCI Standard - Requirement 10		

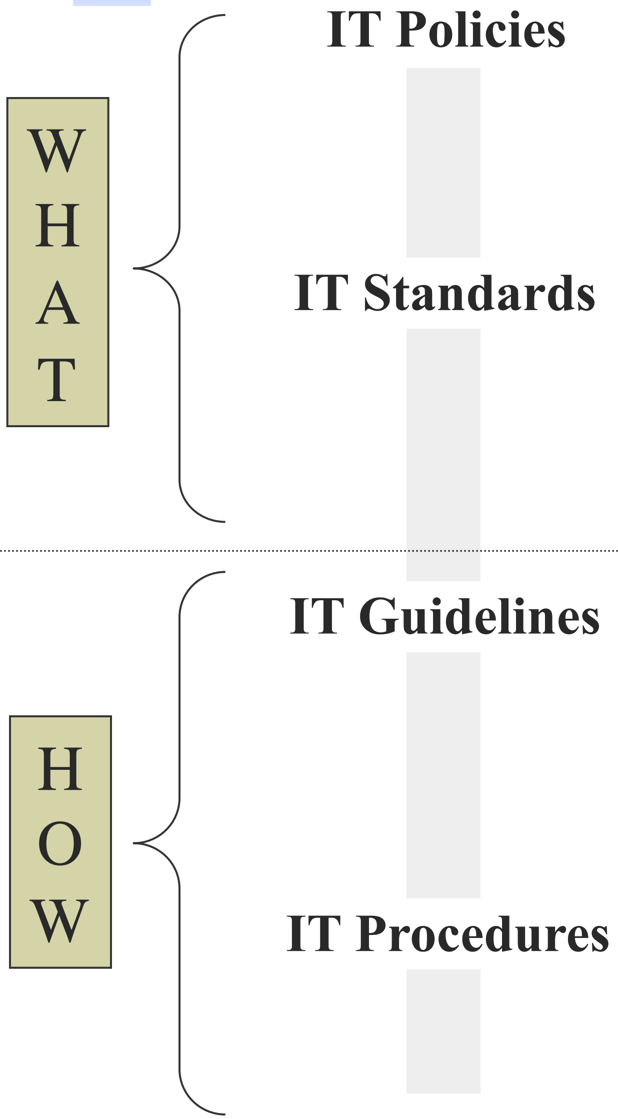
ISACA®

Trust in, and value from, information systems

San Francisco Chapter

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

Policies, Standards, Guidelines & Procedures



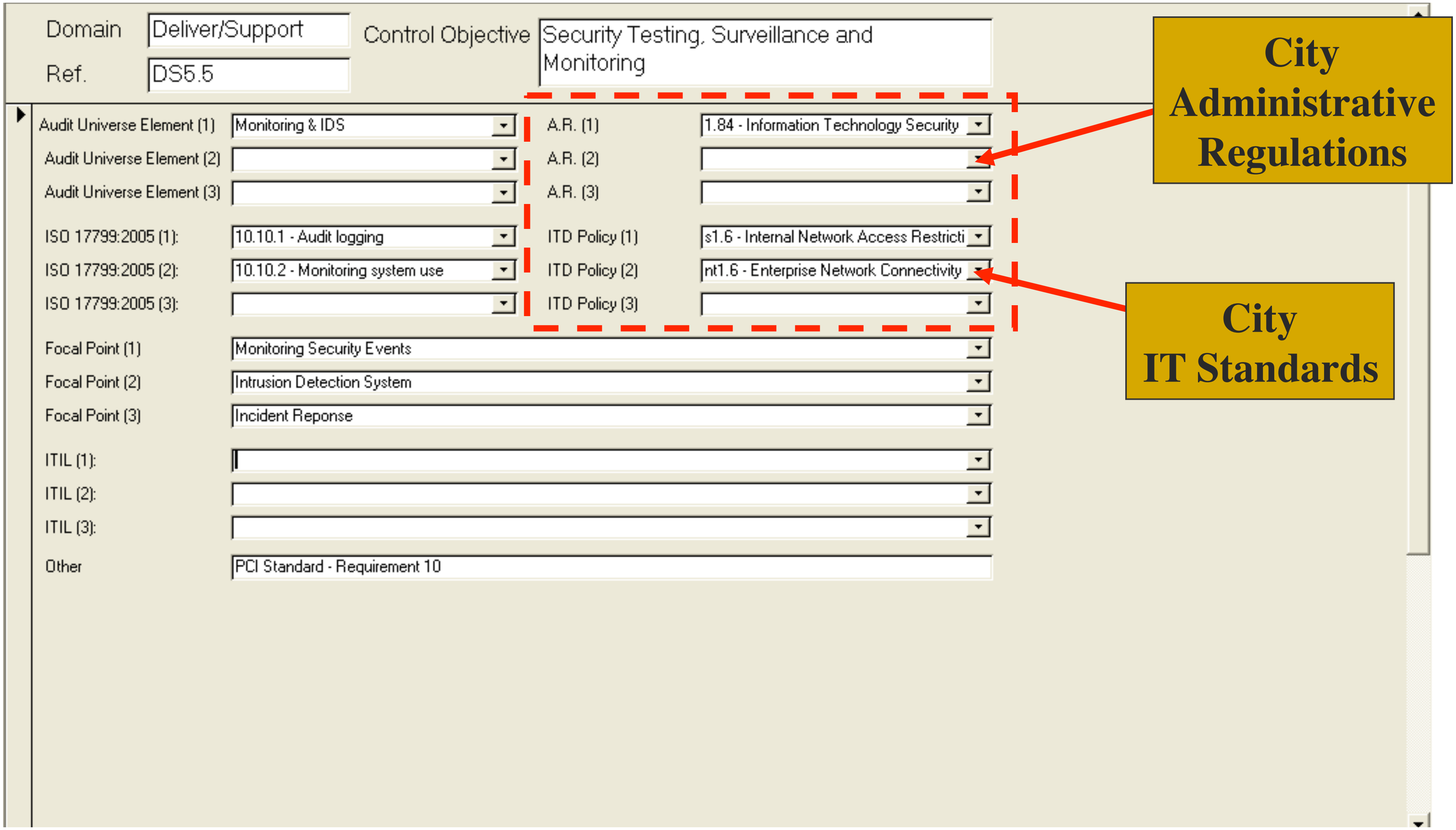
Policies:
High-level statements. When there is no specific standard to follow, policies provide general guidance.

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.

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

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

Map IT Policies / Standards To COBIT®
Mapping Database



Domain	Deliver/Support	Control Objective	Security Testing, Surveillance and Monitoring
Ref.	DS5.5		

Audit Universe Element (1)	Monitoring & IDS	A.R. (1)	1.84 - Information Technology Security
Audit Universe Element (2)		A.R. (2)	
Audit Universe Element (3)		A.R. (3)	
ISO 17799:2005 (1):	10.10.1 - Audit logging	ITD Policy (1)	s1.6 - Internal Network Access Restricti
ISO 17799:2005 (2):	10.10.2 - Monitoring system use	ITD Policy (2)	nt1.6 - Enterprise Network Connectivity
ISO 17799:2005 (3):		ITD Policy (3)	

Focal Point (1)	Monitoring Security Events
Focal Point (2)	Intrusion Detection System
Focal Point (3)	Incident Reponse
ITIL (1):	
ITIL (2):	
ITIL (3):	
Other	PCI Standard - Requirement 10

City Administrative Regulations

City IT Standards

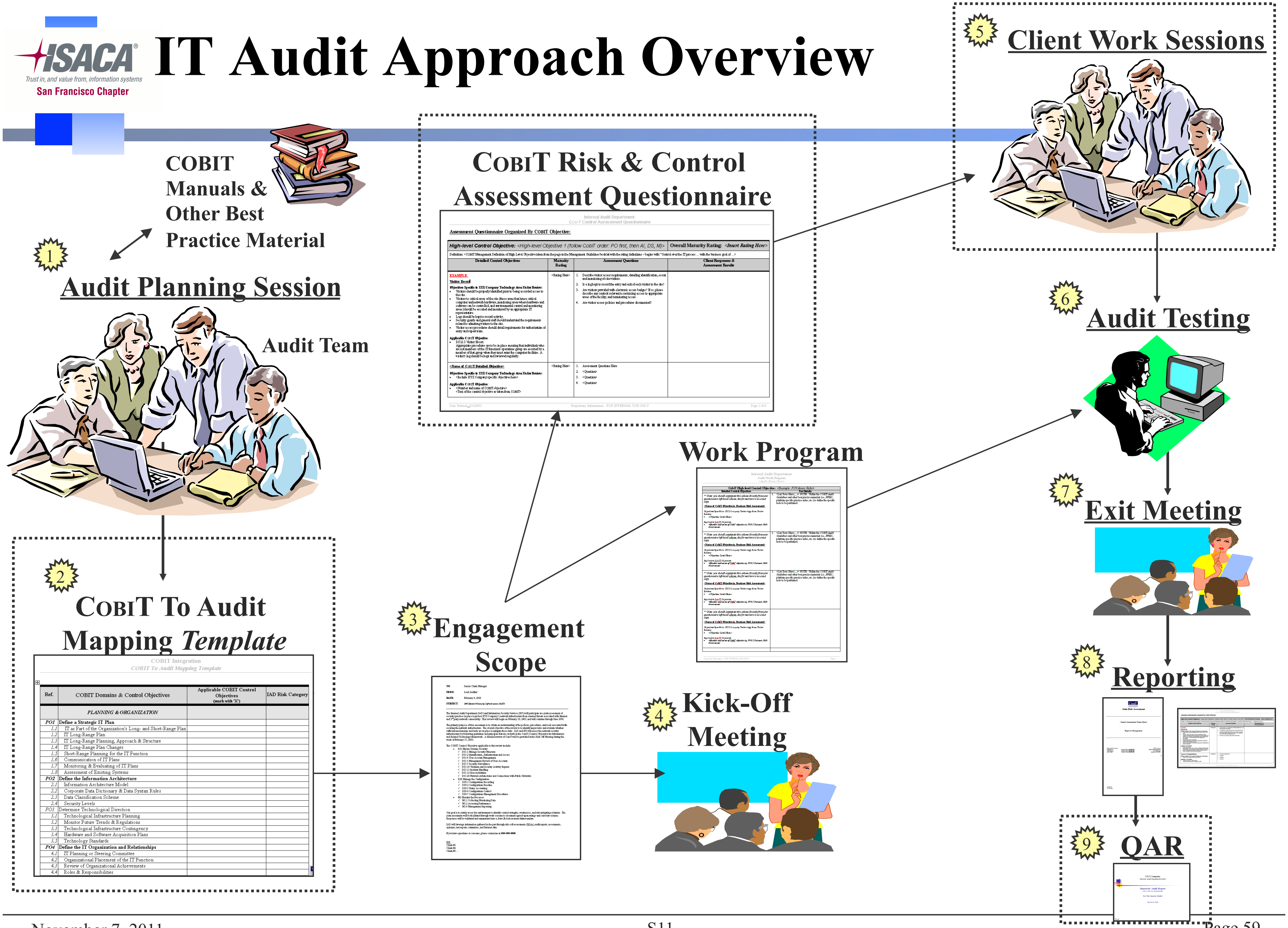
ISACA®
Trust in, and value from, information systems
San Francisco Chapter

AGENDA

- Overview of COBIT®
- Integrating COBIT® Domains into IT Audit Planning & Scope Development
- **Integrating COBIT® into the IT Audit Lifecycle**
- COBIT 5
- Summary & Wrap-up

ISACA
Trust in, and value from, information systems
San Francisco Chapter

IT Audit Approach Overview



COBIT Integration
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		

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 Review:** ▪ <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 2. <Question> 3. <Question> 4. <Question>	

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

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 Information and Related Technology) framework. A detailed review of COBIT will be provided in the Kick-Off Meeting during the 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
  - ✓ DS9.4 Configuration Control
  - ✓ DS9.7 Configuration Management Procedures
- M1 Monitor the Processes
  - ✓ M1.1 Collecting Monitoring Data
  - ✓ M1.2 Assessing Performance
  - ✓ M1.4 Management Reporting

Our goal is to jointly assess the environment to identify control strengths, weaknesses, and risk mitigating solutions. The joint assessment will be facilitated through work sessions to document agreed upon ratings and corrective actions. Responses will be validated and summarized into a *Joint Risk Assessment Memorandum*.

IAD will leverage information gathered in the past through risk self-assessments (RSAs), audit reports, assessments, opinions, test reports, summaries, and Intranet data.

If you have questions or concerns, please contact me at ###-###-####.

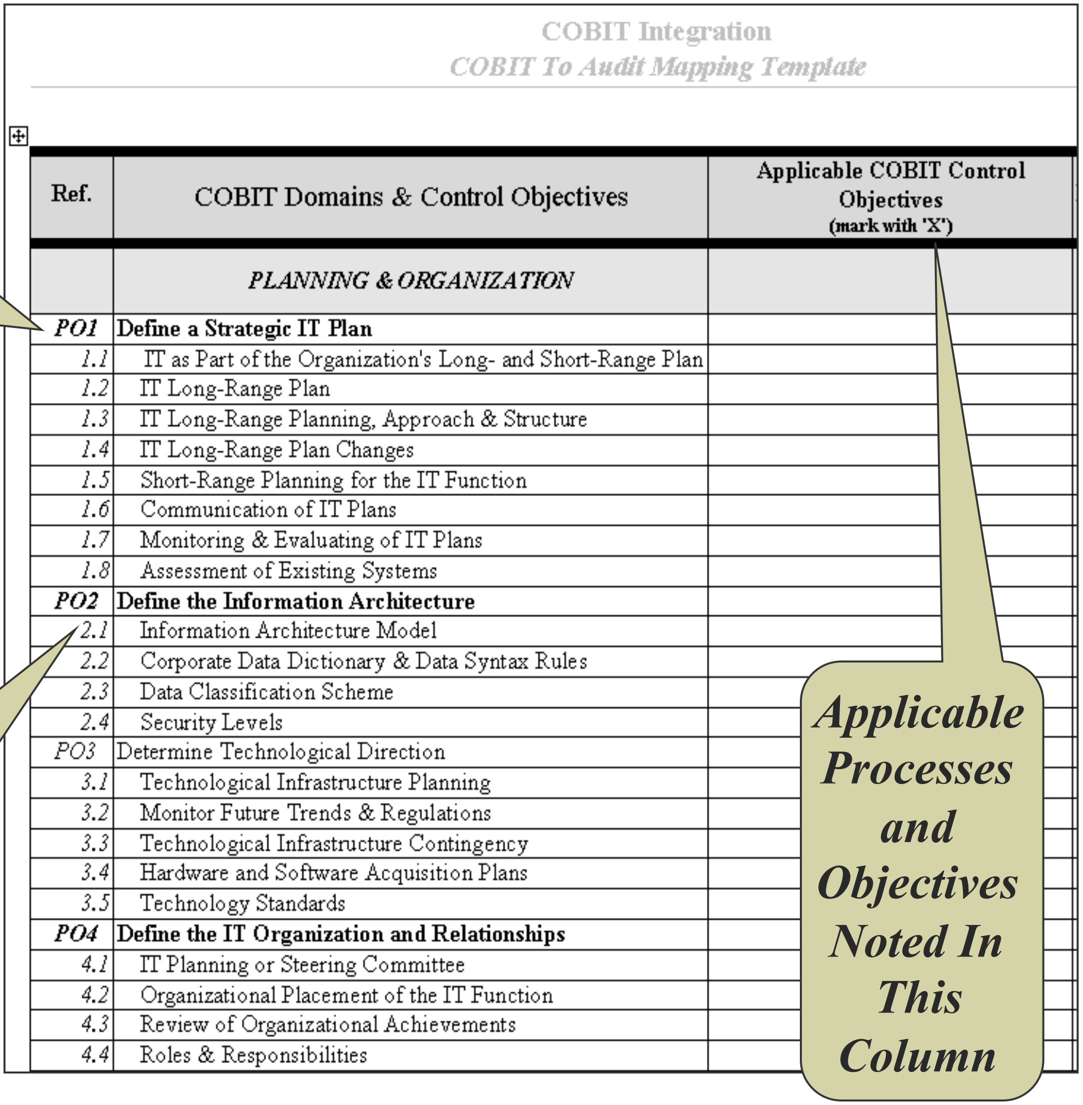
CC:
Client #1
Client #2
Client #3….

Internal Audit Department
Audit Work Program
<Audit Name Here>

CobiT High-level Control Objective: *<Example: PO9 Assess Risks>*	
Detailed Control Objectives	**Test Details**
*** Note: you should copy/paste this column directly from your questionnaire left-hand column, the format here is an exact copy.* **<Name of CobiT Objective ie. Business Risk Assessment>** Objectives Specific to XYZ Company Technology Area Under Review: ▪ <Objectives Listed Here> Applicable CobiT Objective: ▪ *<Number and name of CobiT objective ie. PO9.1 Business Risk Assessment>*	1. <List Tests Here> ← NOTE: Utilize the COBIT *Audit Guidelines* and other best practice materials (i.e., FFIEC, platform specific practice aides, etc.) to define the specific tests to be performed.
*** Note: you should copy/paste this column directly from your questionnaire left-hand column, the format here is an exact copy.* **<Name of CobiT Objective ie. Business Risk Assessment>** Objectives Specific to XYZ Company Technology Area Under Review: ▪ <Objectives Listed Here> Applicable CobiT Objective: ▪ *<Number and name of CobiT objective ie. PO9.1 Business Risk Assessment>*	1. <List Tests Here> ← NOTE: Utilize the COBIT *Audit Guidelines* and other best practice materials (i.e., FFIEC, platform specific practice aides, etc.) to define the specific tests to be performed.
*** Note: you should copy/paste this column directly from your questionnaire left-hand column, the format here is an exact copy.* **<Name of CobiT Objective ie. Business Risk Assessment>** Objectives Specific to XYZ Company Technology Area Under Review: ▪ <Objectives Listed Here> Applicable CobiT Objective: ▪ *<Number and name of CobiT objective ie. PO9.1 Business Risk Assessment>*	1. <List Tests Here> ← NOTE: Utilize the COBIT *Audit Guidelines* and other best practice materials (i.e., FFIEC, platform specific practice aides, etc.) to define the specific tests to be performed.
*** Note: you should copy/paste this column directly from your questionnaire left-hand column, the format here is an exact copy.* **<Name of CobiT Objective ie. Business Risk Assessment>** Objectives Specific to XYZ Company Technology Area Under Review: ▪ <Objectives Listed Here> Applicable CobiT Objective: ▪ *<Number and name of CobiT objective ie. PO9.1 Business Risk Assessment>*	

Proprietary Information - FOR INTERNAL USE ONLY Page 1

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	

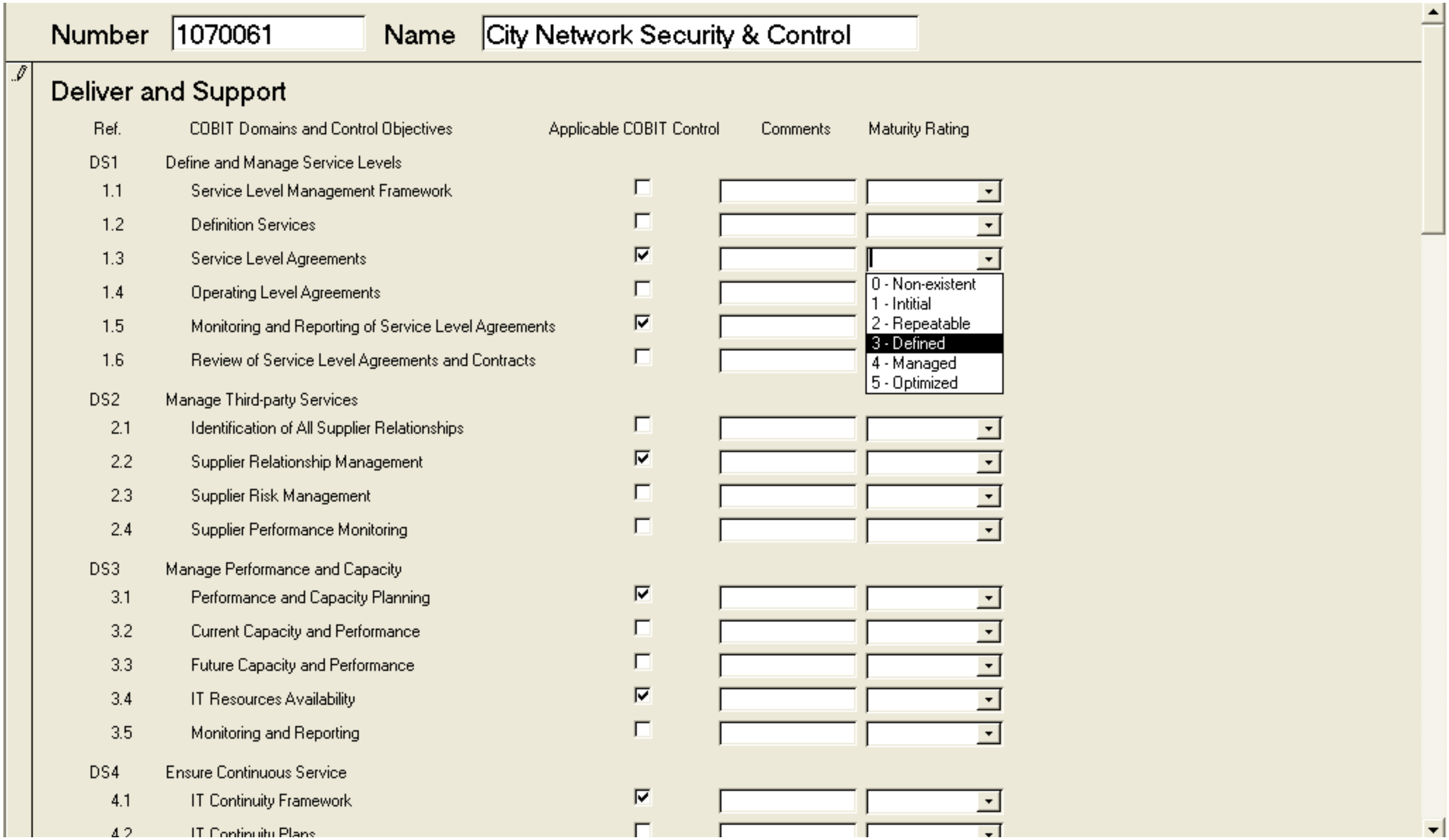
Process (e.g. PO1)

Detailed Control Objective (e.g. 2.1)

Applicable Processes and Objectives Noted In This Column

Map Audit Scope To COBIT®

Mapping Database



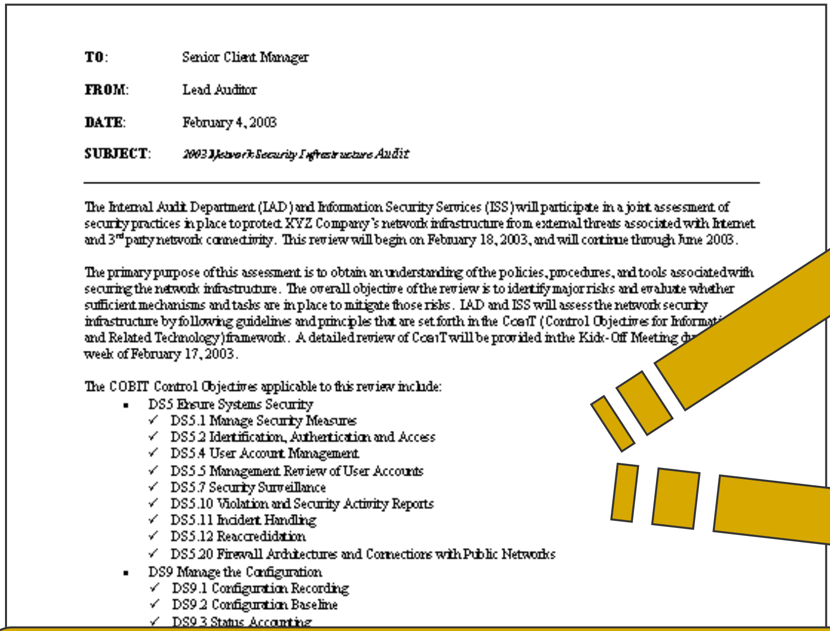
Number 1070061 Name City Network Security & Control

Deliver and Support

Ref.	COBIT Domains and Control Objectives	Applicable COBIT Control	Comments	Maturity Rating
DS1	Define and Manage Service Levels			
1.1	Service Level Management Framework	□		
1.2	Definition Services	□		
1.3	Service Level Agreements	☑		0 - Non-existent 1 - Intitial 2 - Repeatable 3 - Defined 4 - Managed 5 - Optimized
1.4	Operating Level Agreements	□		
1.5	Monitoring and Reporting of Service Level Agreements	☑		
1.6	Review of Service Level Agreements and Contracts	□		
DS2	Manage Third-party Services			
2.1	Identification of All Supplier Relationships	□		
2.2	Supplier Relationship Management	☑		
2.3	Supplier Risk Management	□		
2.4	Supplier Performance Monitoring	□		
DS3	Manage Performance and Capacity			
3.1	Performance and Capacity Planning	☑		
3.2	Current Capacity and Performance	□		
3.3	Future Capacity and Performance	□		
3.4	IT Resources Availability	☑		
3.5	Monitoring and Reporting	□		
DS4	Ensure Continuous Service			
4.1	IT Continuity Framework	☑		
4.2	IT Continuity Plans	□		

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*

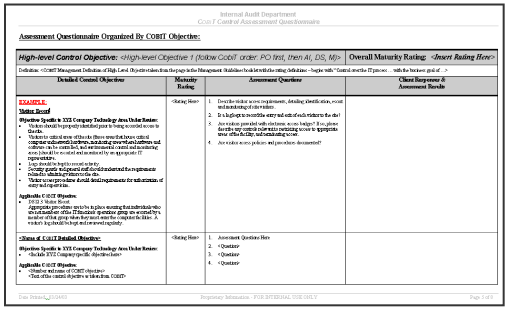
The Internal Audit Department (IAD) and Information Security Services (ISS) will participate in a joint assessment of security practices in place to protect XYZ Company's network infrastructure from external threats associated with Internet and 3rd party network connectivity. This review will begin on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



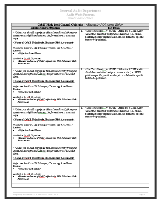
Internal Audit Department
COBIT Control Assessment Questionnaire

Assessment Questionnaire Organized By COBIT Objective:

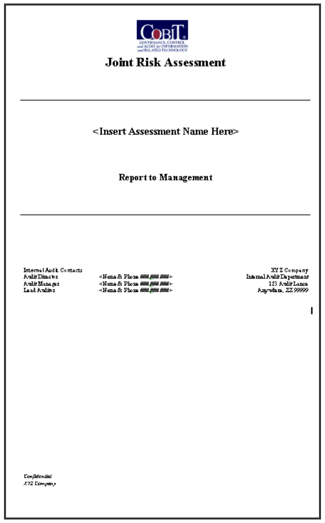
High-level Control Objective: *<High-level Objective 1 (follow CobiT order: PO first, then AI, DS, M)>*			**Overall Maturity Rating:** ***<Insert Rating Here>***
Definition: <COBIT Management Definition of High Level Objective taken from the page in the Management Guidelines booklet with the rating definitions – 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 Review:** ▪ <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 2. <Question> 3. <Question> 4. <Question>	

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

Work Program



Audit Report



COBIT
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

Joint Risk Assessment

<Insert Assessment Name Here>

Report to Management

Internal Audit Contacts		XYZ Company
Audit Director	<Name & Phone ###.###.####>	Internal Audit Department
Audit Manager	<Name & Phone ###.###.####>	123 Audit Lane
Lead Auditor	<Name & Phone ###.###.####>	Anywhere, ZZ 99999

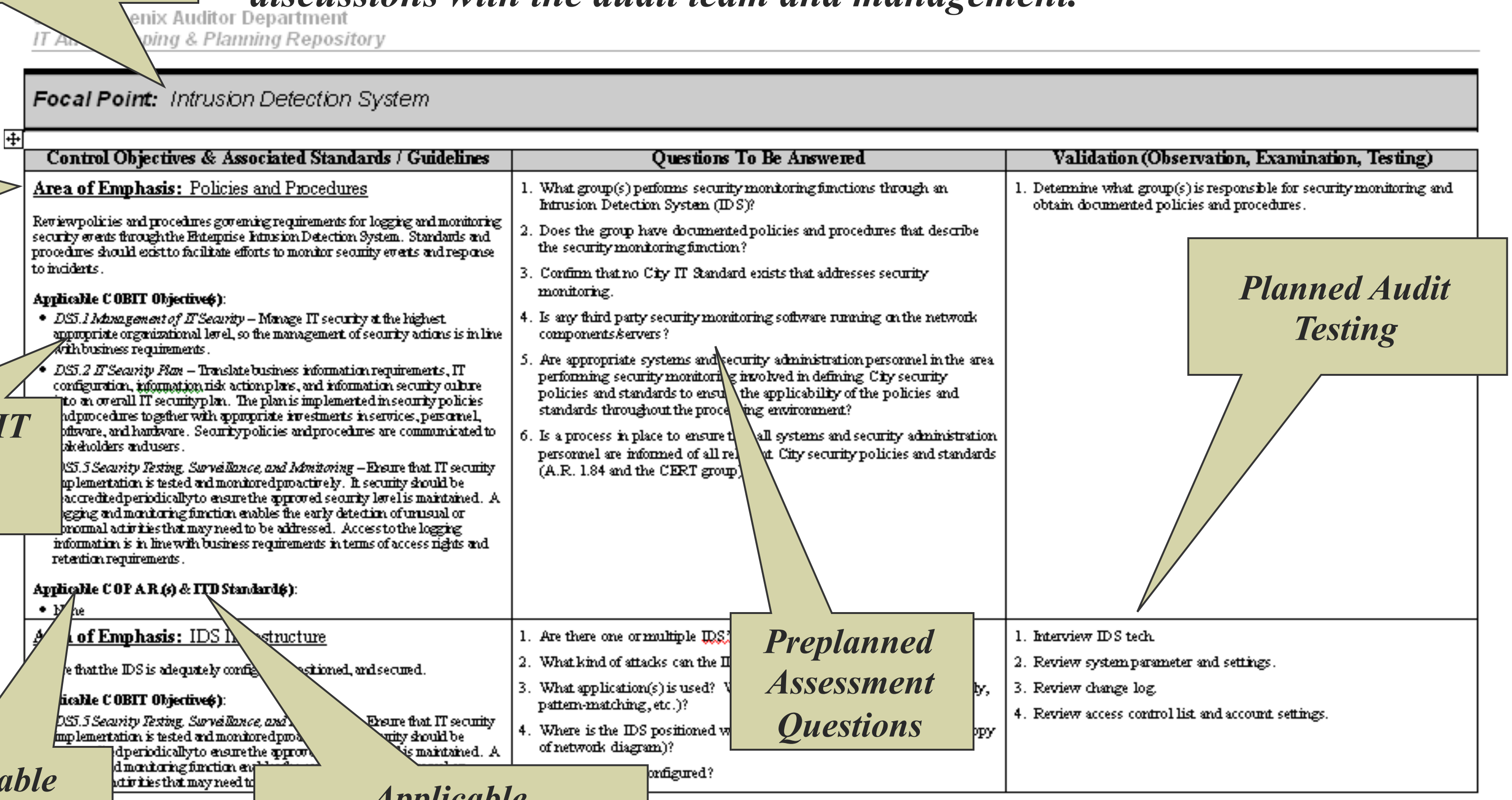
Confidential
XYZ Company

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

Audit Scope & Planning Repository

(i.e., Detailed Audit Scope & Work Program)

Audit Repository is used to document key questions to be answered throughout the audit as well as planned audit validation steps (observation, examination, testing). The Repository is used to facilitate planning discussions with the audit team and management.



enix Auditor Department

IT A ping & Planning Repository

Focal Point: *Intrusion Detection System*

Control Objectives & Associated Standards / Guidelines	Questions To Be Answered	Validation (Observation, Examination, Testing)
Area of Emphasis: Policies and Procedures Review policies and procedures governing requirements for logging and monitoring security events through the Enterprise Intrusion Detection System. Standards and procedures should exist to facilitate efforts to monitor security events and response to incidents. **Applicable COBIT Objective(s):** • *DS5.1 Management of IT Security* – Manage IT security at the highest appropriate organizational 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. *DS5.5 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. **Applicable COP A.R.(s) & ITD Standard(s):** • None	1. What group(s) performs security monitoring functions through an Intrusion Detection System (IDS)? 2. Does the group have documented policies and procedures that describe the security monitoring function? 3. Confirm that no City IT Standard exists that addresses security monitoring. 4. Is any third party security monitoring software running on the network components/servers? 5. Are appropriate systems and security administration personnel in the area performing security monitoring involved in defining City security policies and standards to ensu the applicability of the policies and standards throughout the proce ing environment? 6. Is a process in place to ensure t all systems and security administration personnel are informed of all re t City security policies and standards (A.R. 1.84 and the CERT group)	1. Determine what group(s) is responsible for security monitoring and obtain documented policies and procedures.
A of Emphasis: IDS I structure e that the IDS is adequately config sitioned, and secured. icable COBIT Objective(s): DS5.5 Security Testing, Surveillance, and Ensure that IT security mplementation is tested and monitored pro rity should be dperiodically to ensure the approv is maintained. A d monitoring function en ctivities that may need to	1. Are there one or multiple IDS? 2. What kind of attacks can the I 3. What application(s) is used? V ly, pattern-matching, etc.)? 4. Where is the IDS positioned w py of network diagram)? onfigured?	1. Interview IDS tech. 2. Review system parameter and settings. 3. Review change log. 4. Review access control list and account settings.

One Table For Each Audit Focal Point Included In Audit Scope

One Row For Each Area of Emphasis

Applicable COBIT Control Objectives

Other Applicable Standards / Best Practices / Guidelines

Applicable Organization-Specific IT Policies & Standards

Preplanned Assessment Questions

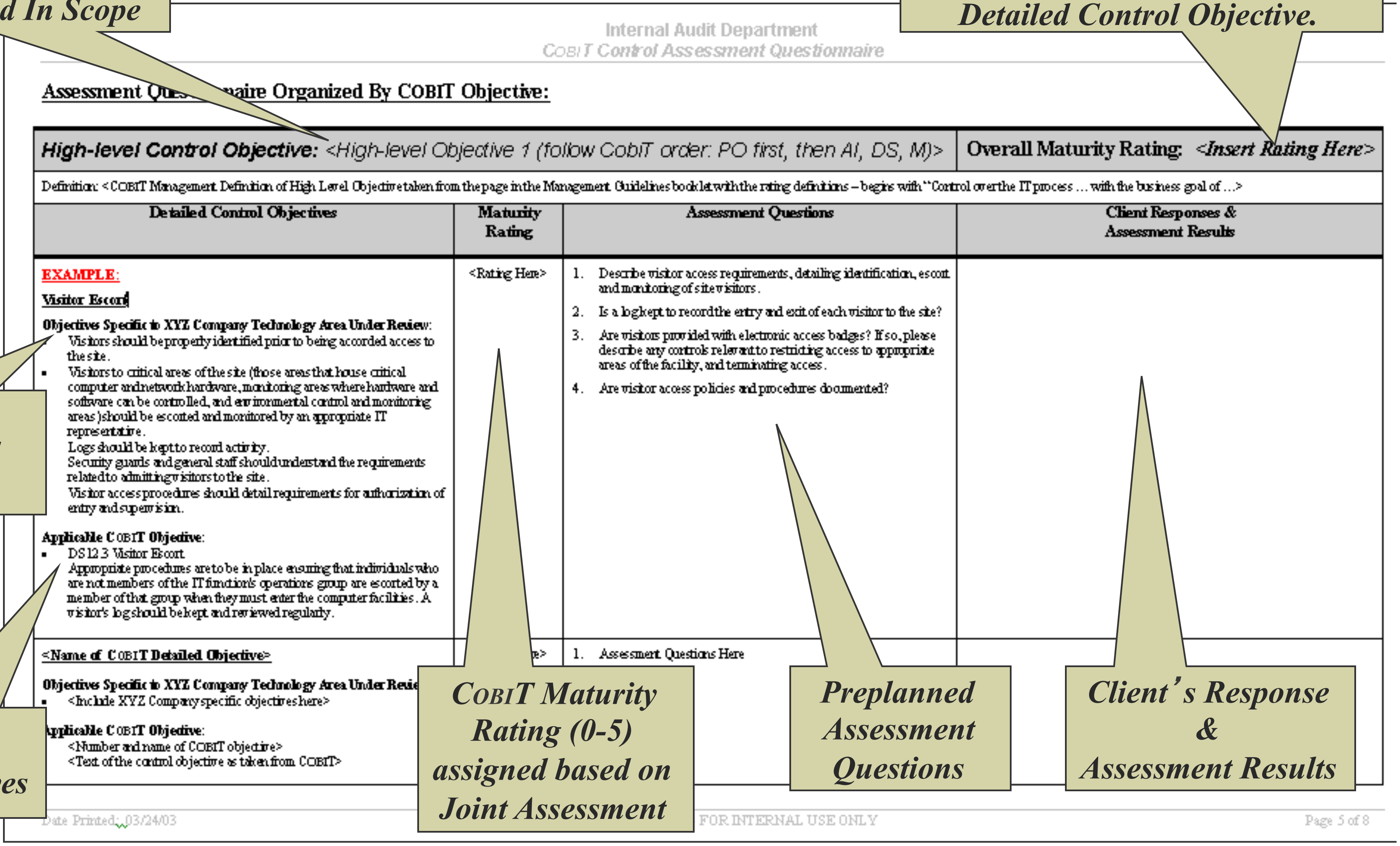
Planned Audit Testing

COBIT® Control Assessment Questionnaire

Questionnaire is used during work sessions held with clients to complete a maturity 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:** ▪ DS 12.3 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 Review** ▪ <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

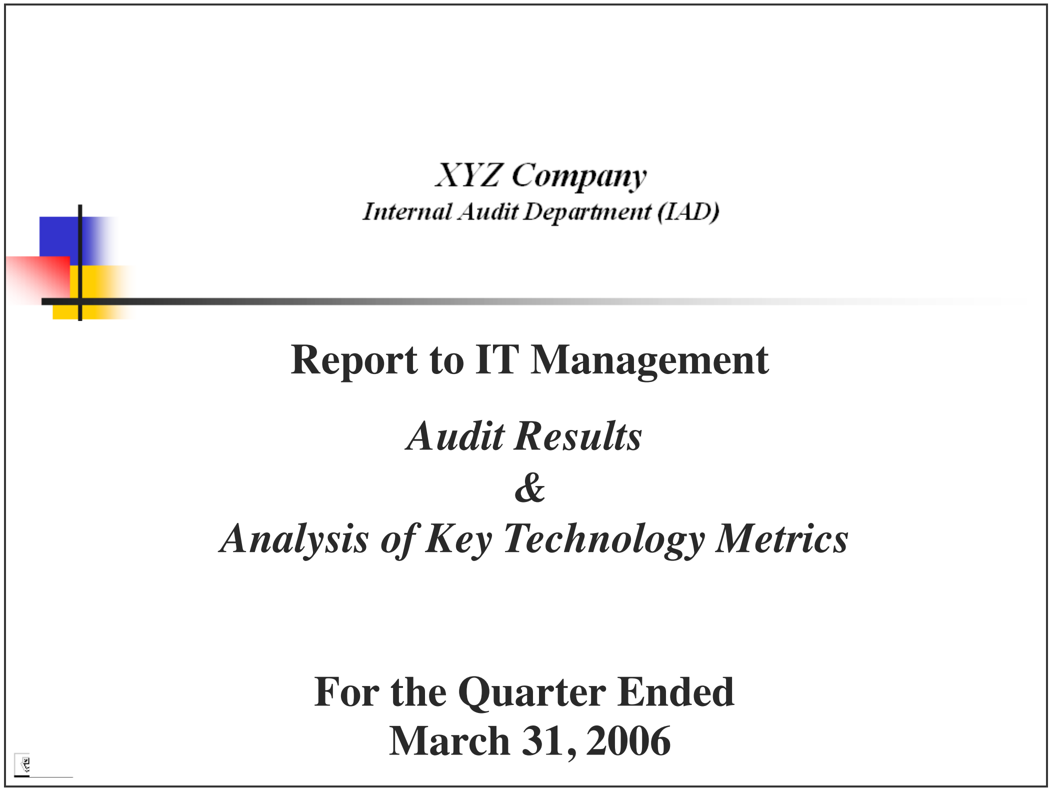
COBIT Control Objectives

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

Preplanned Assessment Questions

Client's Response & Assessment Results

Periodic Management Reports



XYZ Company

Internal Audit Department (IAD)

Report to IT Management

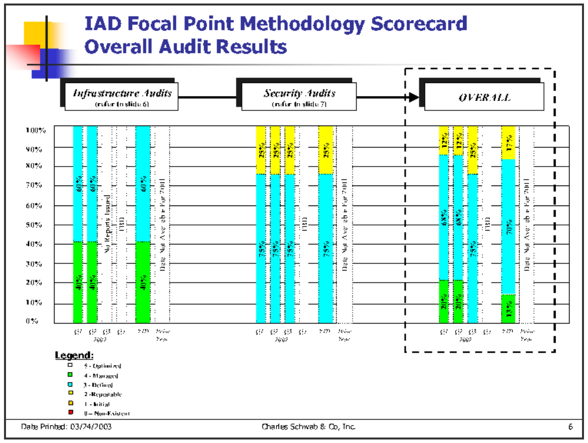
Audit Results

&

Analysis of Key Technology Metrics

For the Quarter Ended
March 31, 2006

Audit Results Metrics

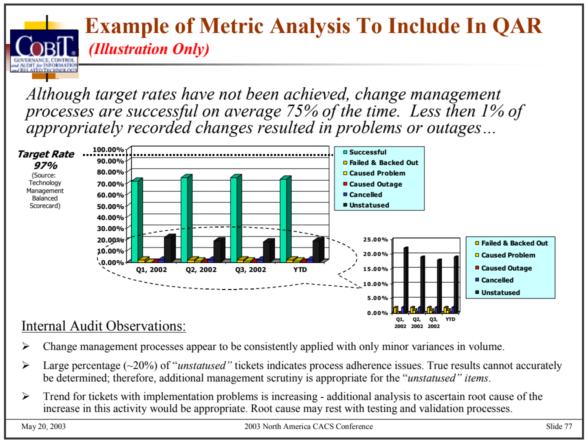


IAD Focal Point Methodology Scorecard
Overall Audit Results

Legend:
- □ 5 - Optimized
- 🟩 4 - Managed
- 🟦 3 - Defined
- 🟨 2 - Repeatable
- 🟧 1 - Initial
- 🟥 0 – Non-Existent

Date Printed: 03/24/2003 Charles Schwab & Co, Inc. 6

Analysis of Key Technology Metrics



Example of Metric Analysis To Include In QAR
(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…

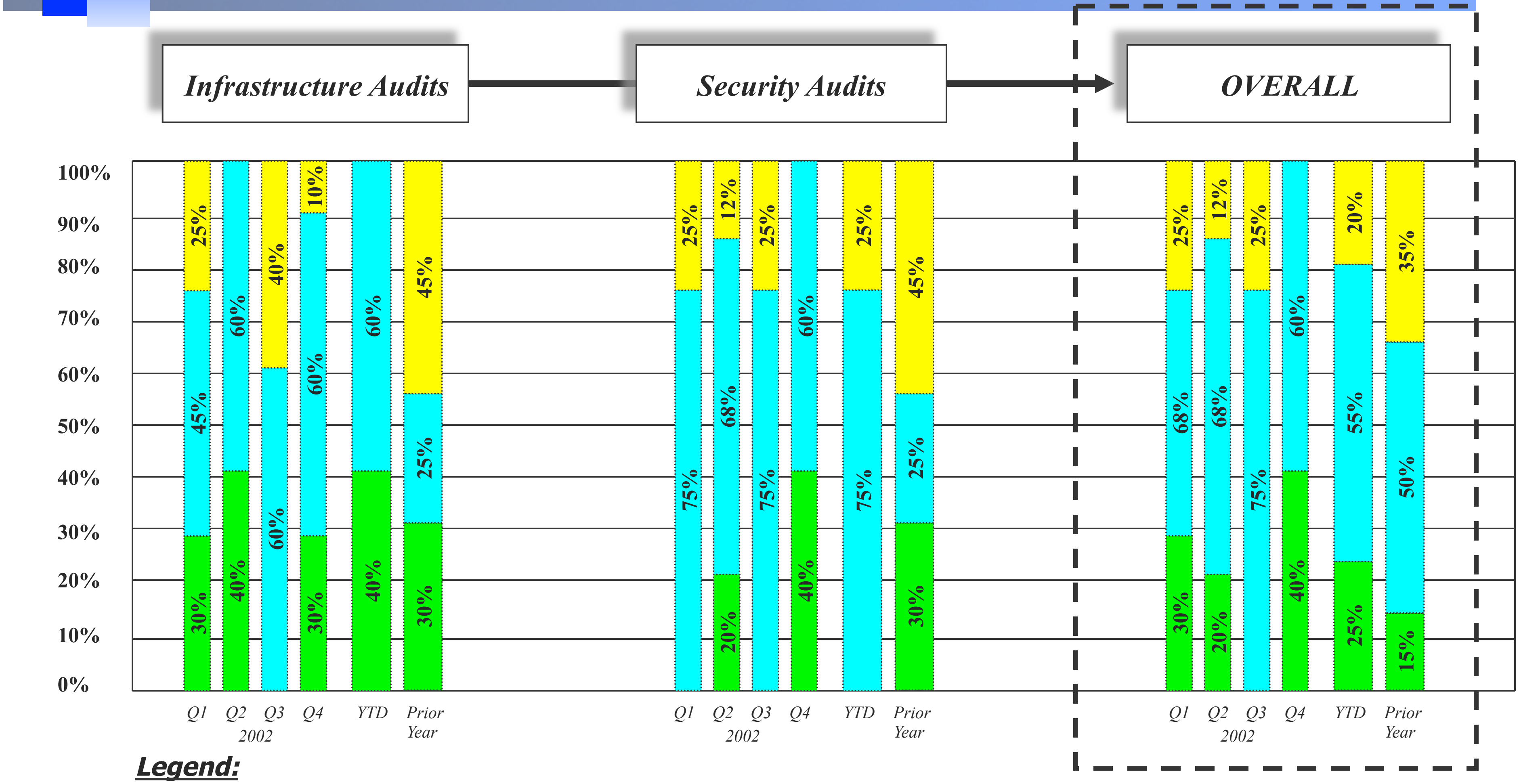
Internal Audit Observations:

- 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.

May 20, 2003 2003 North America CACS Conference Slide 77

Example of Audit Result Metrics

(Illustration Only)



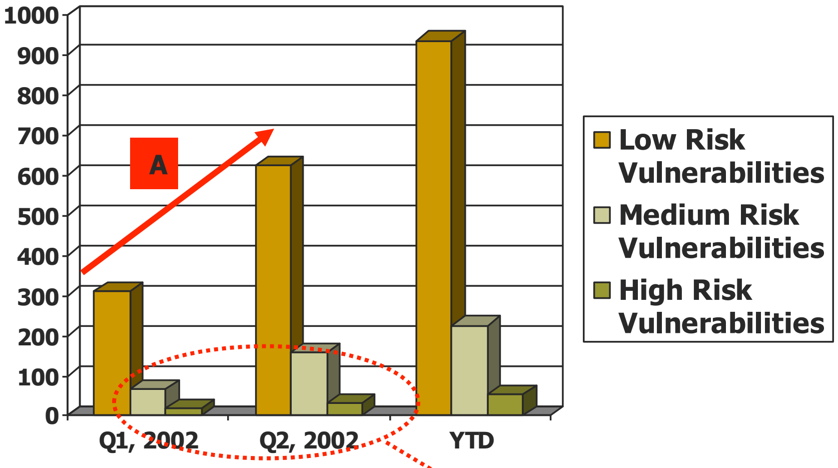
Legend:

- □ 5 - Optimized
- 🟩 4 - Managed
- 🟦 3 - Defined
- 🟨 2 -Repeatable
- 🟧 1 - Initial
- 🟥 0 – Non-Existent

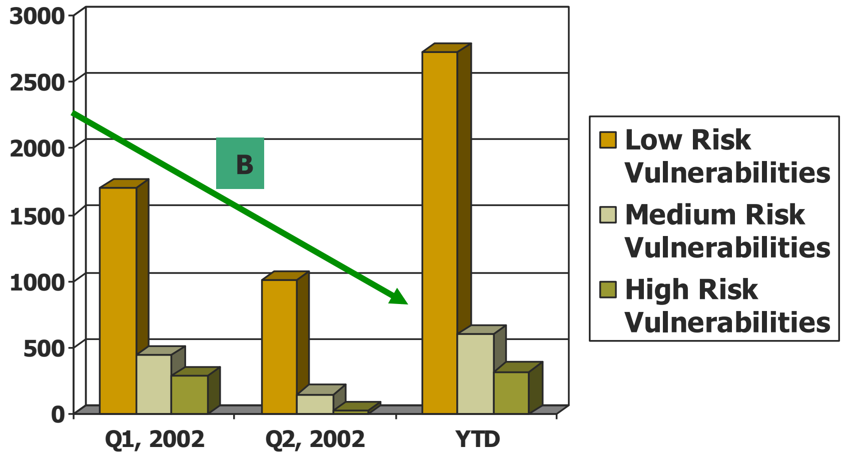
Information Security:
Measuring Performance *(illustration only)*

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

Internal Vulnerability Scans



External Vulnerability Scans



Slight increase in high risk vulnerabilities

Observations:

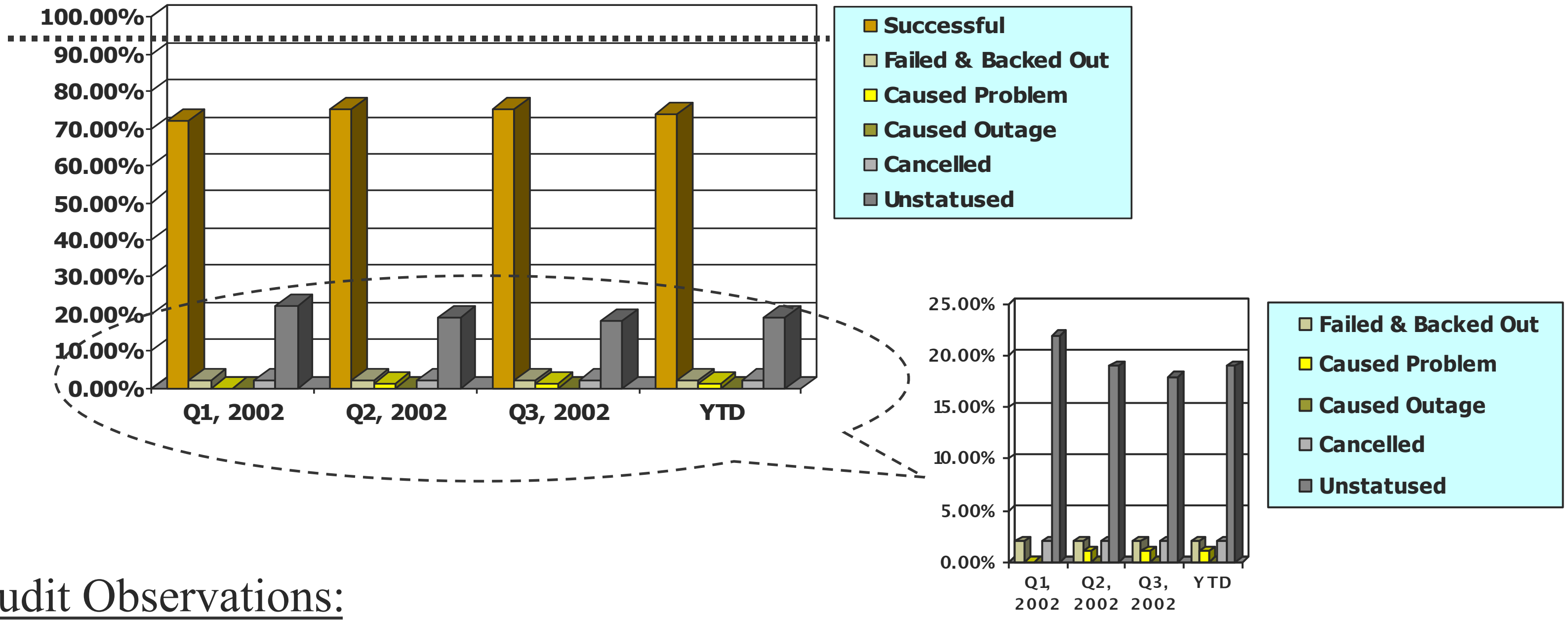
- **A** An increase in *internal* vulnerabilities occurred from Q1 to Q2. The increase is explained due to new system patches checked for by the vulnerability scanner that have not been applied to the XYZ company servers. Technology management appropriately applies patches only after the patches have 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.

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.

AGENDA

- Overview of COBIT®
- Integrating COBIT® Domains into IT Audit Planning & Scope Development
- Integrating COBIT® into the IT Audit Lifecycle
- **COBIT 5 Update**
- Summary & Wrap-up

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

COBIT 5 Update

COBIT 5 Initiative

- The initiative charge from the Board of Directors is to “tie together and reinforce all ISACA knowledge assets with COBIT.”

- The COBIT 5 Task Force:
  - Includes experts from across the ISACA constituency groups
  - Is co-chaired by John Lainhart (Past International President) and Derek Oliver (Past Chairman of the BMIS Development Committee)
  - Reports to the Framework Committee and then the Knowledge Board

COBIT 5 Objectives

COBIT 5 will:

- Provide a renewed and authoritative governance and management framework for enterprise information and related technology, building on the current widely recognized and accepted COBIT framework, linking together and reinforcing all other major ISACA frameworks and guidance such as:

Val IT	**Risk IT**
BMIS	**ITAF**
Board Briefing	**Taking Governance Forward**

- Connect to other major frameworks and standards in the marketplace (ITIL, ISO standards, etc.)

What Will Be Delivered?

- An enterprise-wide, “end-to-end” framework addressing governance and management of information and related technology

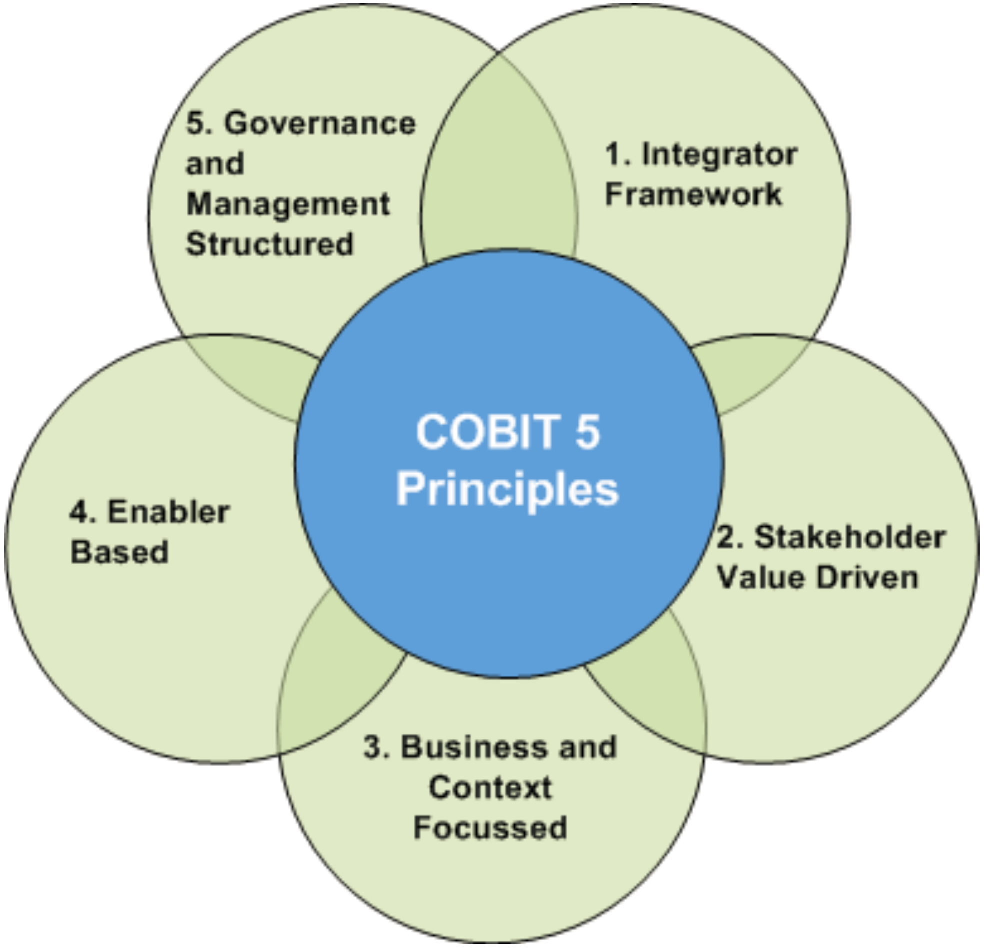
- The framework structure will include familiar components such as a domain/process model and other components such as governance/management practices, RACI charts and inputs/ outputs.

- An initial COBIT 5 product architecture, identifying the types of products and other guidance that could be developed for specific IT professional audiences (e.g., assurance, security, risk) in support of enterprise business needs

The COBIT 5 Framework

- An initial publication introduces, defines and describes the components that make up the COBIT Framework
  - Principles
  - Architecture
  - Enablers
  - Introduction to implementation guidance and the COBIT process assessment approach

COBIT 5 Principles



COBIT 5 Principles

1. Integrator Framework

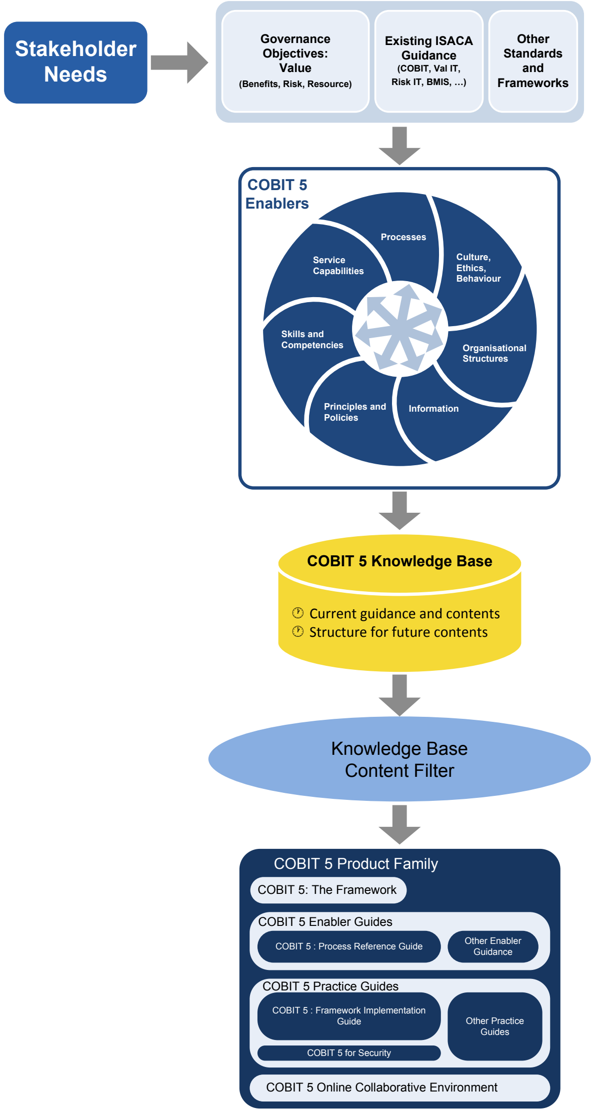
2. Stakeholder Value Driven

3. Business and Context Focussed

4. Enabler Based

5. Governance and Management Structured

COBIT 5 Architecture



Stakeholder Needs

Governance Objectives: Value (Benefits, Risk, Resource)

Existing ISACA Guidance (COBIT, Val IT, Risk IT, BMIS, …)

Other Standards and Frameworks

COBIT 5 Enablers

COBIT 5 Knowledge Base

- Current guidance and contents
- Structure for future contents

Knowledge Base Content Filter

COBIT 5 Product Family

COBIT 5: The Framework

COBIT 5 Enabler Guides

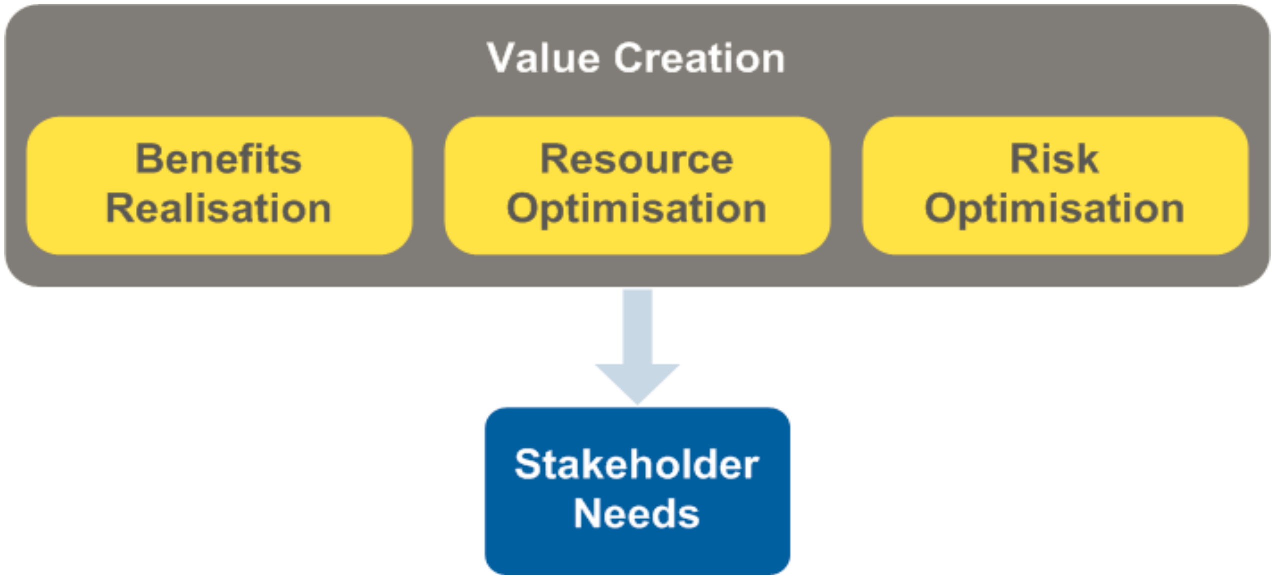
- COBIT 5 : Process Reference Guide
- Other Enabler Guidance

COBIT 5 Practice Guides

- COBIT 5 : Framework Implementation Guide
- COBIT 5 for Security
- Other Practice Guides

COBIT 5 Online Collaborative Environment

Governance Objective

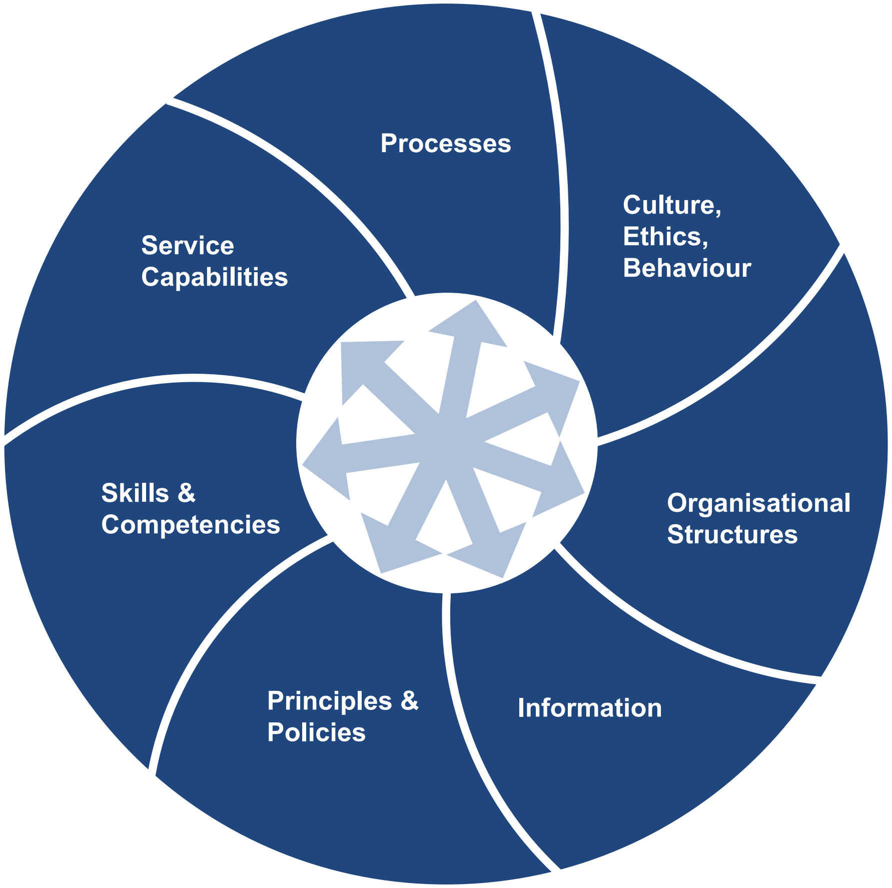


Benefits

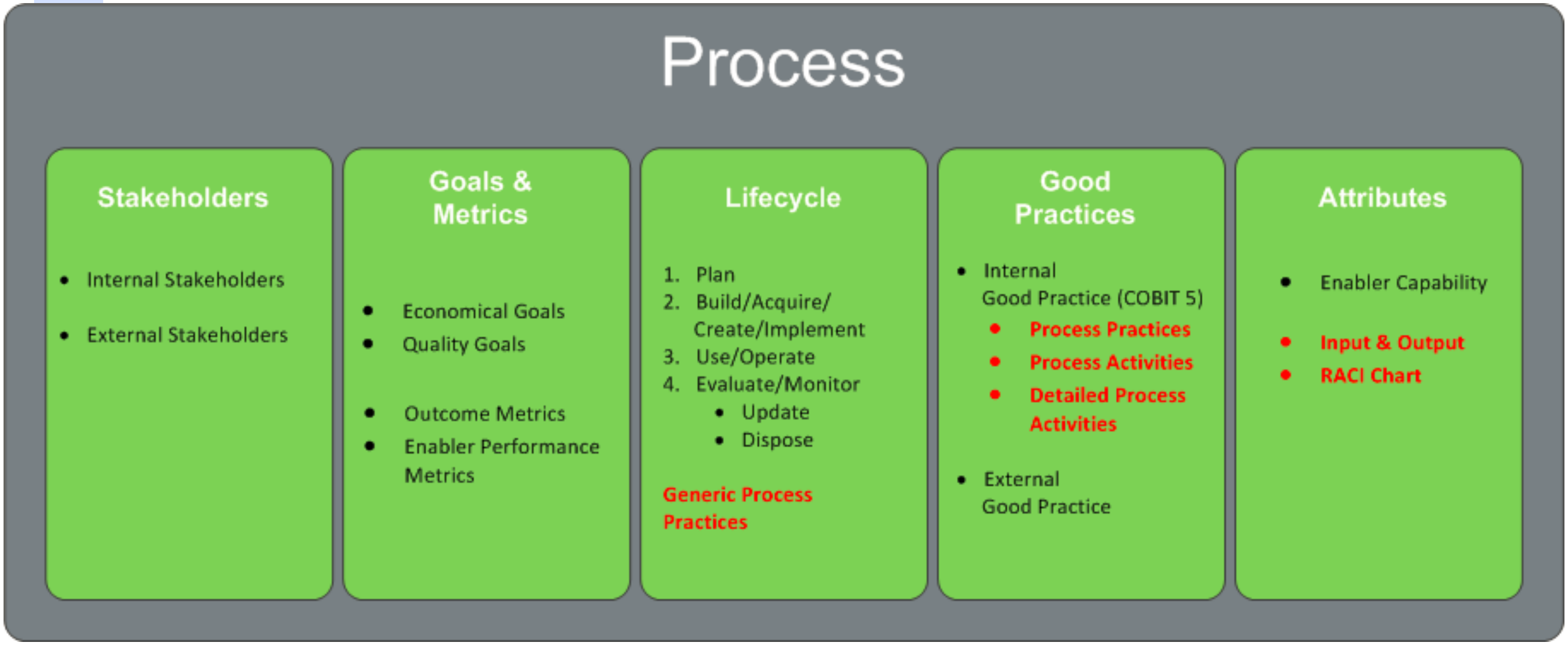
- **Enterprise-wide benefits:**
  - **Increased value creation through effective governance and management of enterprise information and technology assets**
  - **Increased business user satisfaction with IT engagement and services– IT seen as a key enabler.**
  - **Increased compliance with relevant laws, regulations and policies**
- **IT function becomes more business focused**

Enabler-based

COBIT 5 Enablers—Systemic Model With Interacting Enablers



Process Enabler Model



Process

Stakeholders

- Internal Stakeholders
- External Stakeholders

Goals & Metrics

- Economical Goals
- Quality Goals
- Outcome Metrics
- Enabler Performance Metrics

Lifecycle

1. Plan
2. Build/Acquire/Create/Implement
3. Use/Operate
4. Evaluate/Monitor
   - Update
   - Dispose

Generic Process Practices

Good Practices

- Internal Good Practice (COBIT 5)
  - Process Practices
  - Process Activities
  - Detailed Process Activities
- External Good Practice

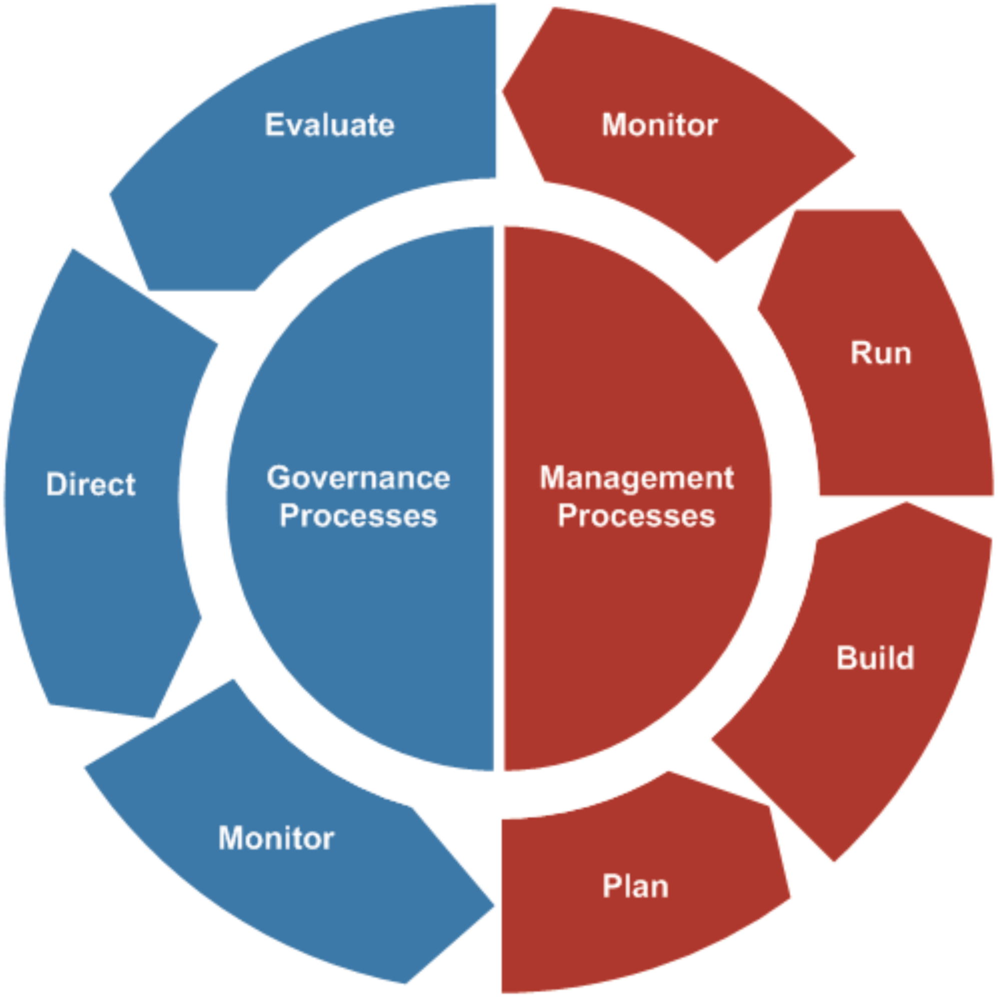
Attributes

- Enabler Capability
- Input & Output
- RACI Chart

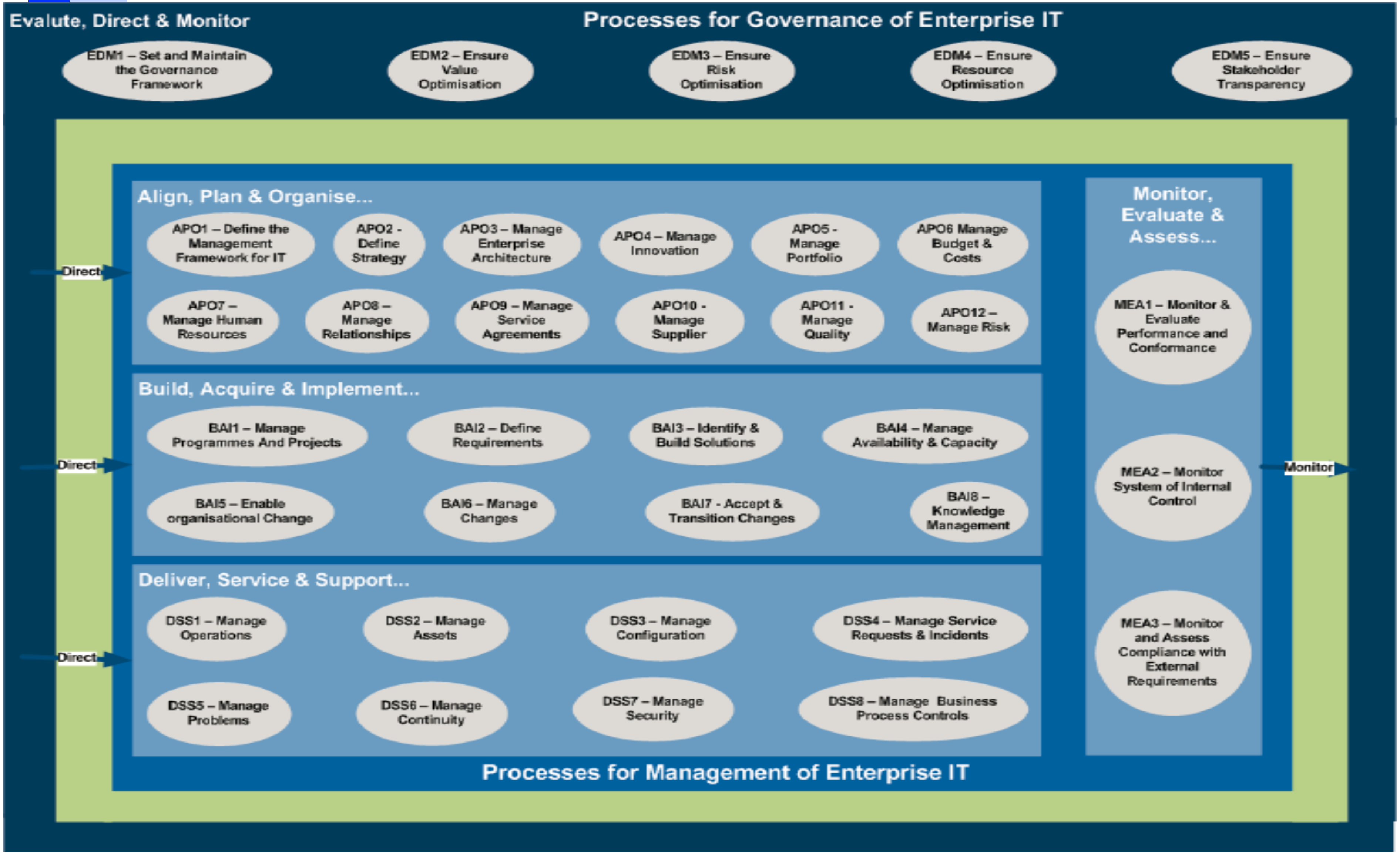
Process Reference Guide

- A separate publication that expands on the process-enabler model
- Contains full details of the COBIT processes in a similar way to the process documentation in COBIT 4.1

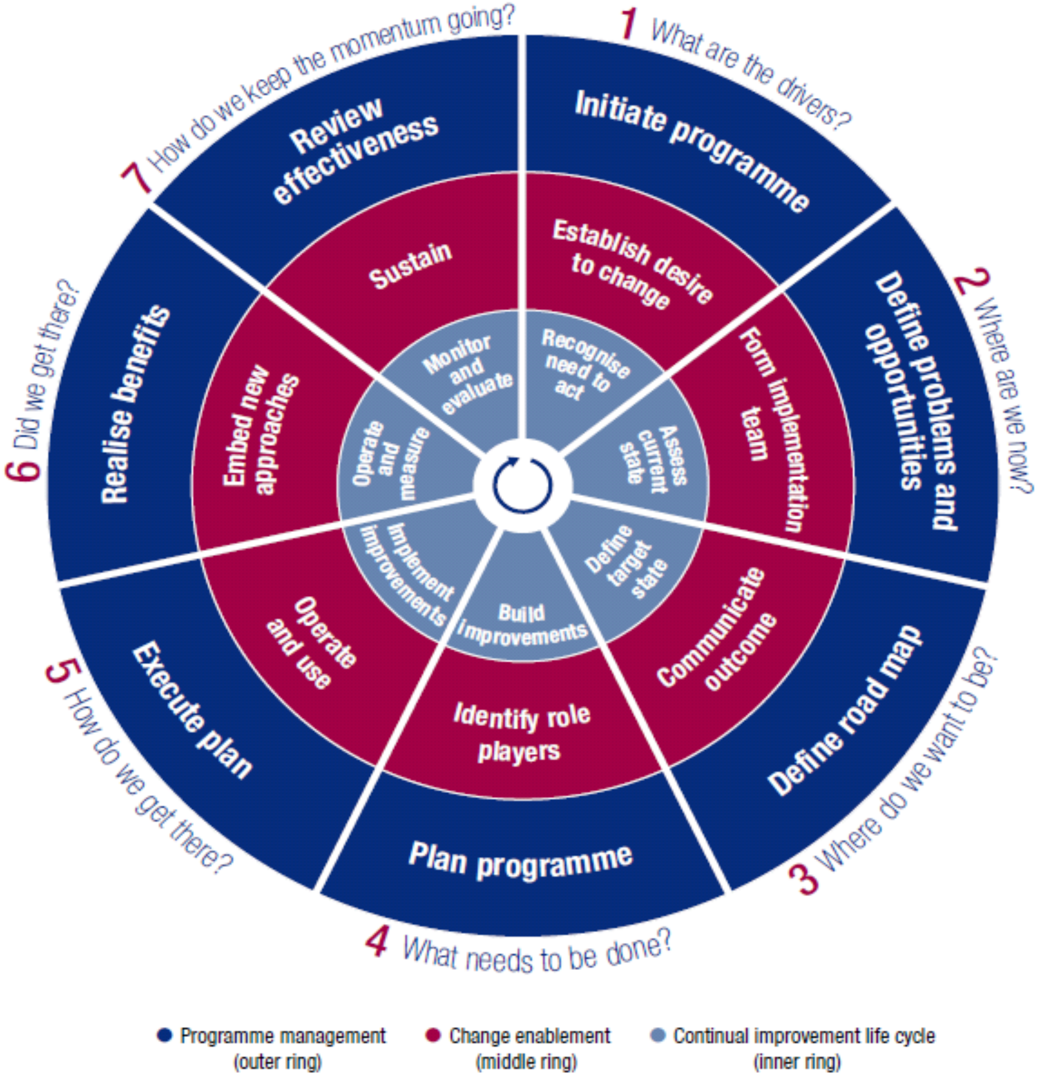
Governance and Management Processes



Process Reference Model
(36 Processes)


Evalute, Direct & Monitor
Processes for Governance of Enterprise IT
EDM1 – Set and Maintain the Governance Framework
EDM2 – Ensure Value Optimisation
EDM3 – Ensure Risk Optimisation
EDM4 – Ensure Resource Optimisation
EDM5 – Ensure Stakeholder Transparency
Align, Plan & Organise...
APO1 – Define the Management Framework for IT
APO2 - Define Strategy
APO3 – Manage Enterprise Architecture
APO4 – Manage Innovation
APO5 - Manage Portfolio
APO6 Manage Budget & Costs
APO7 – Manage Human Resources
APO8 – Manage Relationships
APO9 – Manage Service Agreements
APO10 - Manage Supplier
APO11 - Manage Quality
APO12 – Manage Risk
Build, Acquire & Implement...
BAI1 – Manage Programmes And Projects
BAI2 – Define Requirements
BAI3 – Identify & Build Solutions
BAI4 – Manage Availability & Capacity
BAI5 – Enable organisational Change
BAI6 – Manage Changes
BAI7 - Accept & Transition Changes
BAI8 – Knowledge Management
Deliver, Service & Support...
DSS1 – Manage Operations
DSS2 – Manage Assets
DSS3 – Manage Configuration
DSS4 – Manage Service Requests & Incidents
DSS5 – Manage Problems
DSS6 – Manage Continuity
DSS7 – Manage Security
DSS8 – Manage Business Process Controls
Monitor, Evaluate & Assess...
MEA1 – Monitor & Evaluate Performance and Conformance
MEA2 – Monitor System of Internal Control
MEA3 – Monitor and Assess Compliance with External Requirements
Direct
Direct
Direct
Monitor
Processes for Management of Enterprise IT

Implementation Guidance



- A separate publication
- Based on the current implementation guidance publication

On COBIT Process Capability Assessment

- The process maturity model of COBIT 4.1 has been replaced with a capability model based on ISO/IEC 15504 to align with and support a separate ISACA initiative, the COBIT Assessment Program (CAP).

- There are a number of benefits in doing so:
  - Focus first on confirming that a process is achieving its intended purpose and delivering its required outcomes as expected.
  - Simplification of the content supporting process assessment.
  - Improved reliability and repeatability of process capability assessment activities and evaluations, reduced debates and disagreements between stakeholders on assessment results. Increased usability of process capability assessment results, as the new approach establishes a basis for more formal, rigorous assessments to be performed, for both internal and potential external purposes.
  - Compliance with a generally accepted process assessment standard and therefore strong support for process assessment approach in the market.

Process Capability Model Comparison

COBIT 4.1 Maturity Model Levels	COBIT 5 ISO/IEC 15504 Based Capability Levels	Meaning of the COBIT 5 ISO/IEC 15504 Based Capability Levels	Context
5. Optimised	5. Optimised	Continuously improved to meet relevant current and projected enterprise goals.	Enterprise view/ corporate knowledge
4. Managed and Measurable	4. Predictable	Operates within defined limits to achieve its process outcomes.	
3. Defined	3. Established	Implemented using a defined process that is capable of achieving its process outcomes.	
N/A	2. Managed	Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	Instance view/ individual knowledge
N/A	1. Performed	Process achieves its process purpose.	
2. Repeatable 1. *Ad Hoc* 0. Non-existent	0. Incomplete	Not implemented or little or no evidence of any systematic achievement of the process purpose.	

Key Messages

- See Handout

Summary

- COBIT 5 is a major, high-profile, strategic initiative for ISACA. Market validation of the development work (i.e., the public exposure of the Framework and Process Reference Guide products) is planned for 27 June and to run throughout July to ensure that ISACA remains on the right track to satisfy market needs.
- SME exposure of the implementation guidance will follow later in 2011.
- Delivery of all three products to the market is planned for early 2012.
- More information is on the ISACA web site, *www.isaca.org/COBIT5*

Questions / Thank You!

Lance M. Turcato, CGEIT, CRISC, CISA, CISM, CPA, CITP

VP, Information Systems Audit
FHLBank San Francisco
Email: turcatol@fhlbsf.com