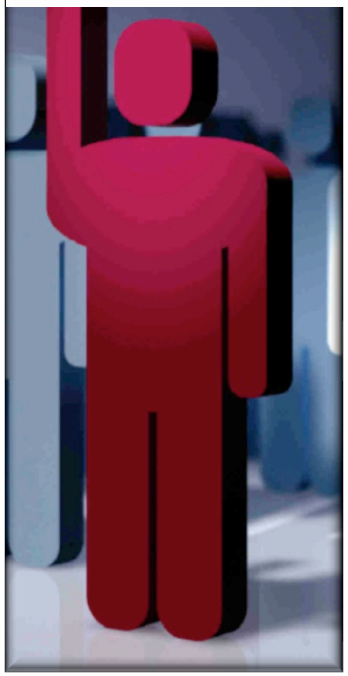
ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Governance Institute®
Leading the IT Governance Community



C13 - COBIT Fundamentals and Uses

Miguel (Mike) O. Villegas, CISA, CISSP

2008 SF ISACA Fall Conference
San Francisco
September 22, 2008

Agenda

- Mission Statement and Objectives
- The Need for COBIT
- COBIT Principle
- IT Governance Focus Areas
- COBIT Content Diagram
- Interrelationships of COBIT Components
- COBIT Framework
- COBIT 4.1 Update
- COBIT Campus
- LA ISACA COBIT Survey
- IT Governance Certification

Mission and Objectives

Mission Statement:

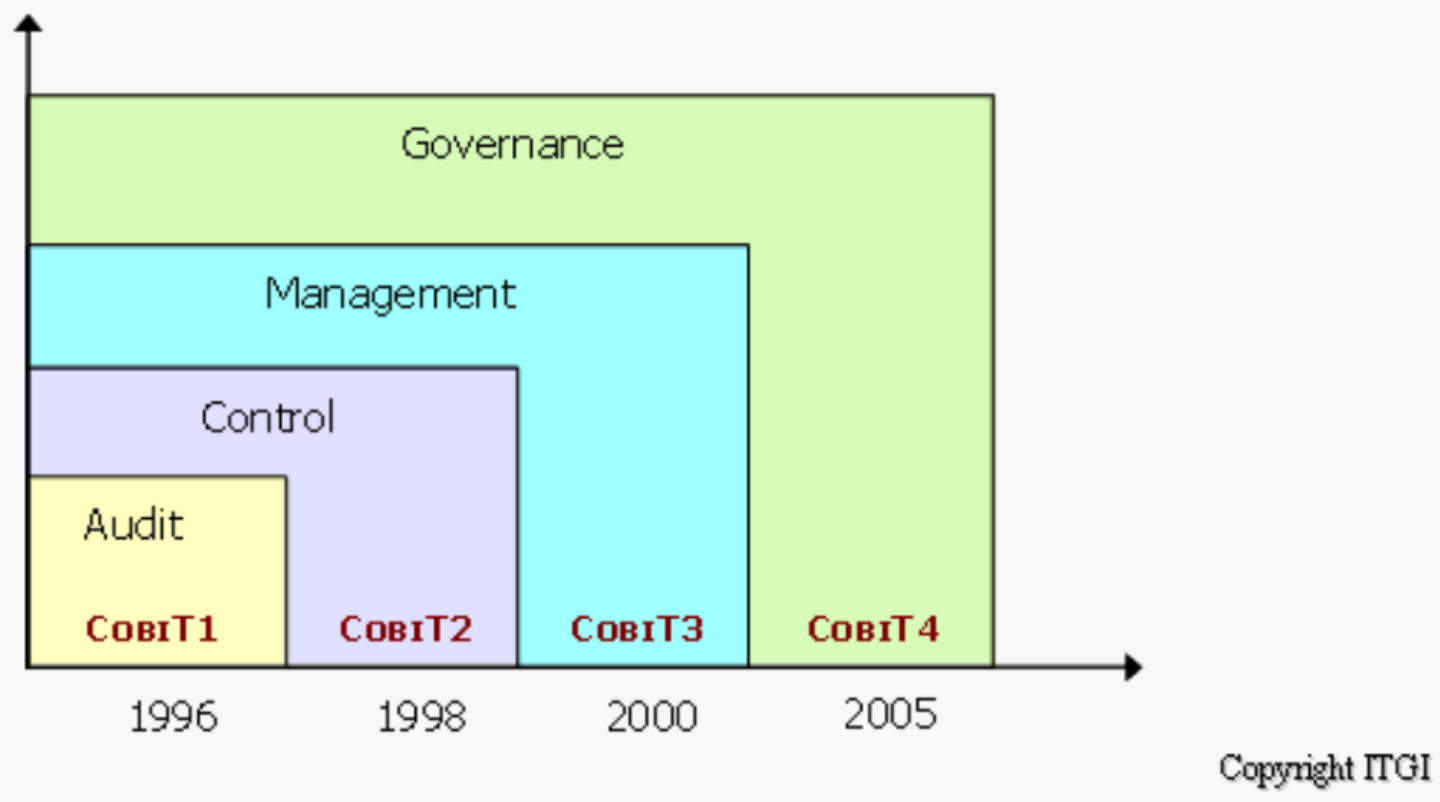
- To research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals

Objectives:

- Aligning IT strategy with the business strategy
- Assuring investors and shareholders that a 'standard of due care' around mitigating IT risks is being met by the organization
- Cascading IT strategy and goals down into the enterprise
- Obtaining value from IT investments
- Providing organizational structures that facilitate the implementation of strategy and goals
- Creating constructive relationships and effective communication between the business and IT, and with external partners
- Measuring IT's performance

History of CobiT

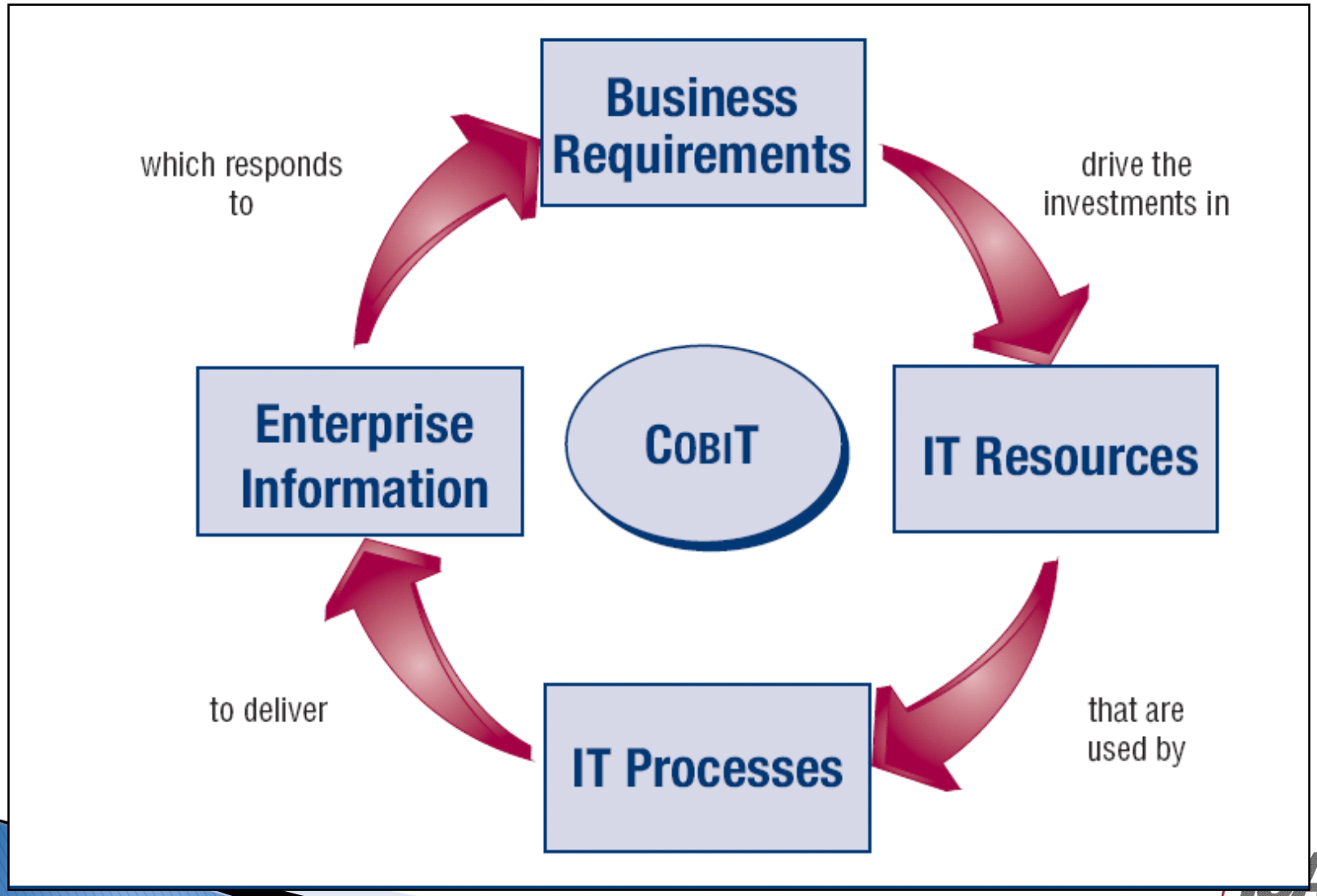
CobiT has evolved from an auditor's tool to an IT governance framework, used increasingly by IT management



The Need for COBIT

- Better return for IT investment
- Concern over generally increasing IT expenditure
- Regulatory requirements for IT controls
- Service provider and vendor management
- Increasingly complex IT-related risks
- IT governance
- IT activities that increase business value and reduce business risk
- Need to optimize costs
- Controls benchmarking
- Growing acceptance of well-regarded frameworks:
  - COBIT
  - ITIL
  - ISO 27000
  - ISO 9001:2000
  - CMMI
  - PRINCE2
  - PMBOK

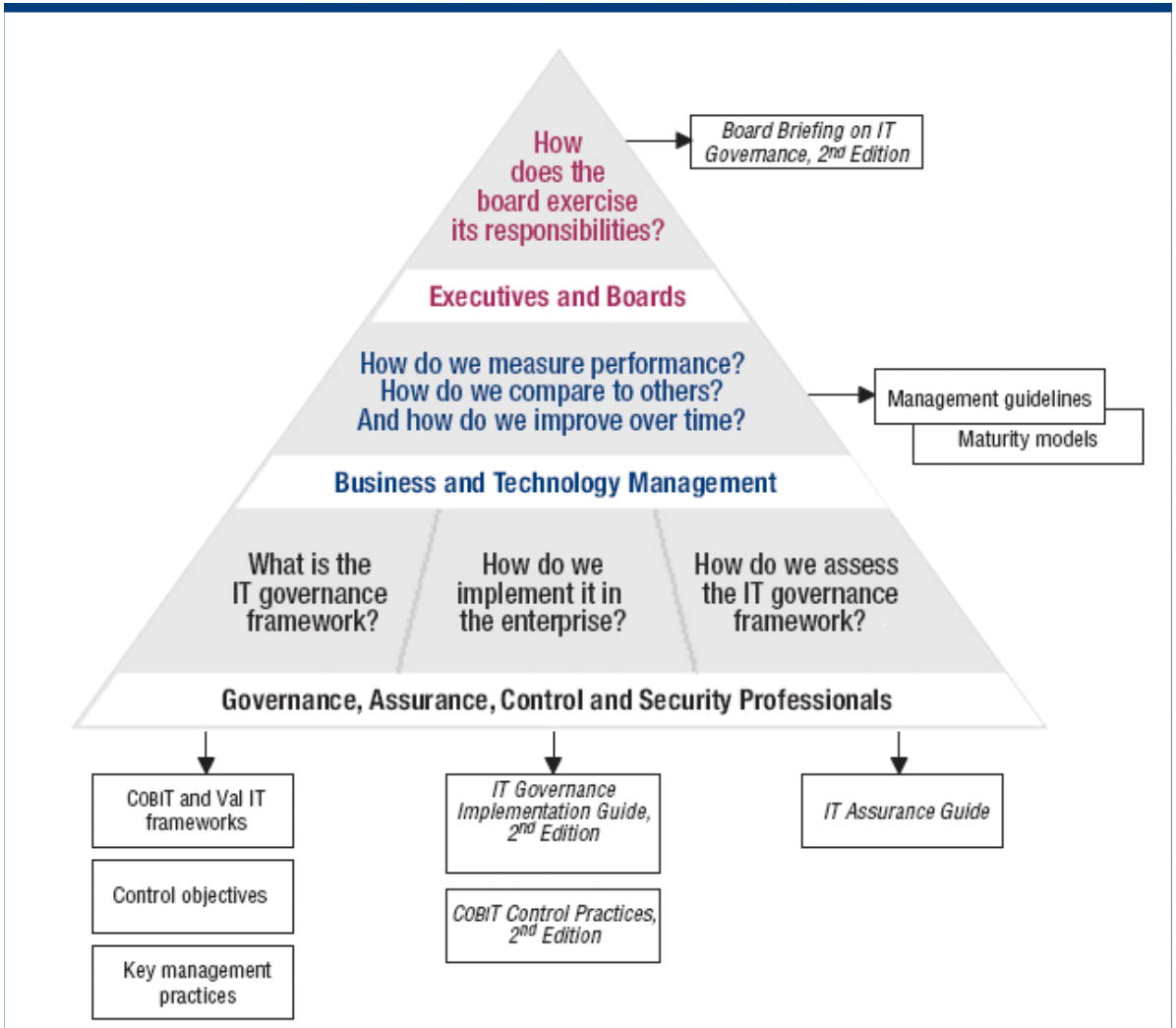
COBIT Principle



IT Governance Focus Areas

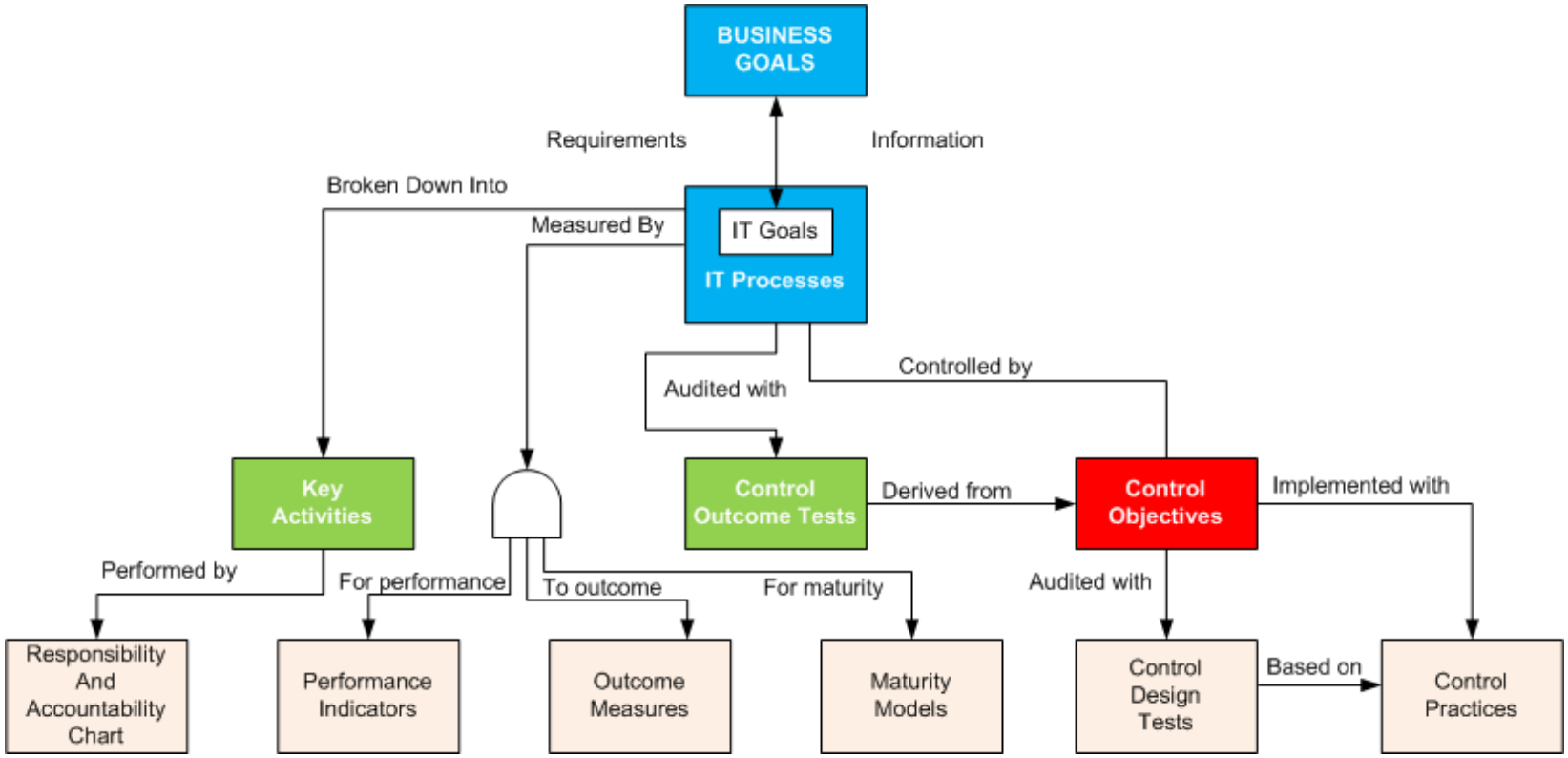
- Strategic Alignment
- Value Delivery
- Resource Management
- Risk Management
- Performance Measures

COBIT Content Diagram



This COBIT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (COBIT *Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (COBIT *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

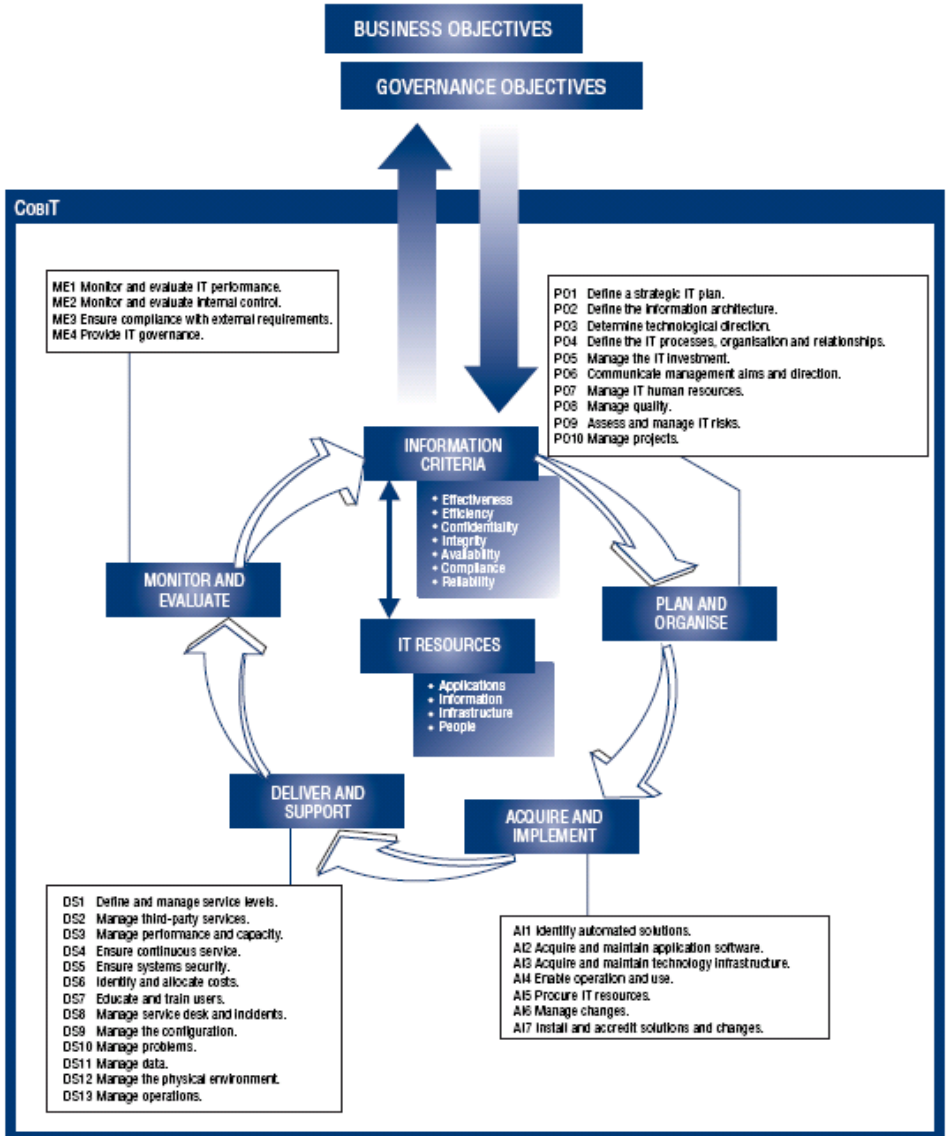
Interrelationships of COBIT Components



ISACA Serving IT Governance Professionals
San Francisco Chapter

COBIT Framework

In more detail, the overall COBIT framework can be shown graphically, as depicted in this schematic. It shows the COBIT process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements.

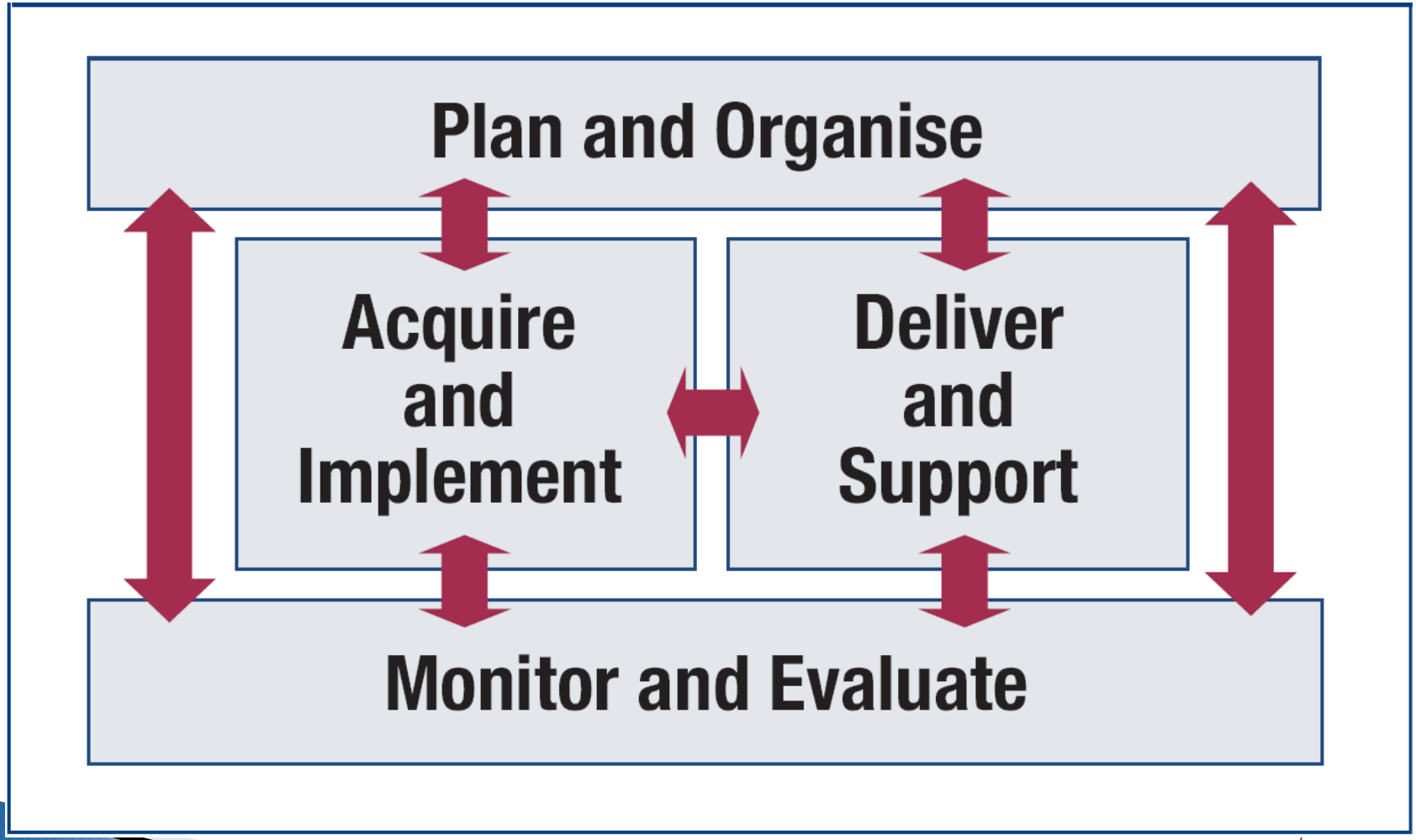


Four Domains:

- PO – Plan and Organize
- AI – Acquire and Implement
- DS – Deliver and Support
- ME – Monitor and Evaluate

10

COBIT Framework (Cont'd)



Plan and Organize

Process	Description
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization 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

Process	Description
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

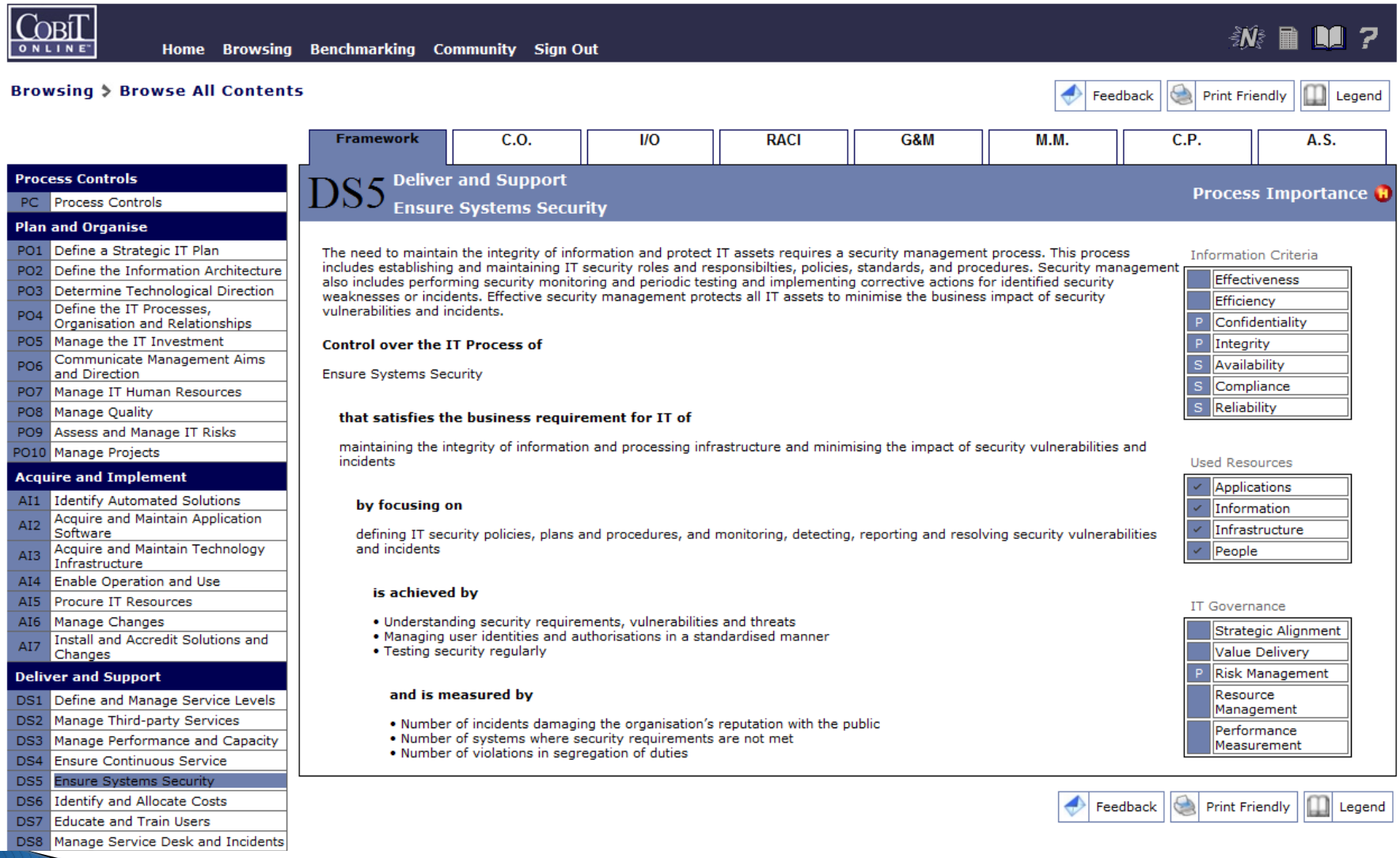
Deliver and Support

Process	Description
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

Process	Description
ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance With External Requirements
ME4	Provide IT Governance

Framework, Control Objectives and Management Guidelines now one integrated book

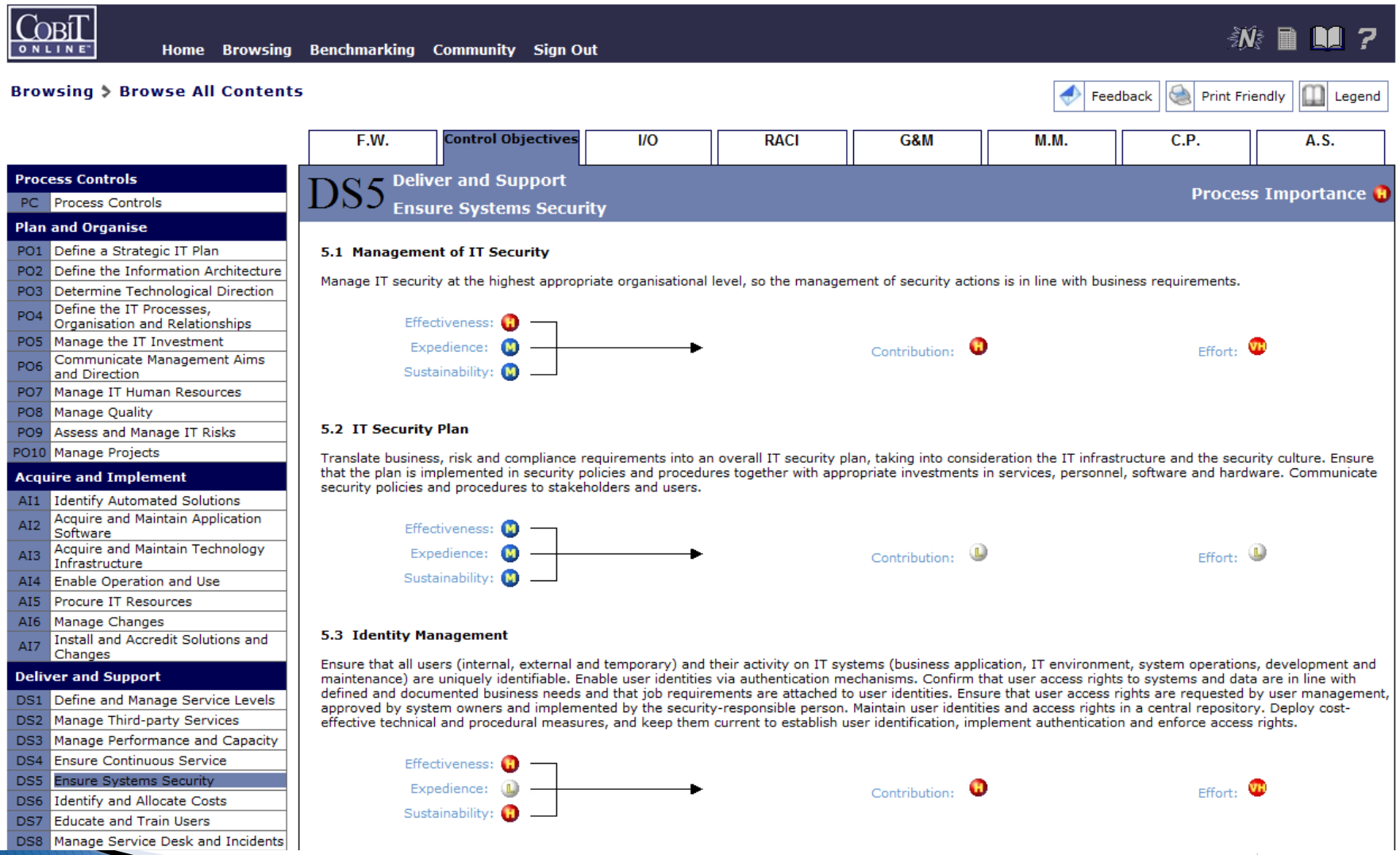


ISACA Serving IT Governance Professionals
San Francisco Chapter

Deliver and Support

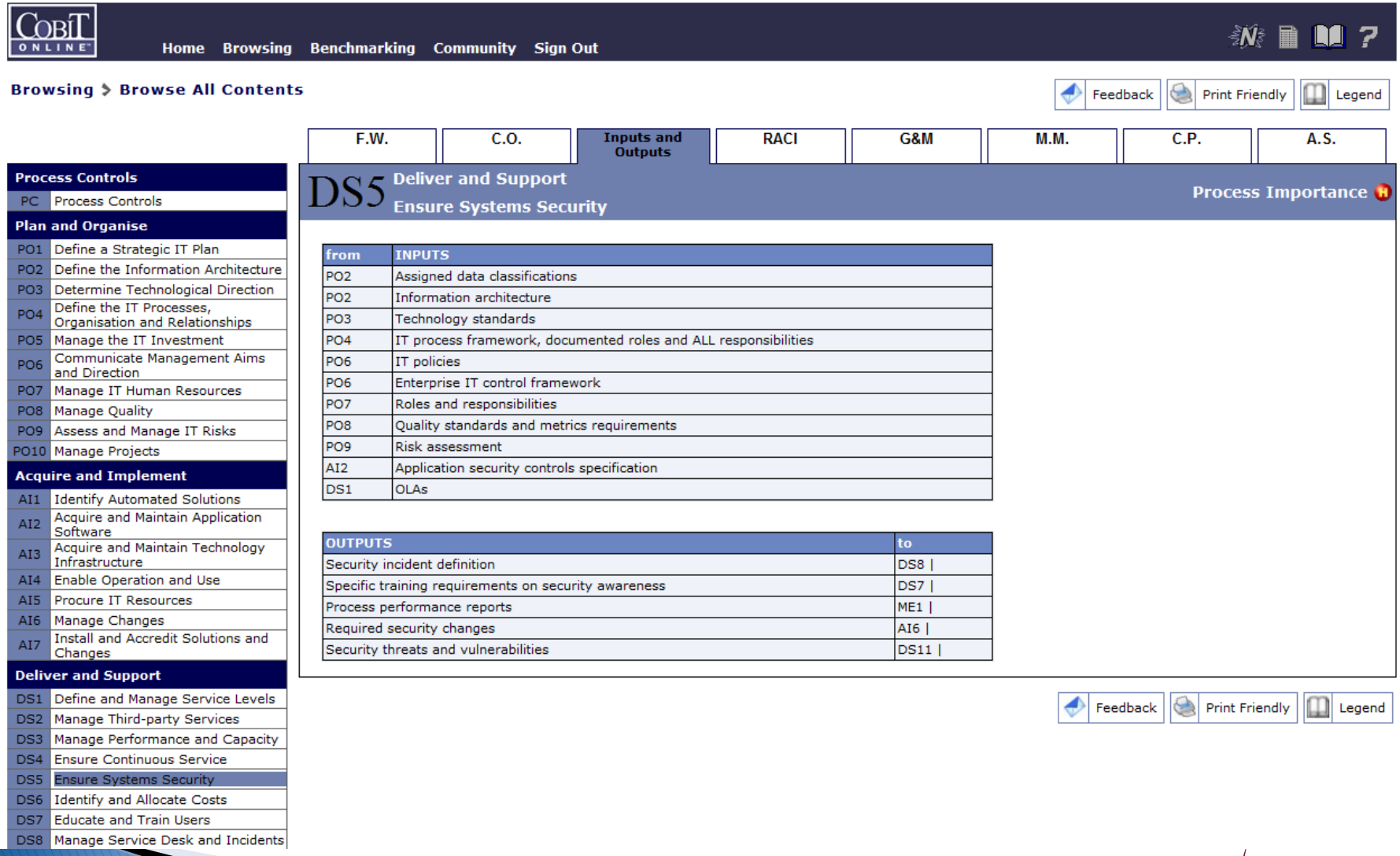
Process	Description
DS5.1	Management of IT Security
DS5.2	IT Security Plan
DS5.3	Identity Management
DS5.4	User Account Management
DS5.5	Security Testing, Surveillance and Monitoring
DS5.6	Security Incident Definition
DS5.7	Protection of Security Technology
DS5.8	Cryptographic Key Management
DS5.9	Malicious Software Prevention, Detection and Correction
DS5.10	Network Security
DS5.11	Exchange of Sensitive Data

Control Objectives

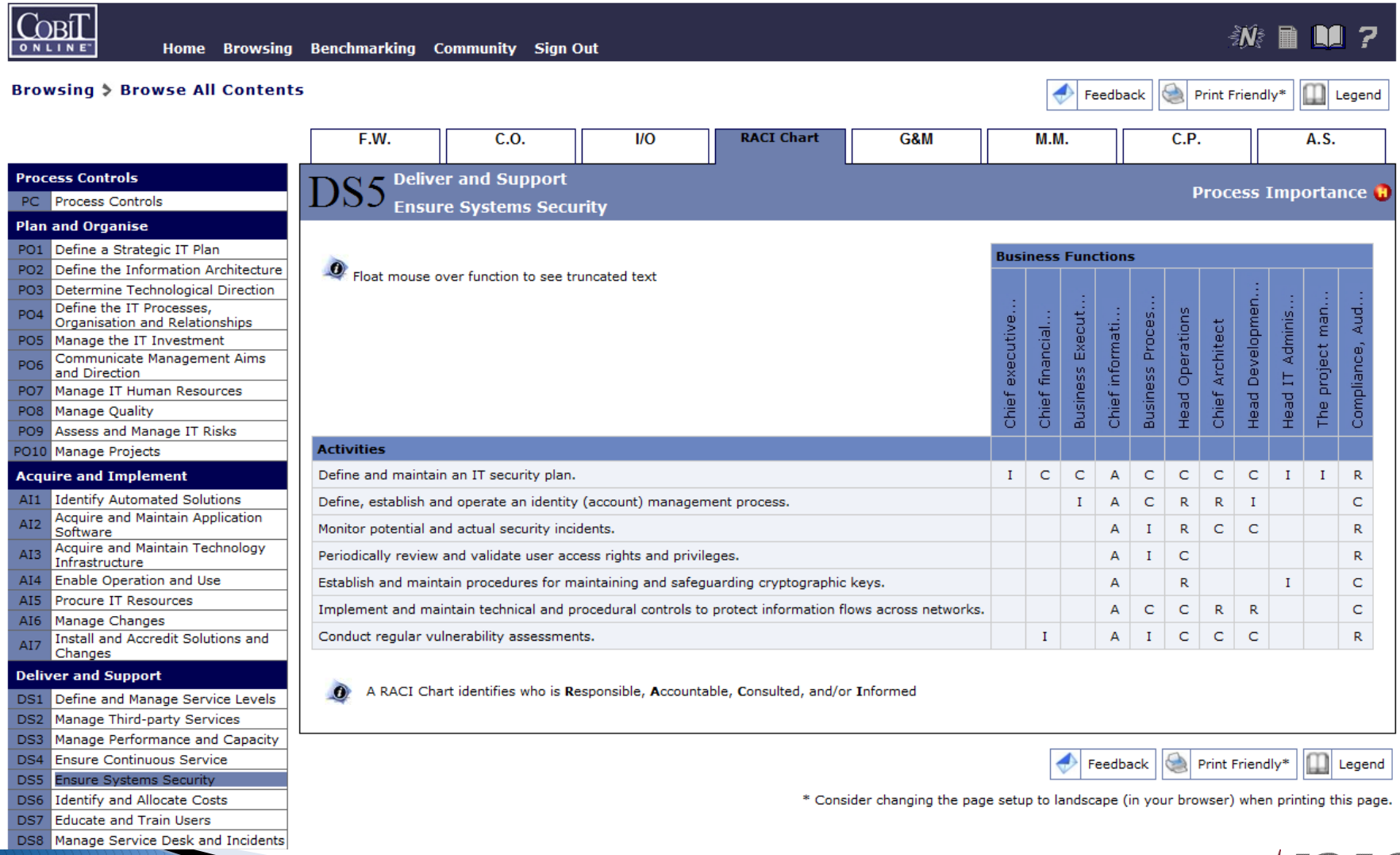


ISACA Serving IT Governance Professionals
San Francisco Chapter

Inputs and Outputs



Added RACI chart (Responsible, Accountable, Consulted, Informed)



COBIT ONLINE

Home | Browsing | Benchmarking | Community | Sign Out

Browsing > Browse All Contents

Feedback | Print Friendly* | Legend

F.W. | C.O. | I/O | RACI Chart | G&M | M.M. | C.P. | A.S.

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
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents

DS5 Deliver and Support
Ensure Systems Security

Process Importance H

Float mouse over function to see truncated text

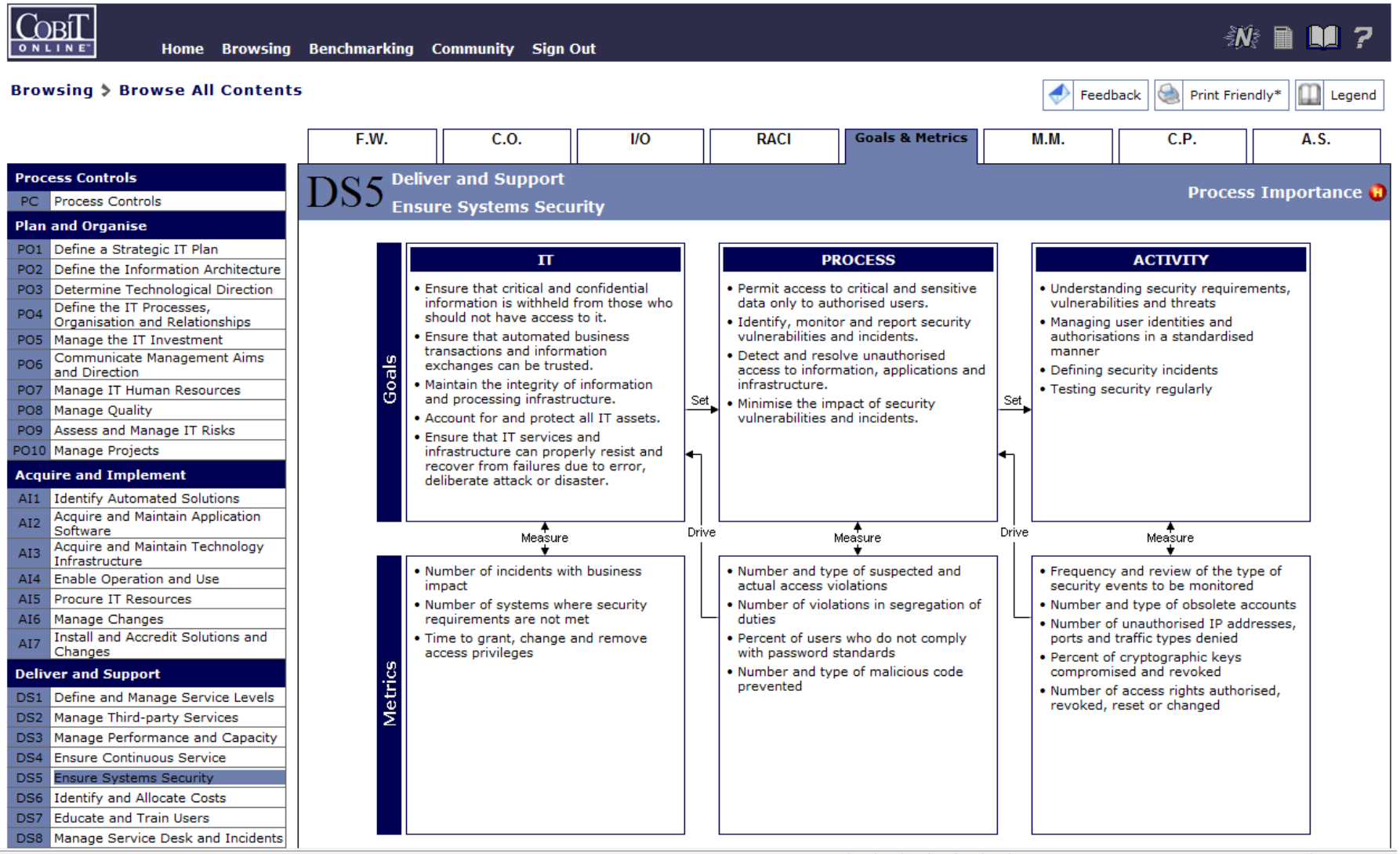
Activities	Chief executive...	Chief financial...	Business Execut...	Chief informati...	Business Proces...	Head Operations	Chief Architect	Head Developmen...	Head IT Adminis...	The project man...	Compliance, Aud...
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate 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.				A	I	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 **R**esponsible, **A**ccountable, **C**onsulted, and/or **I**nformed

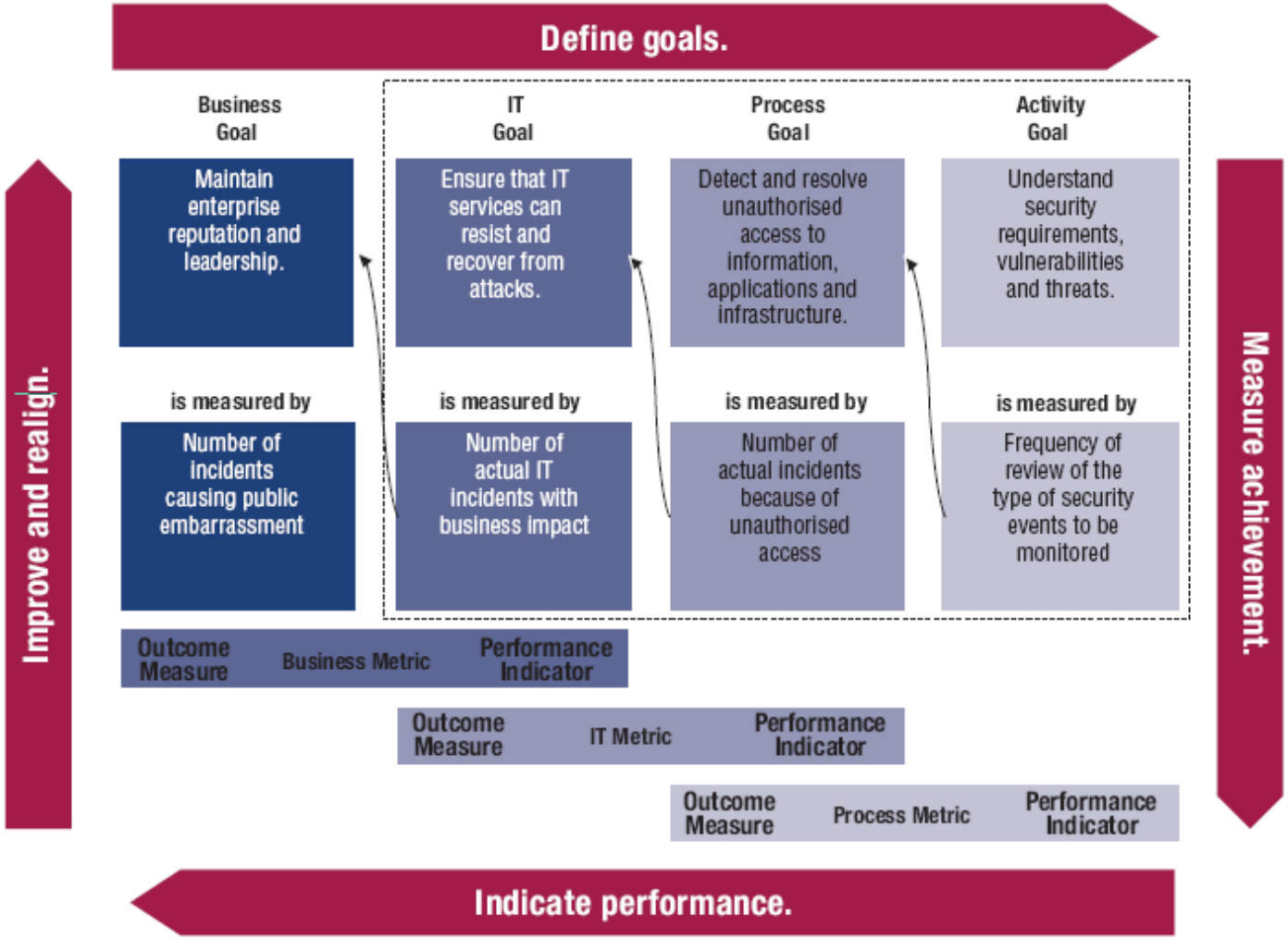
Feedback | Print Friendly* | Legend

* Consider changing the page setup to landscape (in your browser) when printing this page.

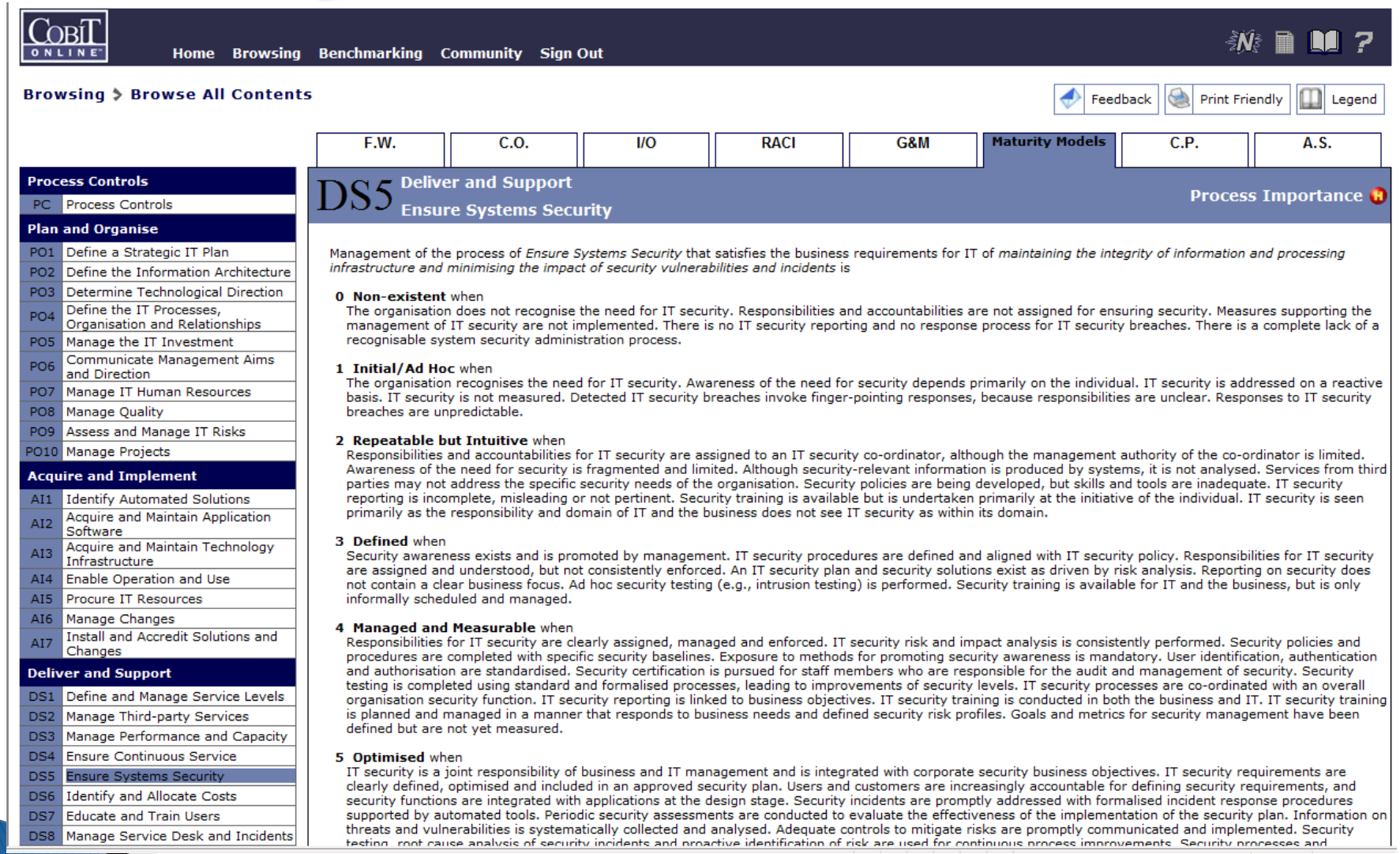
Goals and Metrics



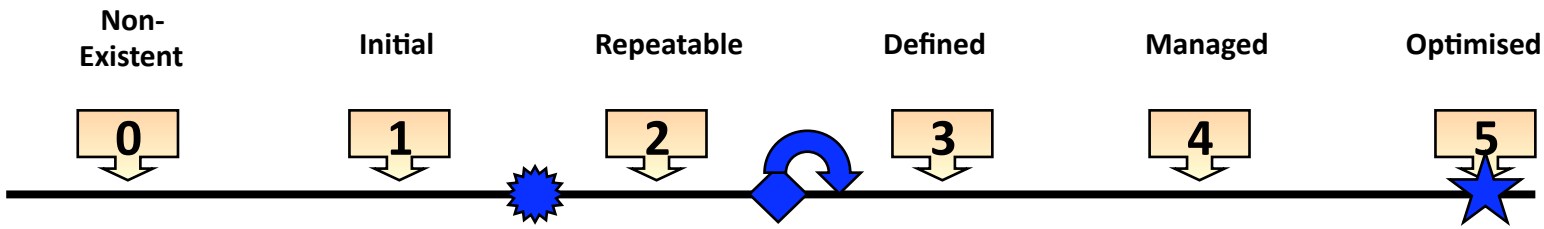
Relationship Between Processes, Goals and Metrics (DS5)



Maturity Model



Maturity Model



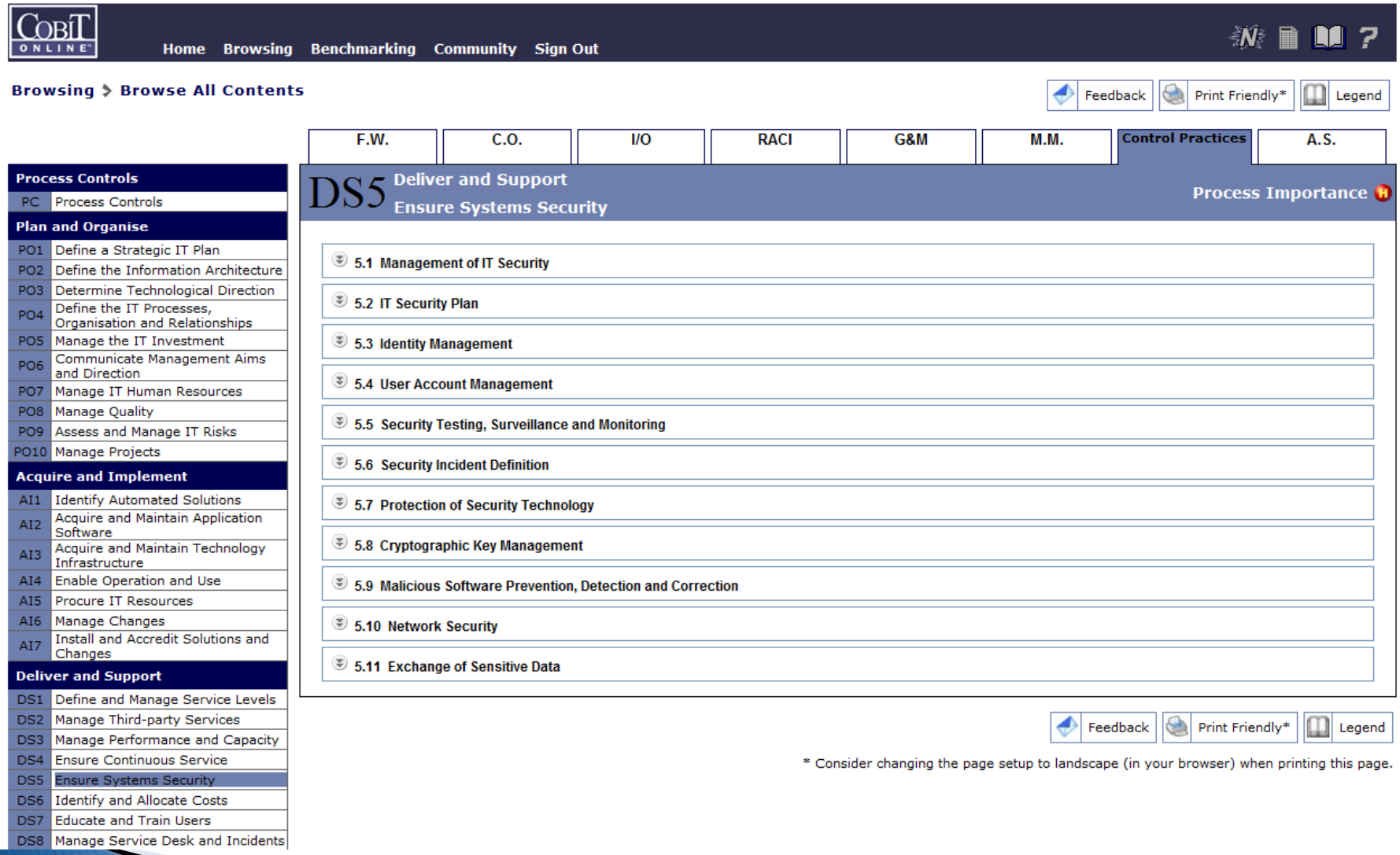
Legend for symbols used

- Enterprise current status
- International standard guidelines
- Industry best practice
- Enterprise strategy

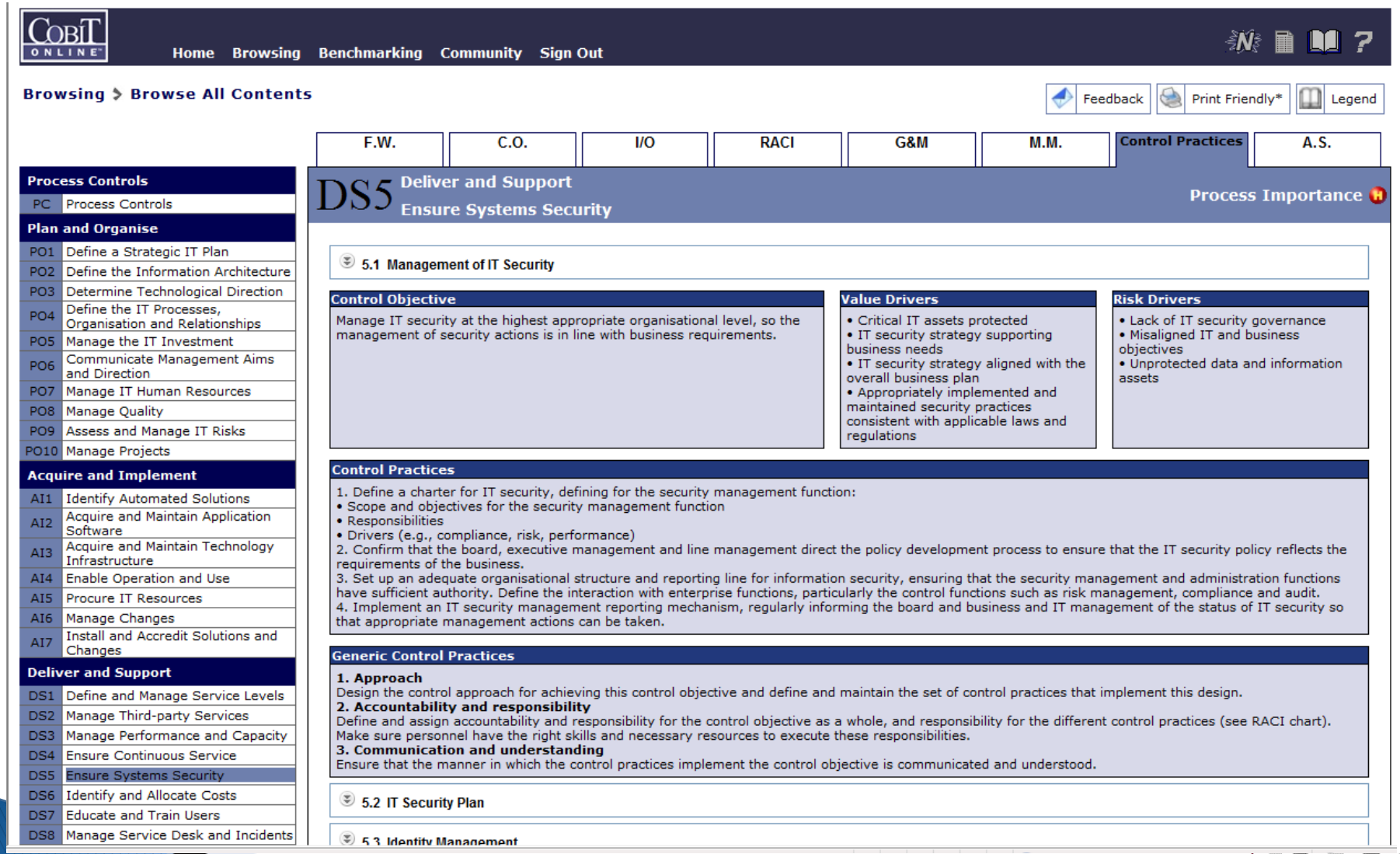
Legend for rankings used

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 - Best practices are followed and automated

Control Practices



Control Practices – DS5.1



Control Practices 5.7

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
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
Application Controls	
AC	Application Controls

5.3 Identity Management

5.4 User Account Management

5.5 Security Testing, Surveillance and Monitoring

5.6 Security Incident Definition

5.7 Protection of Security Technology

Control Objective	Value Drivers	Risk Drivers
Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	• Corporate security technology protected • Reliable information secured • Corporate assets protected	• Exposure of information • Breach of trust with other organisations • Violations of legal and regulatory requirements

Control Practices

1. Ensure that all hardware, software and facilities related to the security function and controls, e.g., security tokens and encryptors, are tamperproof.
2. Secure security documentation and specifications to prevent unauthorised access. However, do not make security of systems reliant solely on secrecy of security specifications.
3. Make the security design of dedicated security technology (e.g., encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorised individuals.
4. Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

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.
2. Accountability and responsibility
Define and assign accountability and responsibility for the control objective as a whole, and responsibility for the different control practices (see RACI chart). Make sure personnel have the right skills and necessary resources to execute these responsibilities.
3. Communication and understanding
Ensure that the manner in which the control practices implement the control objective is communicated and understood.

5.8 Cryptographic Key Management

5.9 Malicious Software Prevention, Detection and Correction

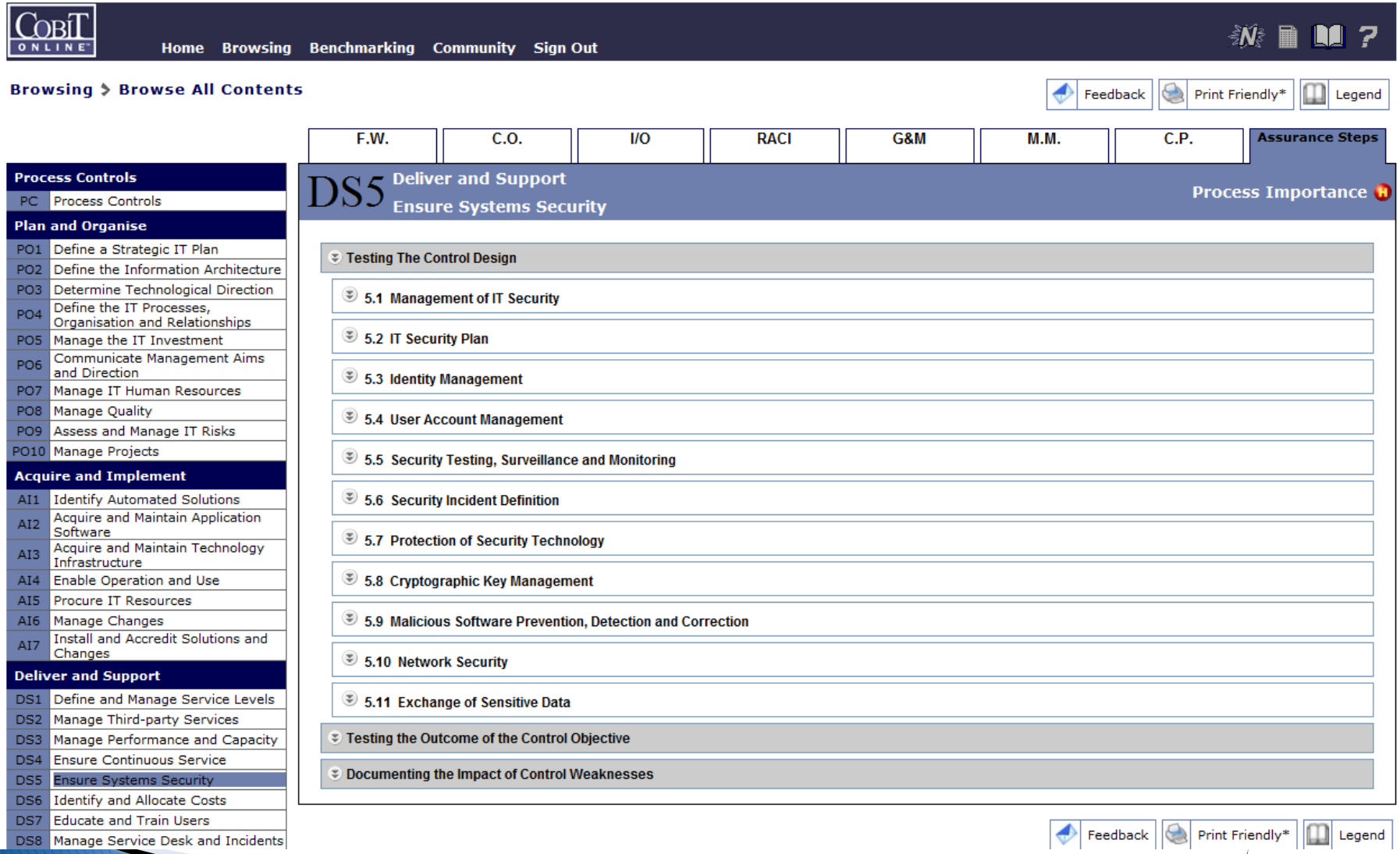
5.10 Network Security

5.11 Exchange of Sensitive Data

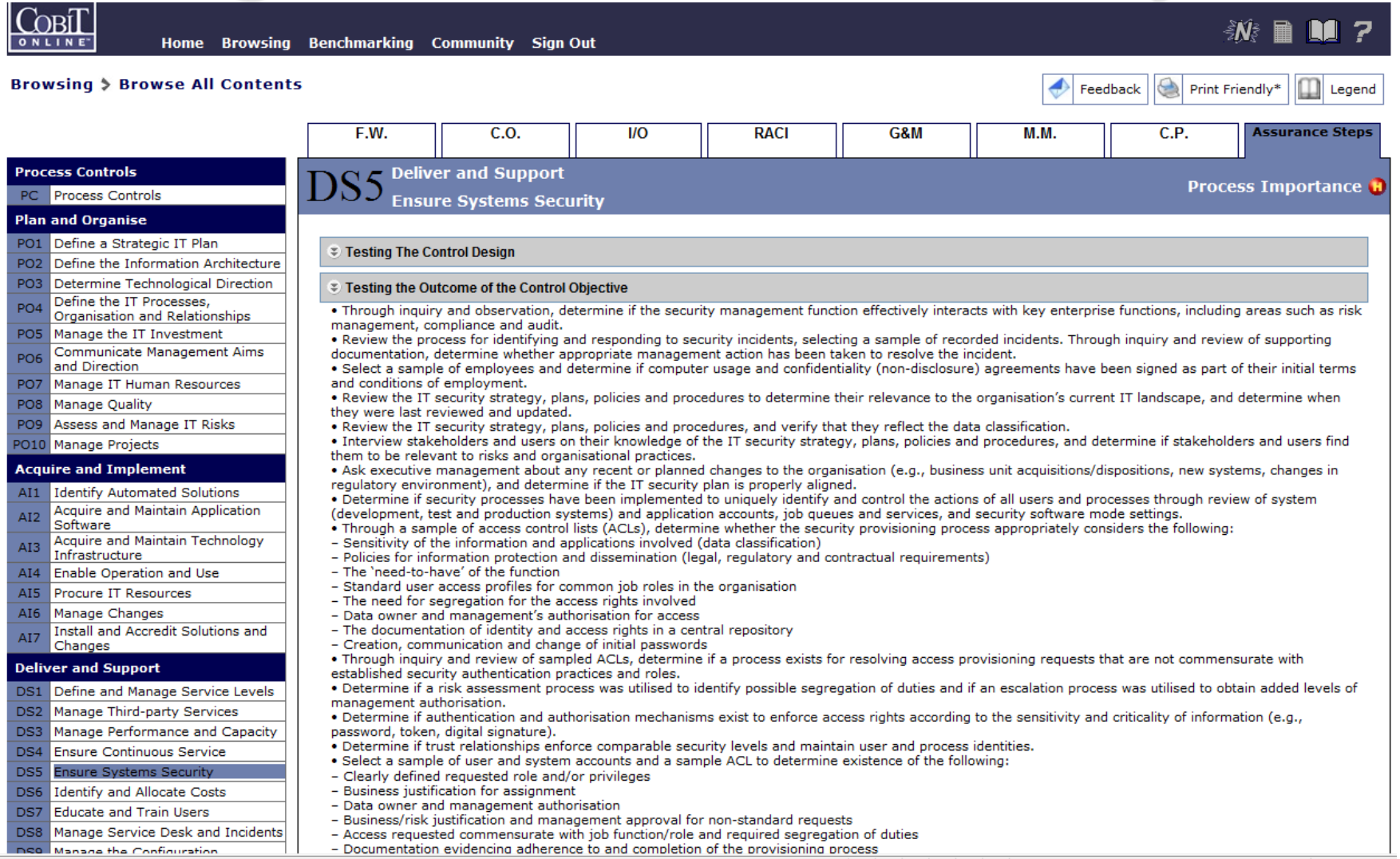
Feedback | Print Friendly* | Legend

* Consider changing the page setup to landscape (in your browser) when printing this page.

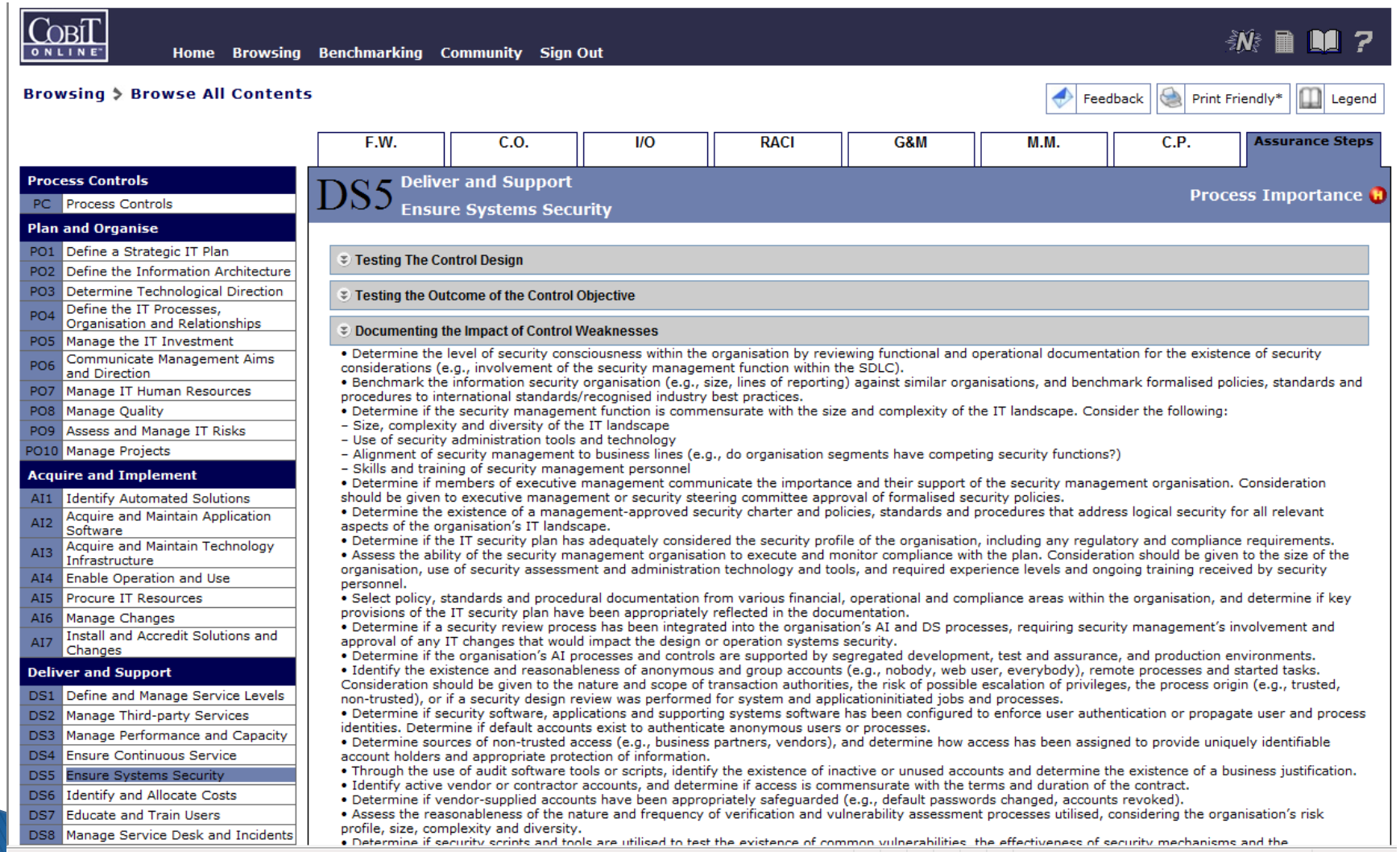
Assurance Steps



Testing the Outcome of Control Objective



Documenting the Impact of Control Weaknesses



COBIT ONLINE

Home | Browsing | Benchmarking | Community | Sign Out

Browsing > Browse All Contents

Feedback | Print Friendly* | Legend

F.W. | C.O. | I/O | RACI | G&M | M.M. | C.P. | Assurance Steps

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
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents

DS5 Deliver and Support
Ensure Systems Security

Process Importance

Testing The Control Design

Testing the Outcome of the Control Objective

Documenting the Impact of Control Weaknesses

- Determine the level of security consciousness within the organisation by reviewing functional and operational documentation for the existence of security considerations (e.g., involvement of the security management function within the SDLC).
- Benchmark the information security organisation (e.g., size, lines of reporting) against similar organisations, and benchmark formalised policies, standards and procedures to international standards/recognised industry best practices.
- Determine if the security management function is commensurate with the size and complexity of the IT landscape. Consider the following:
  - Size, complexity and diversity of the IT landscape
  - Use of security administration tools and technology
  - Alignment of security management to business lines (e.g., do organisation segments have competing security functions?)
  - Skills and training of security management personnel
- Determine if members of executive management communicate the importance and their support of the security management organisation. Consideration should be given to executive management or security steering committee approval of formalised security policies.
- Determine the existence of a management-approved security charter and policies, standards and procedures that address logical security for all relevant aspects of the organisation's IT landscape.
- Determine if the IT security plan has adequately considered the security profile of the organisation, including any regulatory and compliance requirements.
- Assess the ability of the security management organisation to execute and monitor compliance with the plan. Consideration should be given to the size of the organisation, use of security assessment and administration technology and tools, and required experience levels and ongoing training received by security personnel.
- Select policy, standards and procedural documentation from various financial, operational and compliance areas within the organisation, and determine if key provisions of the IT security plan have been appropriately reflected in the documentation.
- Determine if a security review process has been integrated into the organisation's AI and DS processes, requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security.
- Determine if the organisation's AI processes and controls are supported by segregated development, test and assurance, and production environments.
- Identify the existence and reasonableness of anonymous and group accounts (e.g., nobody, web user, everybody), remote processes and started tasks. Consideration should be given to the nature and scope of transaction authorities, the risk of possible escalation of privileges, the process origin (e.g., trusted, non-trusted), or if a security design review was performed for system and applicationinitiated jobs and processes.
- Determine if security software, applications and supporting systems software has been configured to enforce user authentication or propagate user and process identities. Determine if default accounts exist to authenticate anonymous users or processes.
- Determine sources of non-trusted access (e.g., business partners, vendors), and determine how access has been assigned to provide uniquely identifiable account holders and appropriate protection of information.
- Through the use of audit software tools or scripts, identify the existence of inactive or unused accounts and determine the existence of a business justification.
- Identify active vendor or contractor accounts, and determine if access is commensurate with the terms and duration of the contract.
- Determine if vendor-supplied accounts have been appropriately safeguarded (e.g., default passwords changed, accounts revoked).
- Assess the reasonableness of the nature and frequency of verification and vulnerability assessment processes utilised, considering the organisation's risk profile, size, complexity and diversity.
- Determine if security scripts and tools are utilised to test the existence of common vulnerabilities, the effectiveness of security mechanisms and the

Linking Business Goals To IT Goals

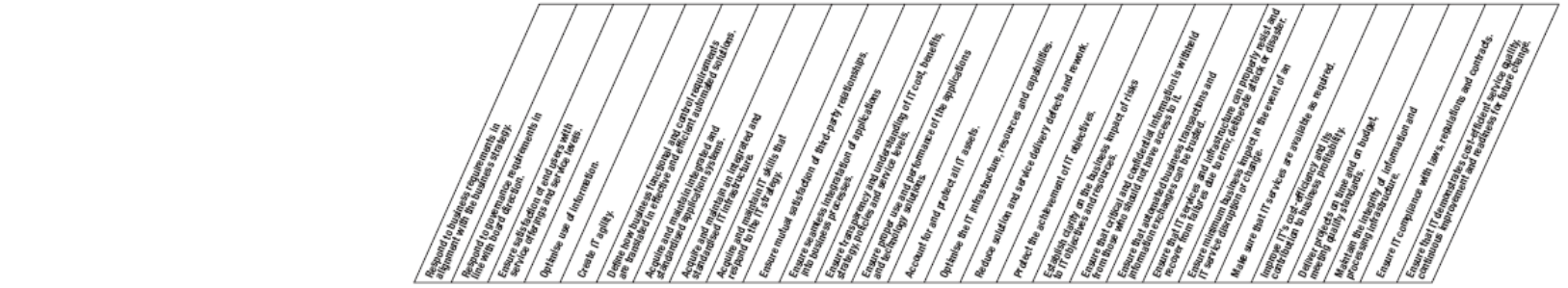
		Business Goals	IT Goals							
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24							
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22
	3	Improve corporate governance and transparency.	2	18						
Customer Perspective	4	Improve customer orientation and service.	3	23						
	5	Offer competitive products and services.	5	24						
	6	Establish service continuity and availability.	10	16	22	23				
	7	Create agility in responding to changing business requirements.	1	5	25					
	8	Achieve cost optimisation of service delivery.	7	8	10	24				
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26			
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11					
	11	Lower process costs.	7	8	13	15	24			
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27	
	13	Provide compliance with internal policies.	2	13						
	14	Manage business change.	1	5	6	11	28			
	15	Improve and maintain operational and staff productivity.	7	8	11	13				
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28					
	17	Acquire and maintain skilled and motivated people.	9							

Linking IT Goals to IT Processes

LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes										CobiT Information Criteria						
												Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4						P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimise the use of information.	PO2	DS11										S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3							P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6								P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5								P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5									S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5									P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2										P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7								P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8						P	S					
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9						S	P					
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Protect the achievement of IT objectives.	PO9	DS10	ME2								P	P	S	S	S	S	S
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9										S	S	P	P	P	S	S
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12									P	P	S	S	S
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5								P			P	S	S	
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12							P	S		S	P		
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13							P	P			P		
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6									S	P					S
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10									P	P		S			S
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5									P	P		P	P		S
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4									S	S		P	S
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4							P	P					P

IT Process to IT Goals Matrix



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
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.			✔										✔		✔													
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.		✔										✔															✔	✔

ISACA® Serving IT Governance Professionals
San Francisco Chapter

CobiT 4.x Release

- Detailed control objectives now covers IT governance more completely, better harmonized and more concise (About 30% few controls). Reduced from 320 (CobiT 3.0) to 215 (CobiT 4.0)
- Generic process-related control objectives moved to the *Framework* as part of Process Goals/Objectives
  - Goals and objectives
  - Ownership
  - Repeatability
  - Roles and Responsibility
  - Policy, Plans and Procedures
  - Process Performance Improvement
- Application controls moved into the *Framework* section from Delivery & Support

COBIT 4.1 Update

- Enhanced *Executive Overview* section

  Very minor changes

- Explanation of goals and metrics in the *Framework* section

  Minor, mostly rearrangement for presentation and additional clarification

- Better definitions of the core concepts. It is important to mention that the definition of a control objective changed, shifting more toward a management practice statement.

  This has been true since CobiT 3.0 to 4.0 update. Progressive verbiage changes were made for clarification or generalizing purposes.

COBIT 4.1 Update (Cont'd)

- Improved control objectives resulting from updated control practices and Val IT development activity. Some control objectives were grouped and/or reworded to avoid overlaps and make the list of control objectives within a process more consistent. Specific revisions include:
  - AI5.5 and AI5.6 were combined with AI5.4

    Software Acquisition + Acquisition of Development Resources + Acquisition of Infrastructure, Facilities, and Related Services = IT Resources Acquisition
  - AI7.9, AI7.10 and AI7.11 were combined with AI7.8

    Software Release + System Distribution + Recording and Tracking of Changes = Promotion to Production
  - ME3 was revised to include compliance with contractual requirements in addition to legal and regulatory requirements

    ME3 = Ensure Compliance With External Requirements.
    More generic with details moved to Control Practices

COBIT 4.1 Update (Cont'd)

- Application controls have been reworked to be more effective, based on work to support controls effectiveness assessment and reporting. 6 application controls replaced the 18 application controls in COBIT 4.0, with further detail provided in COBIT Control Practices, 2nd Edition.
- The list of business goals and IT goals in Appendix I was improved, based on new insights obtained during validation research executed by the University of Antwerp Management School (Belgium).
- The pull-out has been expanded to provide a quick reference list of the COBIT processes, and the overview diagram depicting the domains has been revised to include reference to the process and application control elements of the COBIT framework.
- Improvements identified by COBIT users (COBIT 4.0 and COBIT Online) have been reviewed and incorporated as appropriate.

Impact on Users: CobiT 3.x to 4.0 Update

- CobiT 4.0 is an evolution from the 3rd edition based on the same core principals and structure – no need to "throw away" current work
- CobiT 4.0 build on and extends 3rd edition with stronger business focus and governance practices
- The metrics build on the same principles, are integrated with goals and provide more and better examples to help users design their own
- Full x-references provided in appendices showing how processes and control objectives map in both directions to help conversions

Impact on Users: CobiT 3.x to 4.0 Update

- Still 4 Domains and 34 Processes
- An incremental update to CobiT 4.0
- IT Assurance Guide and CobiT Control Practices were updated with CobiT 4.1

COBIT Campus

With the growing adoption of COBIT, ISACA recognized the need for structured and formal education and worked together with *ITpreneurs* to develop authentic COBIT learning solutions. COBIT training courses help professionals master COBIT and utilize this knowledge for effective implementation within their organizations. Sustainable COBIT competencies help IT organizations and departments align with the goals and objectives of the business and generate strategic value from IT.

The COBIT curriculum includes the following courses:

- COBIT Awareness Course (2 hours, self paced e-learning)
- COBIT Foundation Course (8 hours, self paced e-learning or 14 hours, classroom)
- COBIT Foundation Exam (1 hour, online 40 questions)
- IT Governance Implementation Course (14 hours, classroom)
- COBIT for Sarbanes-Oxley Compliance (5 hours, self paced e-learning)

Continued Efforts

- What other opportunities are there for broader adoption and application?
- How can we support membership in adoption, implementation and sustainable usage?
- Act as a conduit to the CobiT Steering Committee to communicate membership needs - What needs to change in CobiT? Influence CobiT 5.0
- What additional guidance is needed for adopters?
- What training is needed? CPEs for upcoming IT Governance Certification
- How can CobiT work better with other standards and frameworks? (additional mapping projects)
- Stay connected with other CobiT User Groups (Atlanta, Toronto etc.) learn from each other
- Develop CobiT page on chapter website to provide CobiT resources.

FFIEC Mapping Projects

Common FFIEC Index

FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2
1.1.0.0	Audit	Introduction		
1.2.0.0	Audit	IT Audit Roles and Responsibilities		
1.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management	
1.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management	
1.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff	
1.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management	
1.2.5.0	Audit	IT Audit Roles and Responsibilities	External Auditors	
1.3.0.0	Audit	Independence Staffing of Internal IT Audit		
1.3.1.0	Audit	Independence Staffing of Internal IT Audit	Independence	
1.3.2.0	Audit	Independence Staffing of Internal IT Audit	Staffing	
1.4.0.0	Audit	Internal Audit Program		

COBIT to FFIEC

Process #	Process Description	CO	COBIT Control Objective	Coverage	FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	9.3.4.1	Outsourcing Technology Services	Risk Management	Ongoing Monitoring	Key Service Level Agreements and Contract Provisions
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	9.3.3.0	Outsourcing Technology Services	Risk Management	Contract Issues	
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	4.3.2.2	E-Banking	Risk Management of E-Banking Activities	Managing Outsourcing Relationships	Contracts for Third-Party Services
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	10.4.6.4	Retail Payment Systems	Retail Payment System Risk Management	Operational (Transaction) Risk	Vendor and Third Party Management
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	12.5.6.5	Wholesale Payment Systems	Wholesale Payment Systems Risk Management	Operational (Transaction) Risk	Vendor and Third-Party Management
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	7.5.0.2	Management	Management Considerations for Technology Service Providers		Contracts
DS1	Define and manage service levels.	DS1.2	Definition of services	A	9.3.4.1	Outsourcing Technology Services	Risk Management	Ongoing Monitoring	Key Service Level Agreements and Contract Provisions

FFIEC to COBIT

FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2	COBIT #	COBIT Control Objective	Coverage
1.1.0.0	Audit	Introduction			PO6.2	Enterprise IT Risk and Control Framework	A
1.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		ME1.1	Monitoring approach	A
1.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.2	IT Strategy Committee	A
1.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.3	IT Steering Committee	A
1.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.8	Responsibility for Risk, Security and Compliance	A
1.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		ME2.2	Supervisory review	A
1.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		ME4.7	Independent assurance	A
1.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		PO4.8	Responsibility for Risk, Security and Compliance	A
1.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		PO7.4	Personnel Training	A
1.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff		ME4.7	Independent assurance	A
1.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff		PO4.8	Responsibility for Risk, Security and Compliance	A
1.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME2.7	Remedial actions	C
1.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME3.4	Positive assurance of compliance	A
1.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME4.7	Independent assurance	A

COBIT Mapping Documents

CobiT® Mapping Documents

No Login Required: Login Required: Member Only:

- COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1 July 2008
- COBIT Mapping: Mapping of NIST SP800-53 Rev 1 With COBIT 4.1 November 2007
- COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0 June 2007
- COBIT Mapping: Mapping of CMMI® for Development V1.2 With COBIT 4.0 March 2007
- COBIT Mapping: Mapping of ITIL With COBIT 4.0 January 2007
- COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0 January 2007
- COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0 December 2006
- COBIT Mapping: Mapping PMBOK to COBIT 4.0 August 2006
- COBIT Mapping: Mapping SEI's CMM for Software to COBIT 4.0 August 2006
- COBIT Mapping to ISO/IEC 17799 :2000 With COBIT, 2nd Edition May 2006
- COBIT Mapping Overview of International IT Guidance 2nd Edition April 2006
- Aligning COBIT, ITIL and ISO 17799 for Business Benefit November 2005

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Governance Certification

CGEIT - Certified in the Governance of Enterprise IT

- Promoted in the last Expressline and CobiT Focus newsletter.
- CobiT is a key reference in forming the foundation of this certification
- Take advantage of ITPrenuers chapter offering of CobiT education courses (reduced pricing).
- Initial exam is targeted for December 2008 (grandfathering will also be available)

CGEIT Grandfathering

- ISACA/ITGI is not accepting grandfathering applications at this time, but plan to do so in the future. Additional information and details will be posted at a future date when this provision is active. The following is being provided to give you a general sense of this provision.
- Highly experienced professionals who have had a significant management, advisory and/or assurance role relating to the governance of IT will be allowed to apply for CGEIT certification without being required to pass the CGEIT examination.
- To earn the CGEIT certification during this grandfathering period, an applicant must:
- Have and submit evidence of eight (8) years of experience associated with the governance of the IT-related contribution to an enterprise, with a minimum of three (3) of these years performing tasks directly related to any two or more of the aforementioned CGEIT domains.
- Describe (200-500 words) their experience managing, providing advisory and/or assurance services, and/or otherwise supporting the governance of an enterprise's information technology.
- Adhere to the ISACA Code of Professional Ethics
- Agree to comply with the CGEIT Continuing Education Policy
- Pay an application fee:
  - US $595—for ISACA members
  - US $660—for non-ISACA member credential holders in good standing
  - US $725—for all others

Biography

Miguel (Mike) O. Villegas is the Chief Information Security Officer of Newegg, Inc. and is responsible for Information Security, IT Risk Management and PCI DSS (Payment Card Industry Data Security Standard) compliance. Newegg, Inc. is one of the fastest growing E-Commerce companies established in 2001 with an expected $2 Billion in revenue in 2008.

Mike has over 25 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Ernst & Young, LLP and Arthur Andersen over their information systems security and audit groups over a span of nine years. Mike is a CISA and CISSP.

He was the SF ISACA Chapter President during 2005-2006 and the SF Fall Conference Co-Chair from 2002–2007. He also served for two years as Vice President on the Board of Directors for ISACA International. Currently, Mike is involved with the LA ISACA Spring Conference Committee and is the CISA Review Course Coordinator.

Thank You!

Questions?

Miguel (Mike) O. Villegas, CISA, CISSP
(626) 353-2056
Mike.o.villegas@newegg.com