ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Leveraging COBIT® for More Effective Audits

Strategies and Techniques

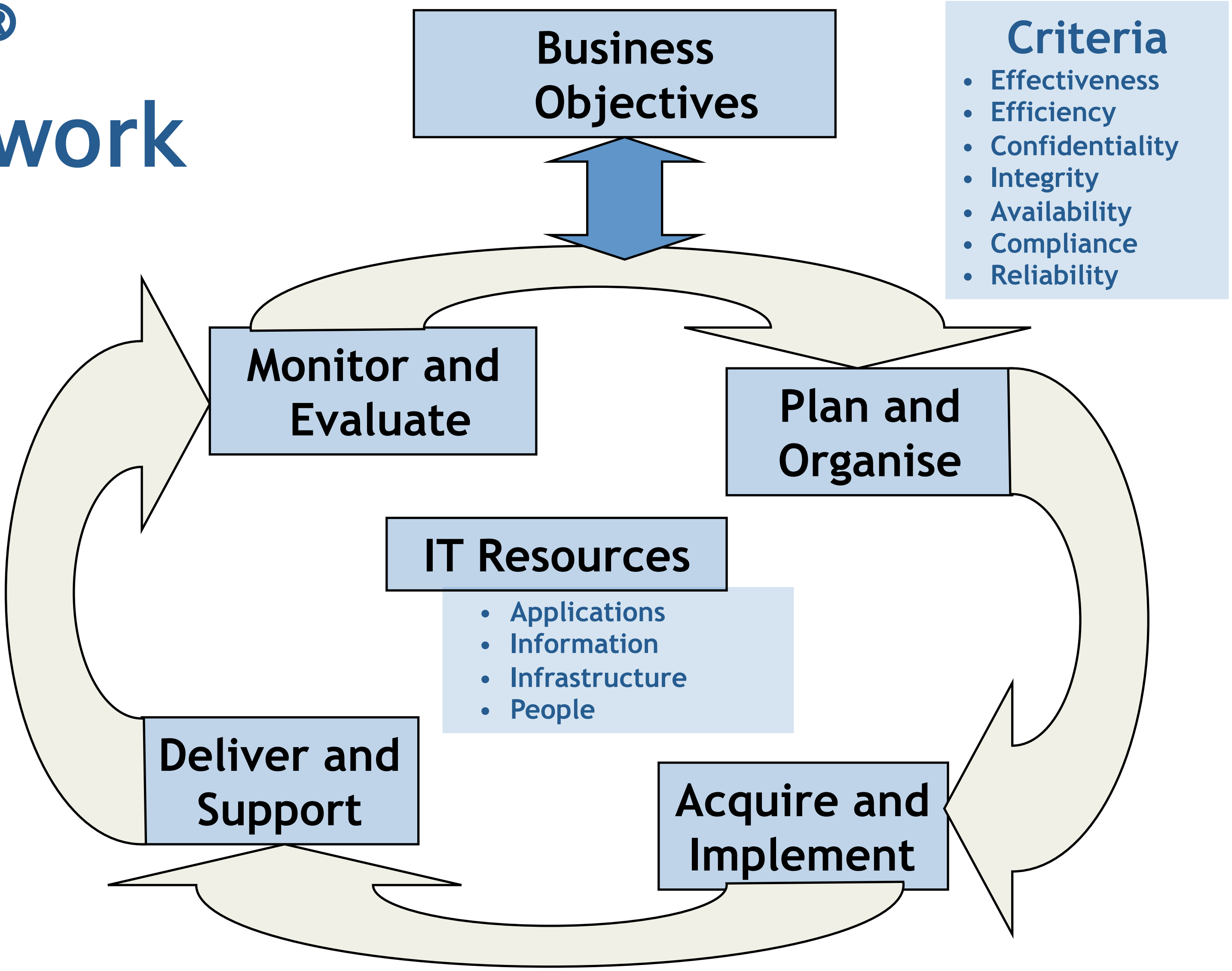
Session ST11

Session Outline

- Leveraging COBIT®
  - COBIT® and Related Products
  - Framework, Processes and Navigation
- Better Audits with Process Focus
  - Process Definition & Controls
  - Lean
  - Six Sigma Methods
- Better Audits with COBIT®
  - IT Assurance Guide
  - Planning
  - Executing
  - Customer Focused Reports and Communications

Leveraging COBIT®

COBIT® Framework



Business Objectives

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

Monitor and Evaluate

Plan and Organise

IT Resources
- Applications
- Information
- Infrastructure
- People

Deliver and Support

Acquire and Implement

COBIT® Processes

Plan and Organise

PO1	Define an IT Strategic 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

COBIT® Processes

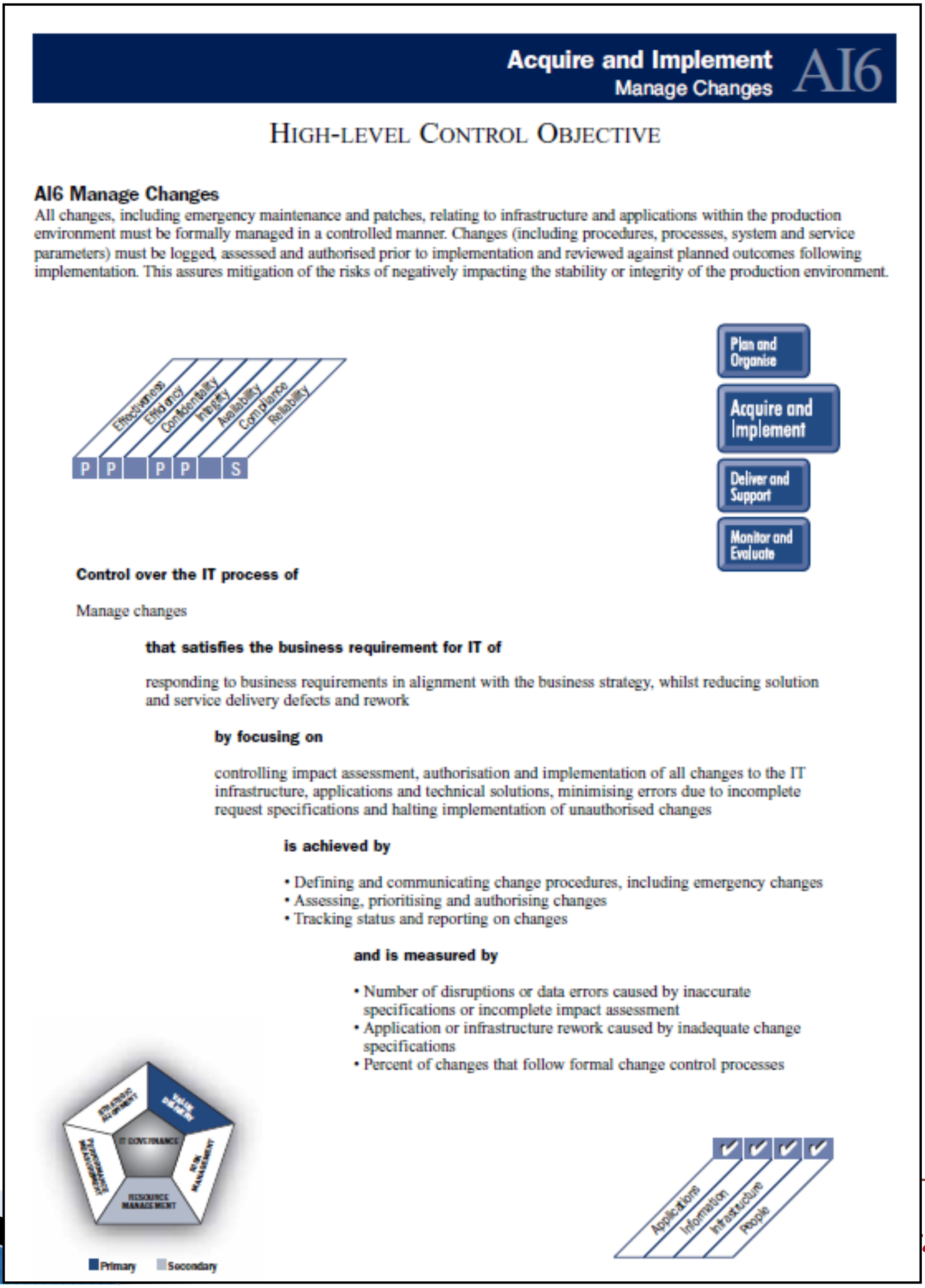
Deliver and Support

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

Process –level Navigating in COBIT®



Acquire and Implement
Manage Changes
AI6

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

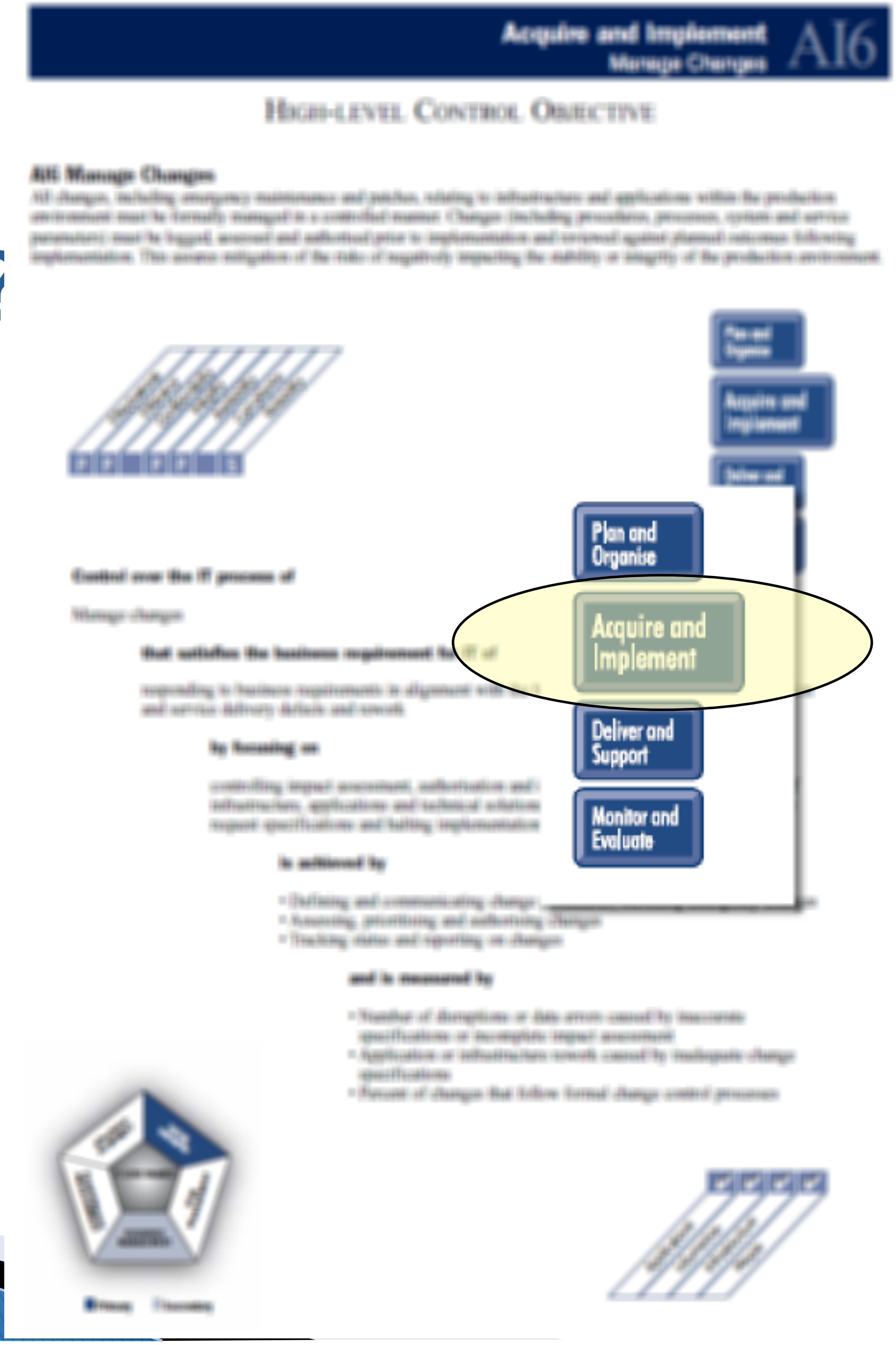
is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

Which Domain?



Acquire and Implement
Manage Changes
AI6

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the b
and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and i
infrastructure, applications and technical solution
request specifications and halting implementation

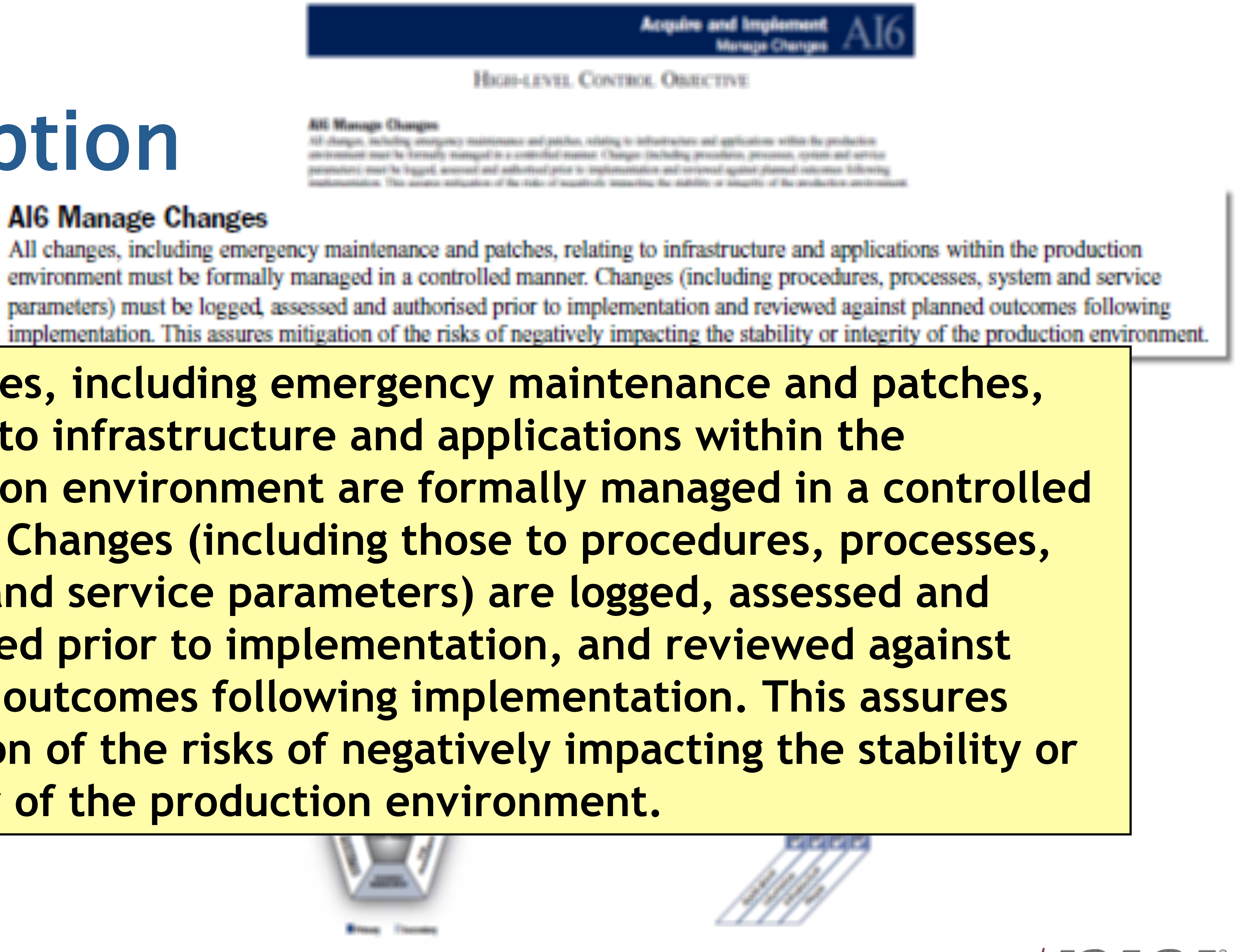
is achieved by

- Defining and communicating change
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

Process Description



Acquire and Implement
Manage Changes
AI6

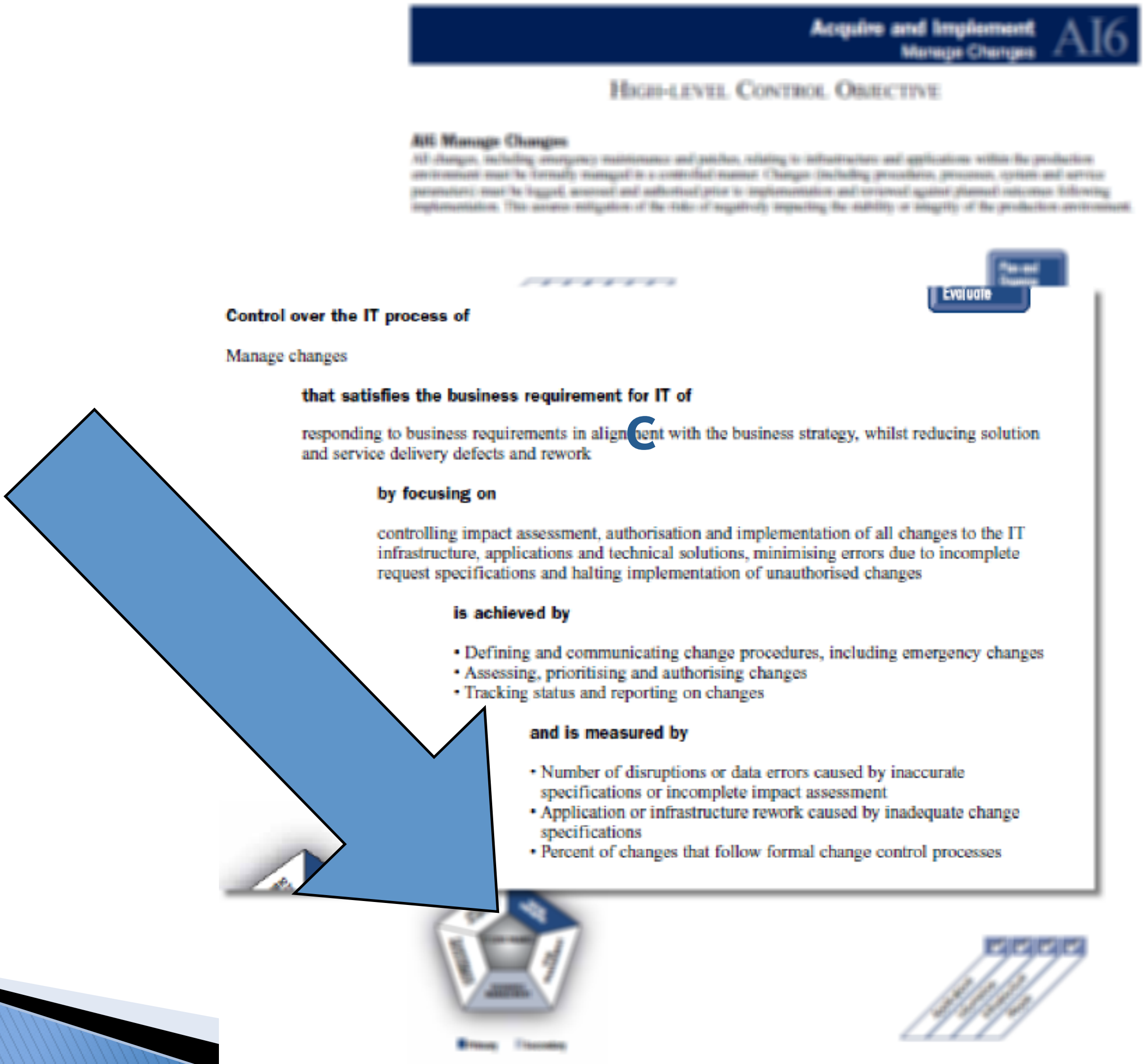
HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation, and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

The Waterfall of Control



Acquire and Implement
Manage Changes
AI6

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes
All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

is achieved by

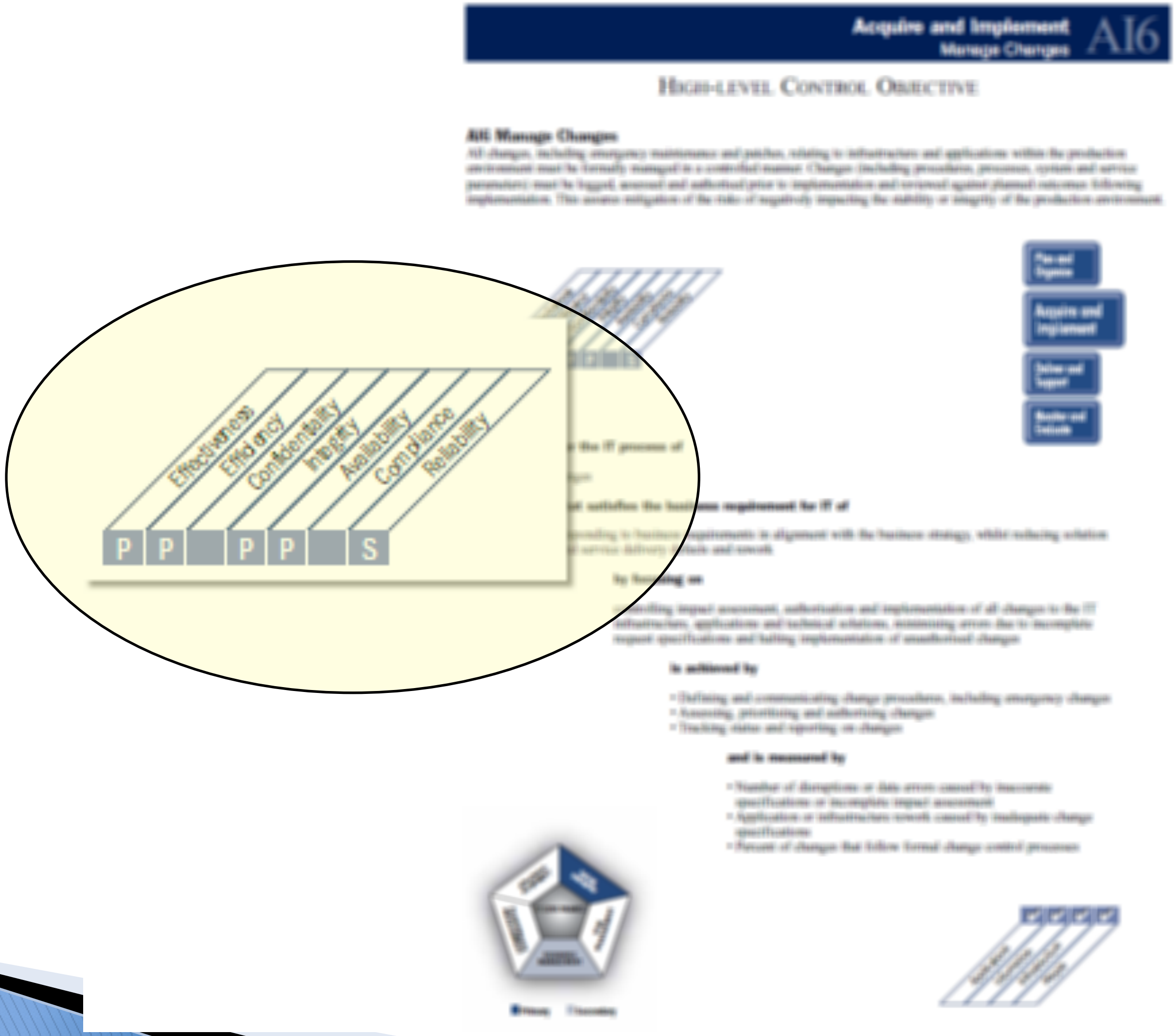
- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Information Criteria



ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Resources

Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate
Applications
Information
Infrastructure
People

Acquire and Implement
Manage Changes
AI6

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes
All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

is achieved by

• Defining and communicating change procedures, including emergency changes

IT Governance

Acquire and Implement
Manage Changes
AI6

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

is achieved by

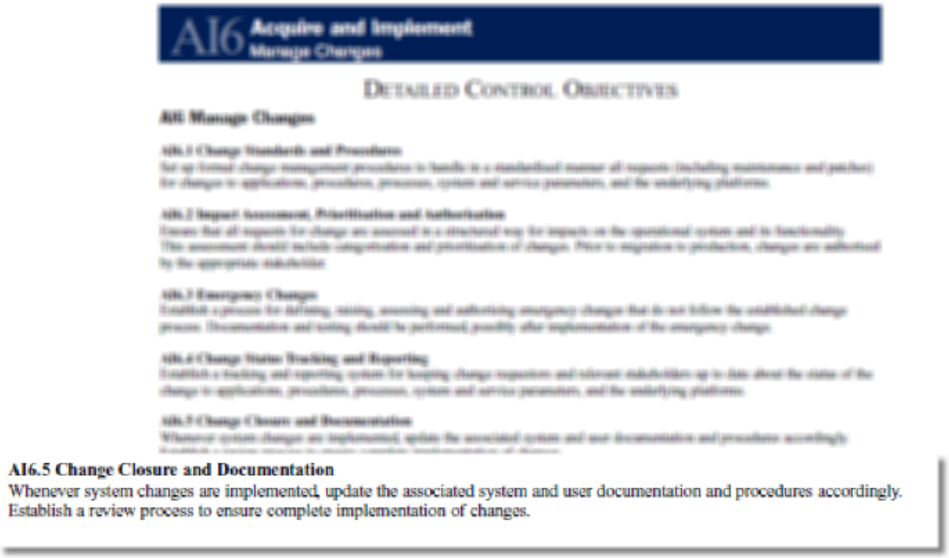
- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Control Objectives



AI6 Acquire and Implement
Manage Changes

DETAILED CONTROL OBJECTIVES

AI6 Manage Changes

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritisation and Authorisation
Ensure that all requests for change are assessed in a structured way for impacts on the operational system and its functionality. This assessment should include categorisation and prioritisation of changes. Prior to migration to production, changes are authorised by the appropriate stakeholder.

AI6.3 Emergency Changes
Establish a process for defining, raising, assessing and authorising emergency changes that do not follow the established change process. Documentation and testing should be performed, possibly after implementation of the emergency change.

AI6.4 Change Status Tracking and Reporting
Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.5 Change Closure and Documentation
Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly.

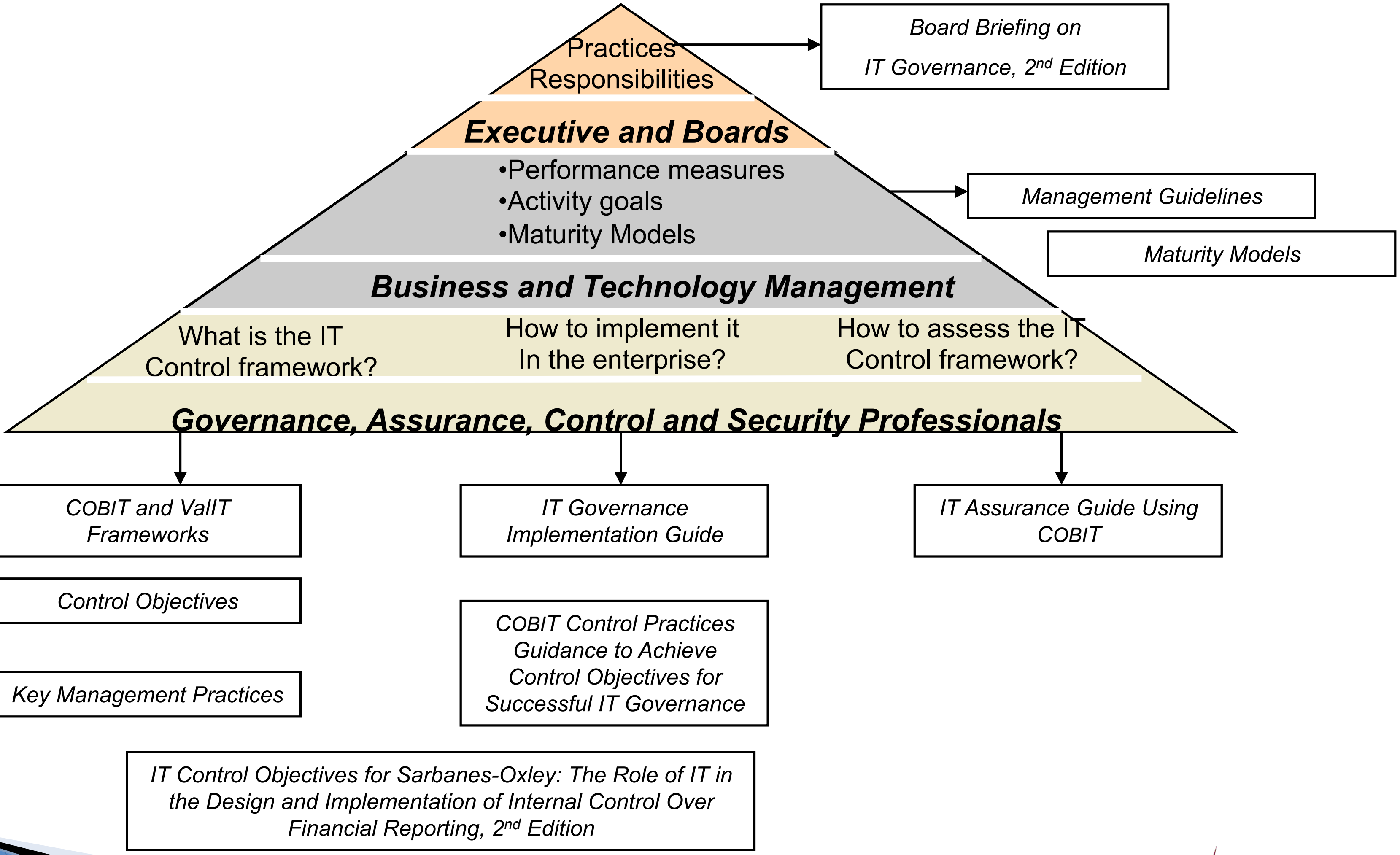
AI6.5 Change Closure and Documentation
Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.

AI6.5 Change Closure and Documentation

Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

Serving IT Governance Professionals
San Francisco Chapter

COBIT® and Related Products



Practices
Responsibilities

Executive and Boards

- Performance measures
- Activity goals
- Maturity Models

Business and Technology Management

What is the IT Control framework?

How to implement it In the enterprise?

How to assess the IT Control framework?

Governance, Assurance, Control and Security Professionals

Board Briefing on IT Governance, 2nd Edition

Management Guidelines

Maturity Models

COBIT and ValIT Frameworks

Control Objectives

Key Management Practices

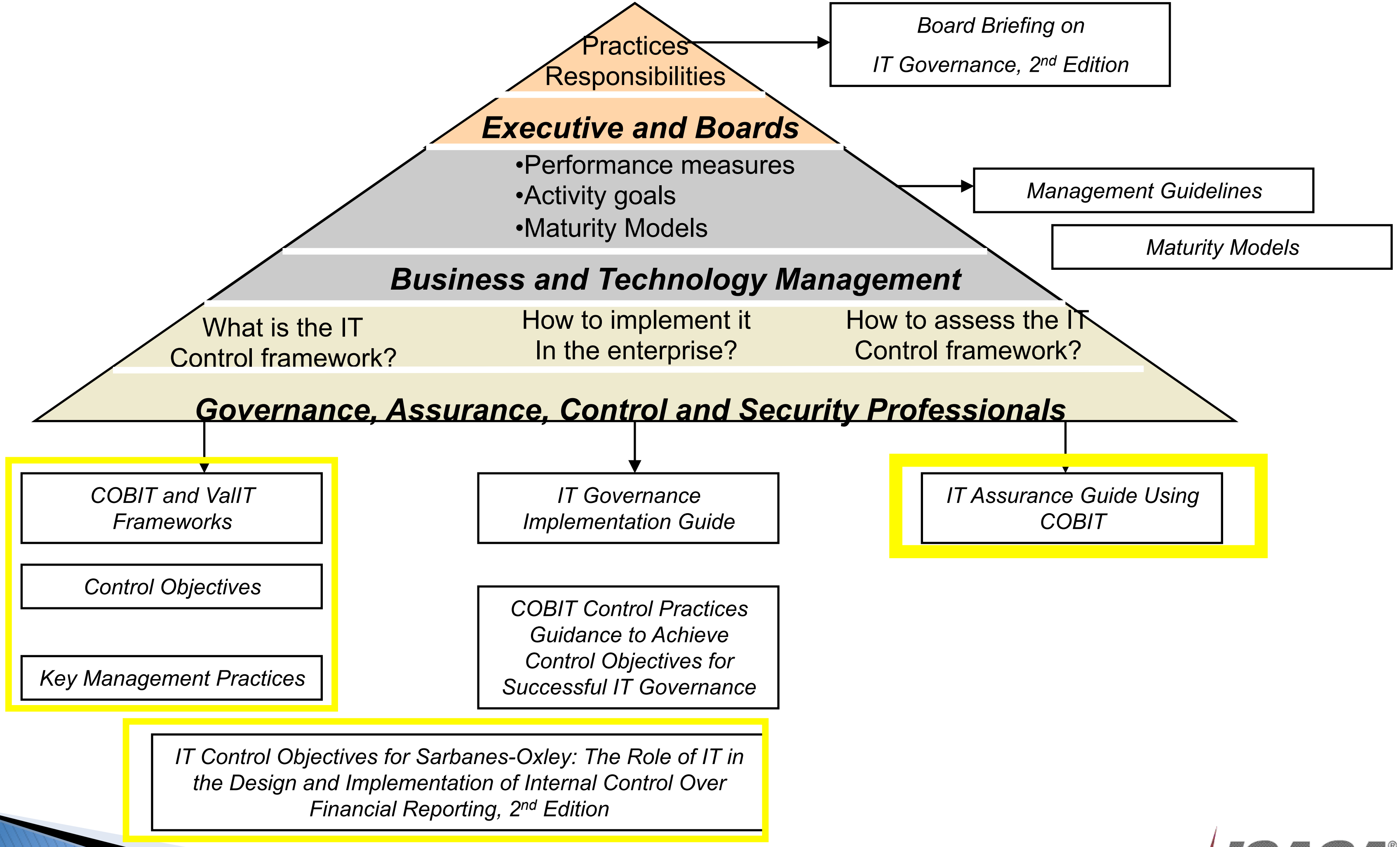
IT Governance Implementation Guide

COBIT Control Practices Guidance to Achieve Control Objectives for Successful IT Governance

IT Assurance Guide Using COBIT

IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition

COBIT® and Related Products of interest to the IT Auditor



Practices
Responsibilities

Executive and Boards

- Performance measures
- Activity goals
- Maturity Models

Business and Technology Management

What is the IT
Control framework?

How to implement it
In the enterprise?

How to assess the IT
Control framework?

Governance, Assurance, Control and Security Professionals

Board Briefing on IT Governance, 2nd Edition

Management Guidelines

Maturity Models

COBIT and ValIT Frameworks

Control Objectives

Key Management Practices

IT Governance Implementation Guide

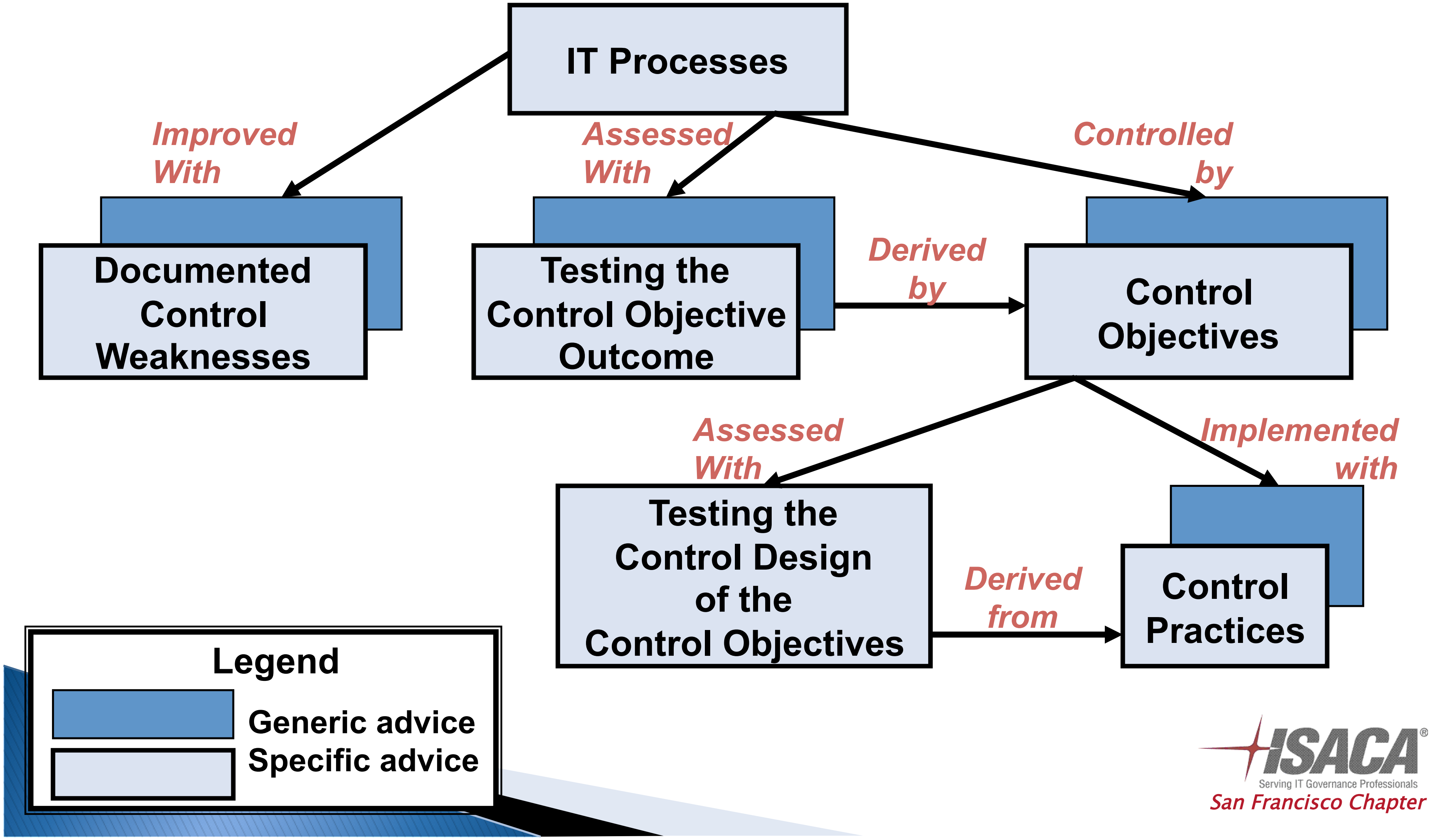
COBIT Control Practices Guidance to Achieve Control Objectives for Successful IT Governance

IT Assurance Guide Using COBIT

IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IT Assurance Guide Advice



IT Processes

Improved With

Documented Control Weaknesses

Assessed With

Testing the Control Objective Outcome

Controlled by

Control Objectives

Derived by

Assessed With

Testing the Control Design of the Control Objectives

Implemented with

Control Practices

Derived from

Legend

🟦 Generic advice

□ Specific advice

ISACA®

Serving IT Governance Professionals

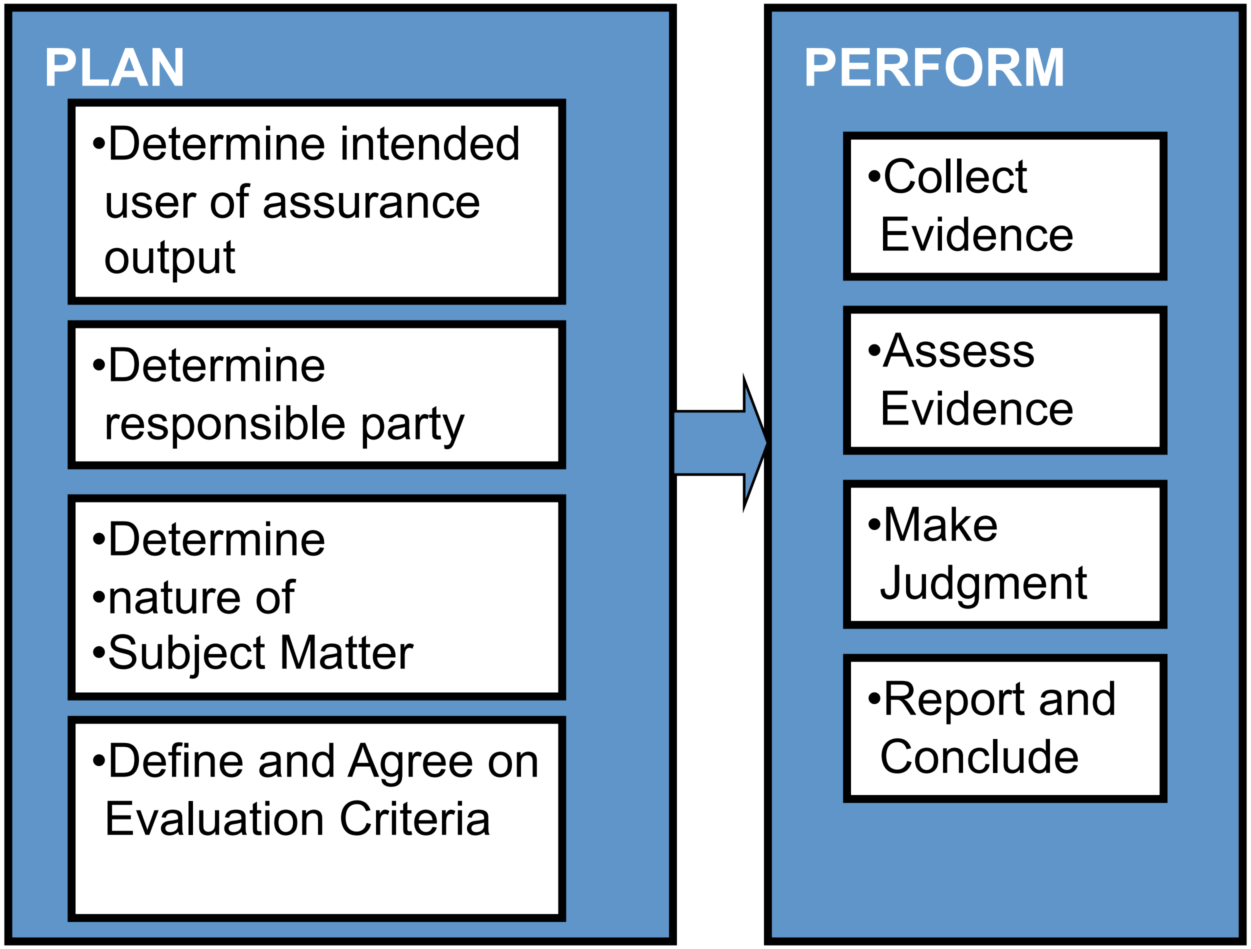
San Francisco Chapter

Better Audits with Process Focus

Serving IT Governance Professionals

San Francisco Chapter

How we do audits*



PLAN

- Determine intended user of assurance output
- Determine responsible party
- Determine
- nature of
- Subject Matter
- Define and Agree on Evaluation Criteria

PERFORM

- Collect Evidence
- Assess Evidence
- Make Judgment
- Report and Conclude

Source: IAASB from IT Assurance Guide Intro

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

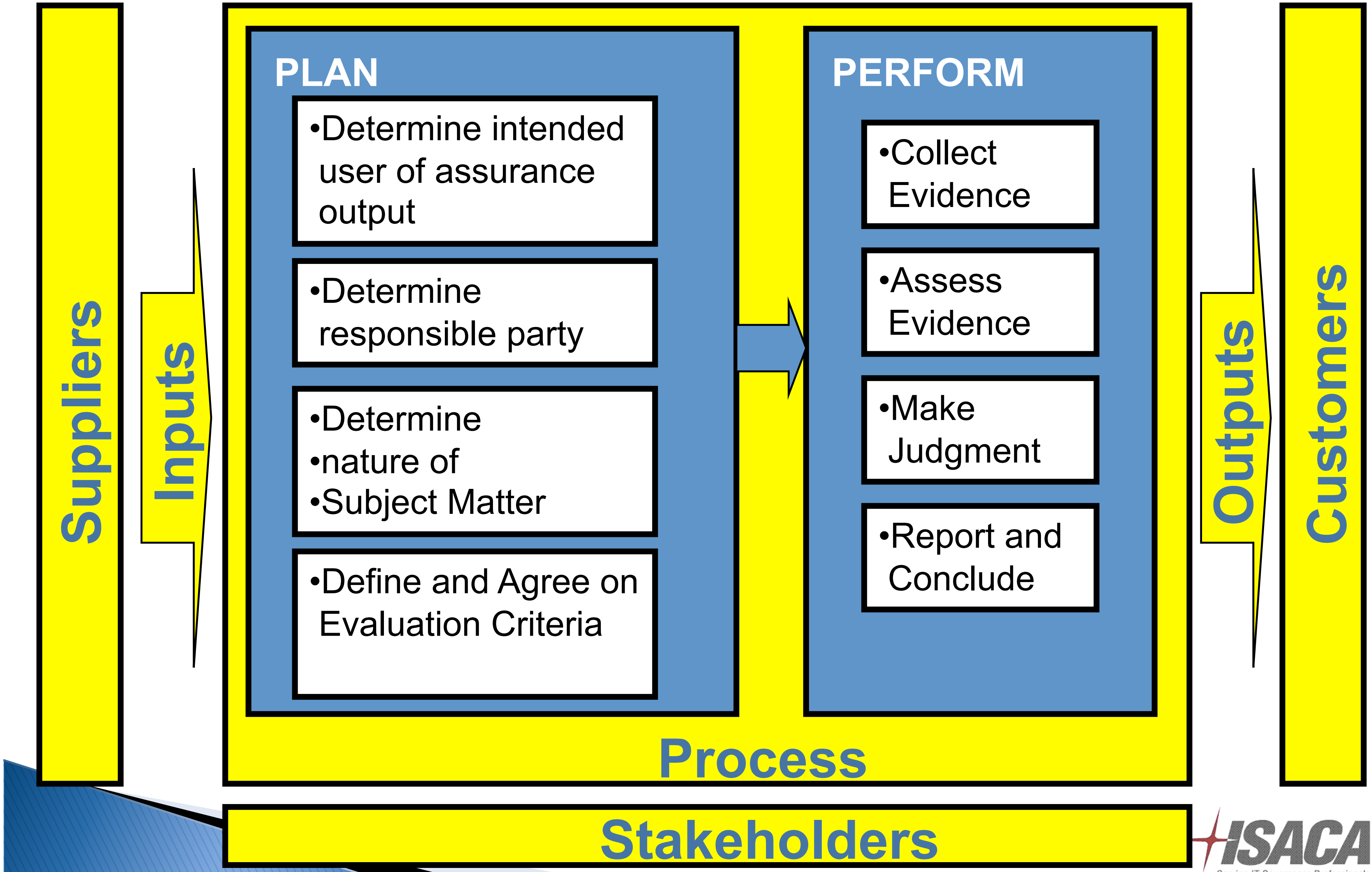
Reason for defining how we do audits as a process:

- **So we know what we are doing**
  - A defined process is repeatable and more consistently produces the expected results with less likelihood of errors.
- **Value Drivers:**
  - Increased efficiency and effectiveness
  - Ease of process maintenance
  - Ability to demonstrate process effectiveness to external auditors and regulators
  - Alignment with overall IT organization goals
- **Risk Drivers**
  - High reliance on process specialists
  - Processes unable to react to problems and new requirements.

Steps to Define the Audit Process

- Identify Process S-I-P-O-C
  - Suppliers & Inputs
  - Outputs & Customers
  - Process Flow: Activities & Role/Responsibilities
- Evaluate the Process for
  - Control
  - Customer’s Value
  - Business Management Value
- Identify gaps & correct.
- Execute, Learn, Improve, Repeat

Audit Process as S-I-P-O-C



Suppliers

Inputs

PLAN

- Determine intended user of assurance output
- Determine responsible party
- Determine
- nature of
- Subject Matter
- Define and Agree on Evaluation Criteria

PERFORM

- Collect Evidence
- Assess Evidence
- Make Judgment
- Report and Conclude

Process

Outputs

Customers

Stakeholders

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Suppliers & Inputs

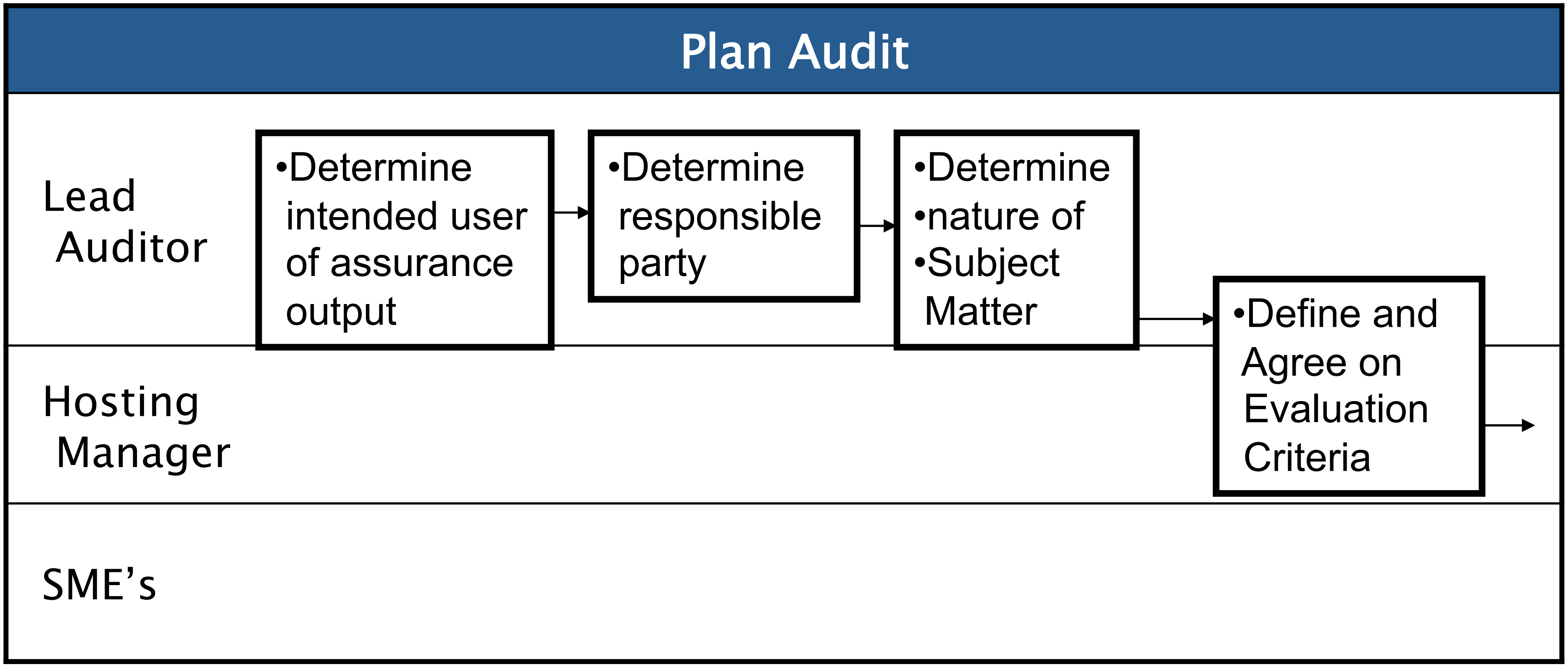
From (Suppliers)	Inputs
IT Assurance Strategy	Scope
IT Assurance Function	Qualified Resources
Policy, Standards & Procedures	Performance expectations & direction

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Outputs & Customers

Outputs	Customers (To)
Report	Intended User
Conclusions	Responsible Party
Communications	Management

Process: Flow
Activities & Roles for Plan



Plan Audit

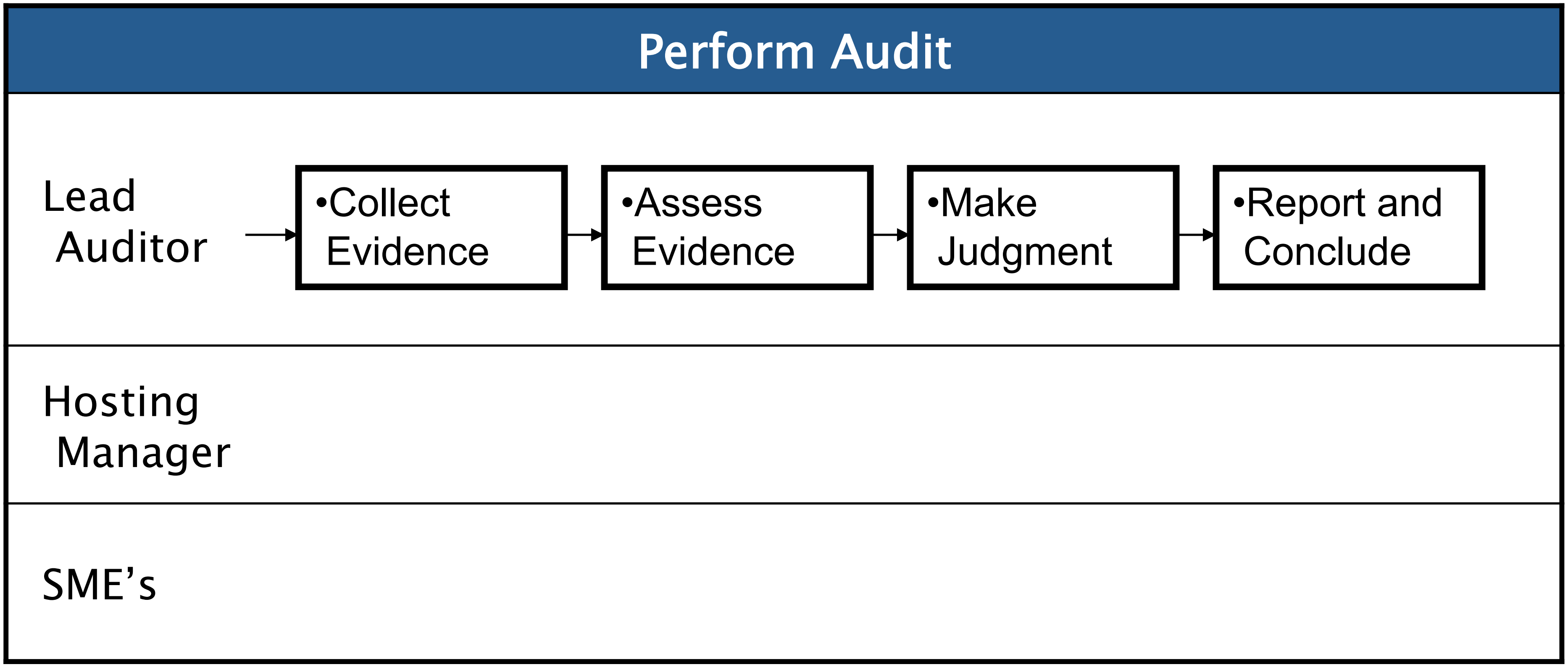
Lead Auditor

- Determine intended user of assurance output
- Determine responsible party
- Determine
- nature of
- Subject Matter
- Define and Agree on Evaluation Criteria

Hosting Manager

SME’s

Process Flow:
Activities & Roles for Perform



Perform Audit

Lead Auditor

- Collect Evidence
- Assess Evidence
- Make Judgment
- Report and Conclude

Hosting Manager

SME's

Evaluate the Process for Control

- Reason: if the Audit Process is under control then:
  - Risk is mitigated
  - Value is delivered more reliably
  - Efficiency is increased
  - Errors and Rework are Reduced or eliminated
  - Improvements are easier to recognize and achieve
  - Process is sustainable and maintained
- **Audit Management Stakeholders are happy!**

Note: This step assures basic COBIT Process Controls are in place

Checklist for Process Controls

Process Controls Checklist

Evaluate process for Customer Value:

- Reason: if the Audit Process is delivering what the customer wants then:
  - Customer has more trust and greater loyalty
  - Customer recognizes the value more reliably (and rewards accordingly)
  - Efficiency is increased
  - Errors and Rework are Reduced or eliminated
  - Improvements are easier to justify, recognize and achieve
- **Customers are Happy!**

Note: This is a Lean/Six Sigma Voice of the Customer (VOC) Process Step

Evaluating for Customer's Value: What the Customers want

Customers	What Customers want (Critical To Quality Factors):
Intended User	‣Accurate, No surprises ‣Recognize work done well ‣Keep it Short (not overwhelming) ‣Use Specifics ‣Give Reason finding & corrective action is important ‣Say How to test for success.
Responsible Party	‣Stay Focused ‣Summarize Risks & Importance ‣Summarize State of Internal Controls

Evaluating process for Business Stakeholder's Value:

- Reason: if the Audit Process is delivering what the Business stakeholder wants then:
  - Customers' Stakeholders and Management Stakeholders have more trust
  - Management Stakeholders recognize the value more reliably (and rewards accordingly)
  - Efficiency is increased
  - Errors and Rework are Reduced or eliminated
  - Improvements are easier to justify, recognize and achieve
- **Business Stakeholders happy –"transparency"**

Note: This is a COBIT IT Governance and Six Sigma (Voice of the Business) Process Step

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Evaluating for Stakeholder Value: What Stakeholders want

Stakeholder	What Stakeholder wants:
Business Management	‣Keep it Simple ‣Keep Context Clear ‣Say How well process & controls are performing ‣Use Numbers & Stories for support ‣Show Strategic Impact/alignment ‣Highlight Process & Control benefits realized for investments made ‣How long it will take, what it will cost, when you’ll be done

Fill in Gaps and Repeat

- Gap: Risks
  - Customer Value:
    - Intended User Want: Give Reason finding & corrective action is important
    - Responsible Party Want: Summarize risks and importance

- Gaps: Business & IT Goals
  - Process Control:
    - Goal alignment with Business Goals.
  - Stakeholder Value:
    - Stakeholder want: Results Show Strategic Impact/alignment

Added Suppliers and Inputs correct Customer & Stakeholder gaps:

From (Suppliers)	Inputs
Business Strategy	Business Goals
IT Strategy	IT Goals
Risk Assessment	Risks
IT Assurance Strategy	Scope
IT Assurance Function	Qualified Resources
Policy, Standards & Procedures	Performance expectations & direction

Lean – Removing 7 Deadly Wastes

- 7 Deadly Wastes
- Also called “Muda”
- DOTWIMP
  - Defects
  - Over-production
  - Transportations
  - Waiting
  - Inventory
  - Motion
  - Processing

- Lean Techniques
  - Value
  - Value-Stream Mapping
  - Flow or 5 “S” Standards
  - Pull
  - Perfection
  - Replicate

Start with Defects, Values & Flow
See www.isixsigma.com for more information

Flow: 5 “S” Standards

1. ***Seiri*/Sort**: Sorting or segregating through the contents of the workplace and removing all unnecessary items.

2. ***Seiton*/Straighten**: Putting or arranging the necessary items in their place and providing easy access by clear identification.

3. ***Seiso*/Shine**: Cleaning everything, keeping it clean and using cleaning to inspect the workplace and equipment for defects.

4. ***Seiketsu*/Standardize**: Creating visual controls and guidelines for keeping the workplace organized, orderly and clean, in other words, maintaining the *seiso*, or shine.

5. ***Shitsuke*/Sustain**: Instituting training and discipline to ensure that everyone follows the 5S standards.

Six Sigma in context

- **Methods** – Using statistics and analytics to improve control/reduce variation.
  - Six Sigma is a Statistical term describing the standard deviation of a process about it's mean that produces less than 3.4 defects per million opportunities.
- **Methodology** – Using Rigorous Process Improvement Methodology to improve control and performance.
  - Six Sigma DMAIC and Design for Six Sigma are methods that can be used by a Process improvement project to achieve breakthrough process performance improvement.
- **Muscle** – Bring on the "Belts"
  - Six Sigma is the Company-wide Initiative or "Breakthrough Strategy" credited with savings in the billions of dollars by early adopter companies

Six Sigma in Context

- **Method** – Using statistics and analytics (scientific method) to improve control/reduce variation.
  - Six Sigma is a Statistical term describing the standard deviation of a process about it's mean that produces less than 3.4 defects per million opportunities.
- **Methodology** – Using Rigorous Process Improvement Methodology to measurably improve performance – especially financial performance.
  - Six Sigma DMAIC and Design for Six Sigma are methods that can be used by a Process improvement project to achieve breakthrough process performance improvement.
- **Muscle** – Bring on the "Belts"
  - Six Sigma is the Company-wide Initiative or "Breakthrough Strategy" credited with savings in the billions of dollars by early adopter companies. Six Sigma Programs employ Black Belts.

Defined processes are quickly improved using scientific methods.

	Level 1: Initial/ Ad Hoc	Level 2: Repeatable/ Intuitive	Level 3: Defined Process	Level 4: Managed and Measured	Level 5: Optimized
Breakthrough Strategy				X	X
Improvement Project			X	X	X
Statistical Methods		X	X	X	X

Six Sigma “Value-Add” Table

“X” indicates Six Sigma Method, Methodology or Muscle that will deliver performance improvement based on the Process Maturity

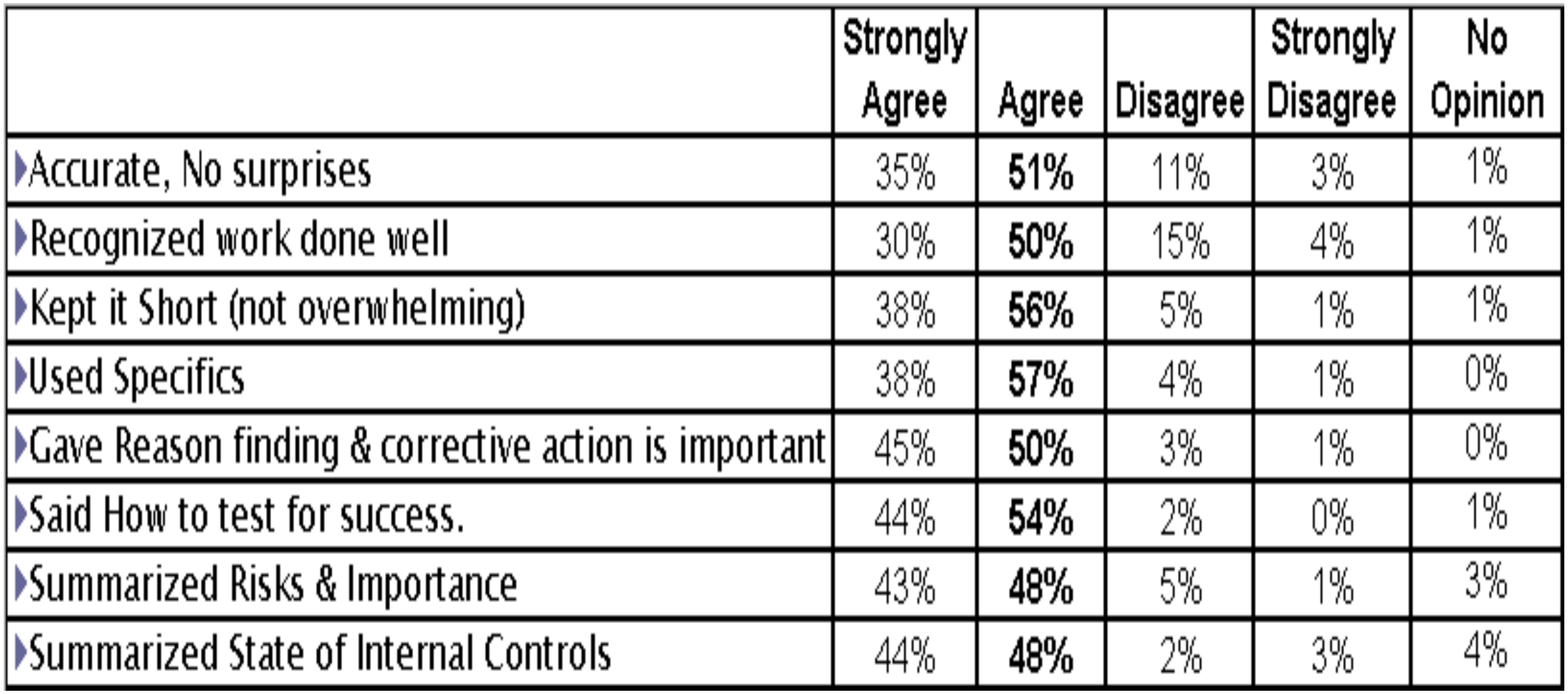
Audit Output Metrics

- % of audit findings corrected out of audit findings reported
- Audit findings reported by category or risk
- Average time lag between identification of an audit finding and corrective action
- # of Pages & # of defects logged/page in review/walkthrough of audit report
- Process Control Checklist (as a self -assessment survey)
- Customer or Stakeholder satisfaction survey

Audit Customer Satisfaction Survey

- Audit Process:
  - defined
  - a report standard template is used.
  - a peer review of the report was conducted by the team before presentation
- Audit Information:
  - Audit Team: 3
  - Time Spent: 1 week (120 hours)
  - Pages in final report: 30
    - 5 summary, 25 in appendices
  - Rating: Satisfactory
  - Findings: 2 critical or serious, 10 needs attention
  - Findings verified corrected:
    - 7 critical or serious findings corrected, 100% of previously identified findings requiring correction
- Customer Satisfaction Survey (21% response rate):
- See results on next page

Customer Satisfaction Survey Baseline Results



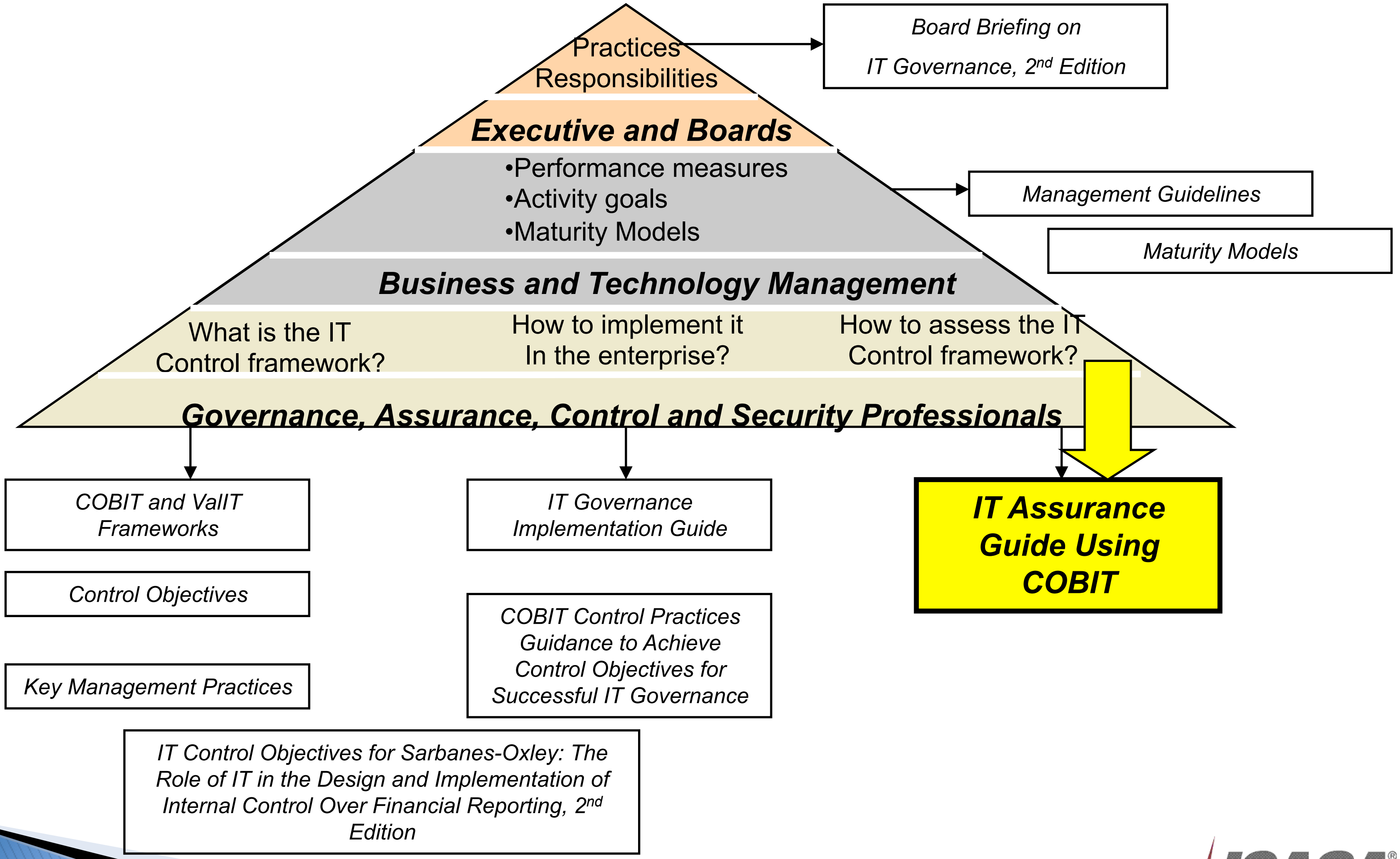
	Strongly Agree	Agree	Disagree	Strongly Disagree	No Opinion
Accurate, No surprises	35%	**51%**	11%	3%	1%
Recognized work done well	30%	**50%**	15%	4%	1%
Kept it Short (not overwhelming)	38%	**56%**	5%	1%	1%
Used Specifics	38%	**57%**	4%	1%	0%
Gave Reason finding & corrective action is important	45%	**50%**	3%	1%	0%
Said How to test for success.	44%	**54%**	2%	0%	1%
Summarized Risks & Importance	43%	**48%**	5%	1%	3%
Summarized State of Internal Controls	44%	**48%**	2%	3%	4%

What would you do to improve?

- Set a Target: Improve Customer Satisfaction
- Look at Survey results for options:
  - Remove sources of disagreement with source
  - Build on sources of agreement
  - Look to comments!
- Check for impact in:
  - Inputs and outputs
  - Activities
  - Role/Responsibilities
- Make a hypothesis –
  - **"If we include target SME's in the peer review of the report, we expect to see an improvement from Agree to Strongly Agree with Accuracy and Recognition"**
- Make the Change
  - Define/refine peer review activity to include SME's
  - Add identify/notify/train SME's and their managers about review activity
- Repeat – Test improvement

Better Audits with COBIT®

COBIT Products & IT Assurance Process



Practices
Responsibilities

Board Briefing on
IT Governance, 2nd Edition

Executive and Boards

- Performance measures
- Activity goals
- Maturity Models

Management Guidelines

Maturity Models

Business and Technology Management

What is the IT Control framework?

How to implement it In the enterprise?

How to assess the IT Control framework?

Governance, Assurance, Control and Security Professionals

COBIT and ValIT Frameworks

Control Objectives

Key Management Practices

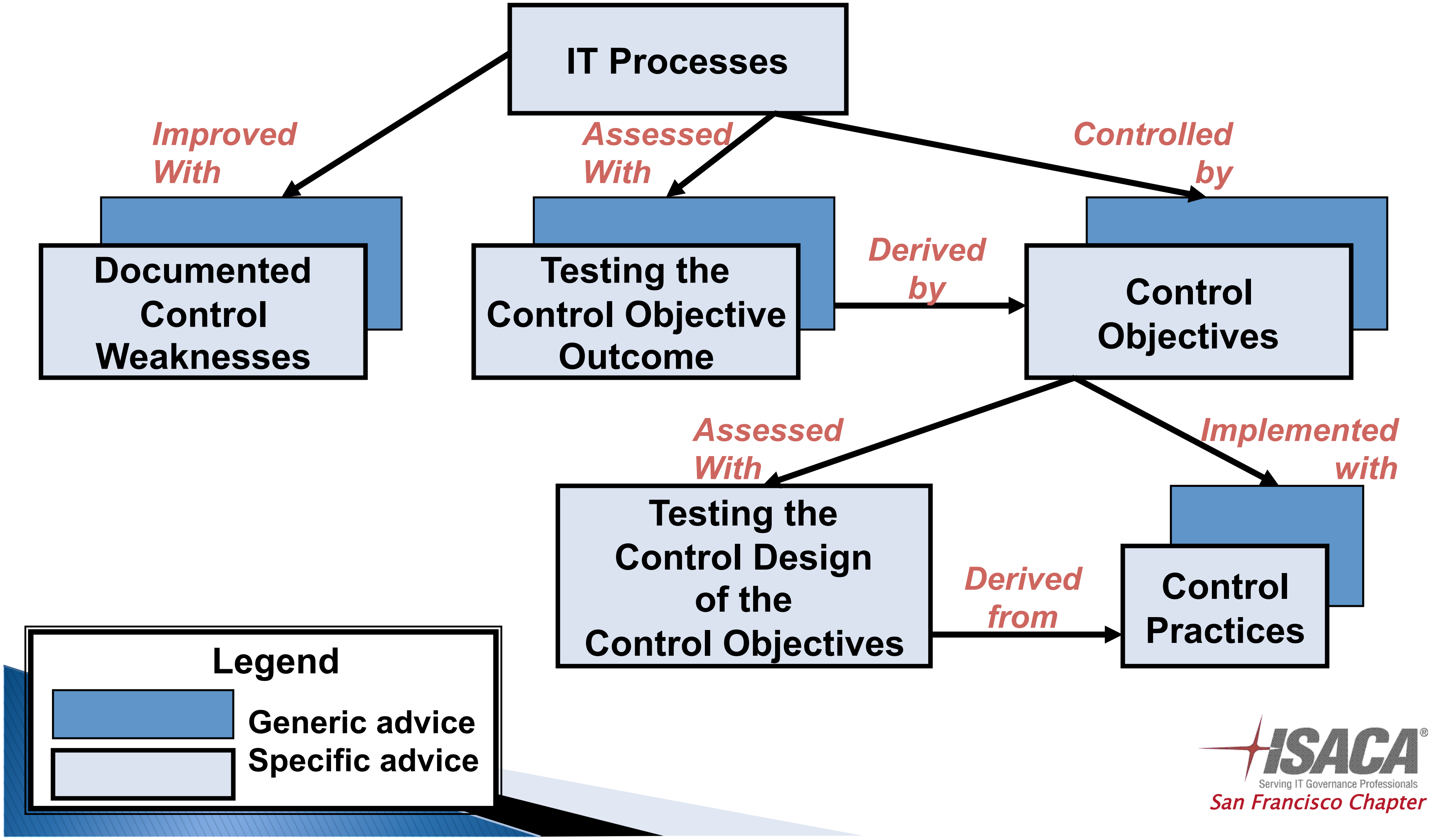
IT Governance Implementation Guide

COBIT Control Practices Guidance to Achieve Control Objectives for Successful IT Governance

IT Assurance Guide Using COBIT

IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition

IT Assurance Guide Advice



IT Processes

Improved With

Documented Control Weaknesses

Assessed With

Testing the Control Objective Outcome

Controlled by

Derived by

Control Objectives

Assessed With

Testing the Control Design of the Control Objectives

Implemented with

Derived from

Control Practices

Legend

🟦 Generic advice

⬜ Specific advice

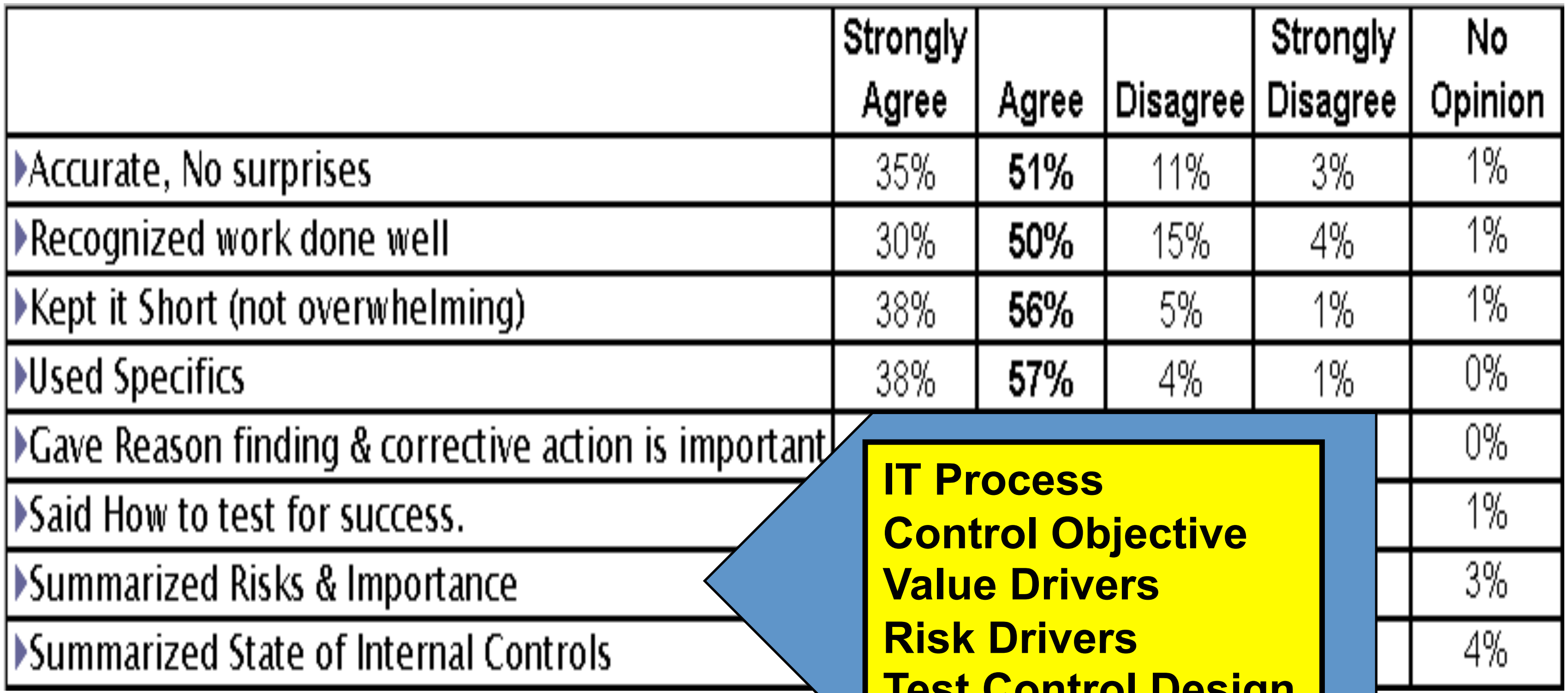
IT Assurance Guide using COBIT®

- **Table of Contents:**
  - Introduction
  - IT Assurance Principles and Context
  - Assurance Planning
  - IT Resource and Control Scoping
  - Assurance Initiative Execution
  - Assurance Guidance for COBIT® Processes and Controls
  - How COBIT® Components Support IT Assurance Activities
  - Appendix I – Process Control (PC)
  - Appendix II – Plan and Organize (PO)
  - Appendix III – Acquire and Implement (AI)
  - Appendix IV – Deliver and Support (DS)
  - Appendix V – Monitor and Evaluate (ME)
  - Appendix VI – Application Control (AC)
  - Appendix VII – Maturity Model for Internal Control
  - Appendix VIII – IT Scoping
  - Appendix IX – COBIT and Related Products

The really useful information for auditors is in the Appendices

- For each COBIT Process Control Objective /Detailed Control objective, you find:
  - Description of the Control Objective
  - Value Drivers
  - Risk Drivers
  - Test the Control Design

Where the IT Assurance Guide supports Customer Satisfaction with Audits

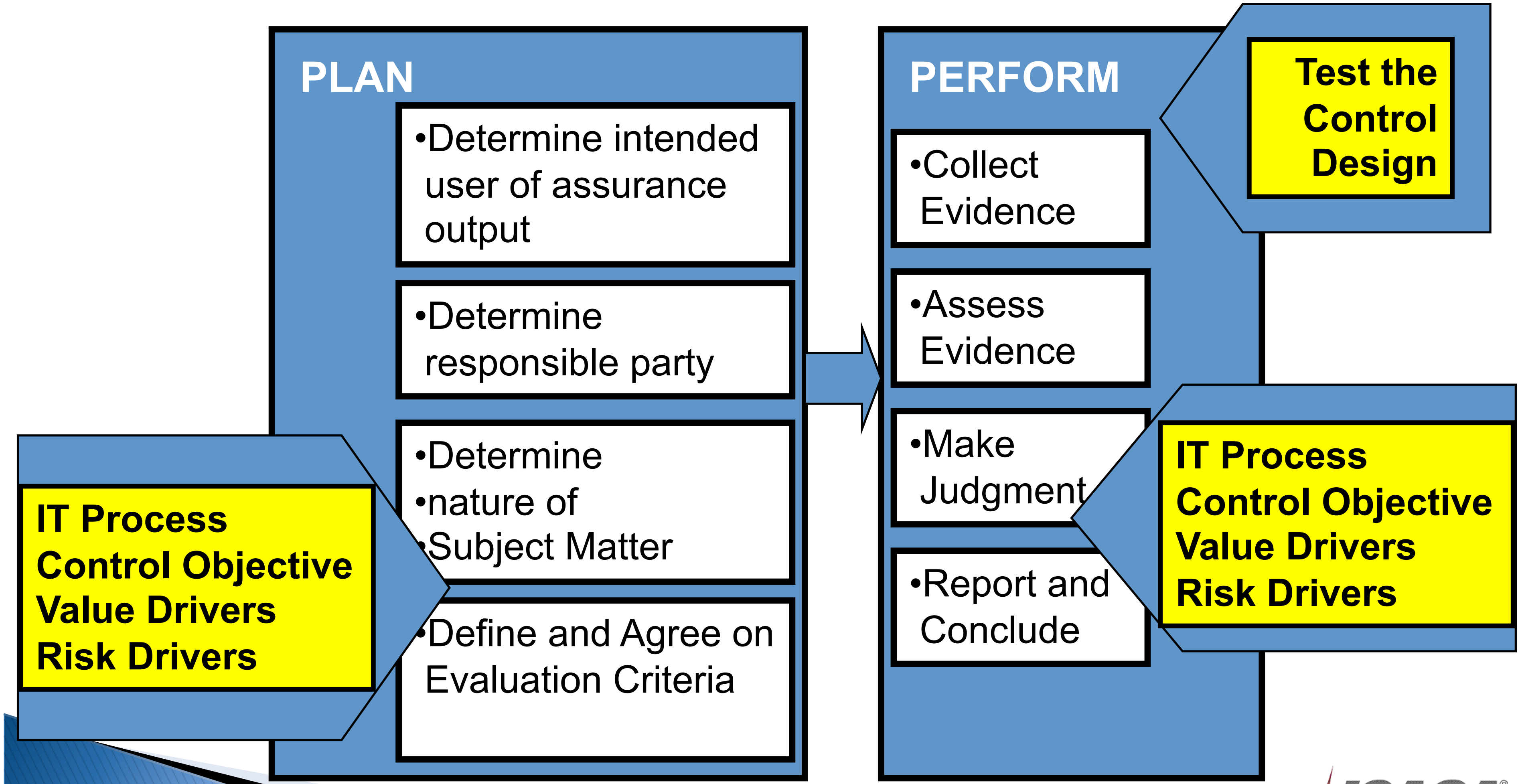


	Strongly Agree	Agree	Disagree	Strongly Disagree	No Opinion
▸Accurate, No surprises	35%	**51%**	11%	3%	1%
▸Recognized work done well	30%	**50%**	15%	4%	1%
▸Kept it Short (not overwhelming)	38%	**56%**	5%	1%	1%
▸Used Specifics	38%	**57%**	4%	1%	0%
▸Gave Reason finding & corrective action is important					0%
▸Said How to test for success.					1%
▸Summarized Risks & Importance					3%
▸Summarized State of Internal Controls					4%

IT Process
Control Objective
Value Drivers
Risk Drivers
Test Control Design

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Where the IT Assurance Guide supports the IT Audit Process



IT Process
Control Objective
Value Drivers
Risk Drivers

PLAN

- •Determine intended user of assurance output
- •Determine responsible party
- •Determine
- •nature of
- •Subject Matter
- •Define and Agree on Evaluation Criteria

PERFORM

- •Collect Evidence
- •Assess Evidence
- •Make Judgment
- •Report and Conclude

Test the Control Design

IT Process
Control Objective
Value Drivers
Risk Drivers

What would you do to improve?

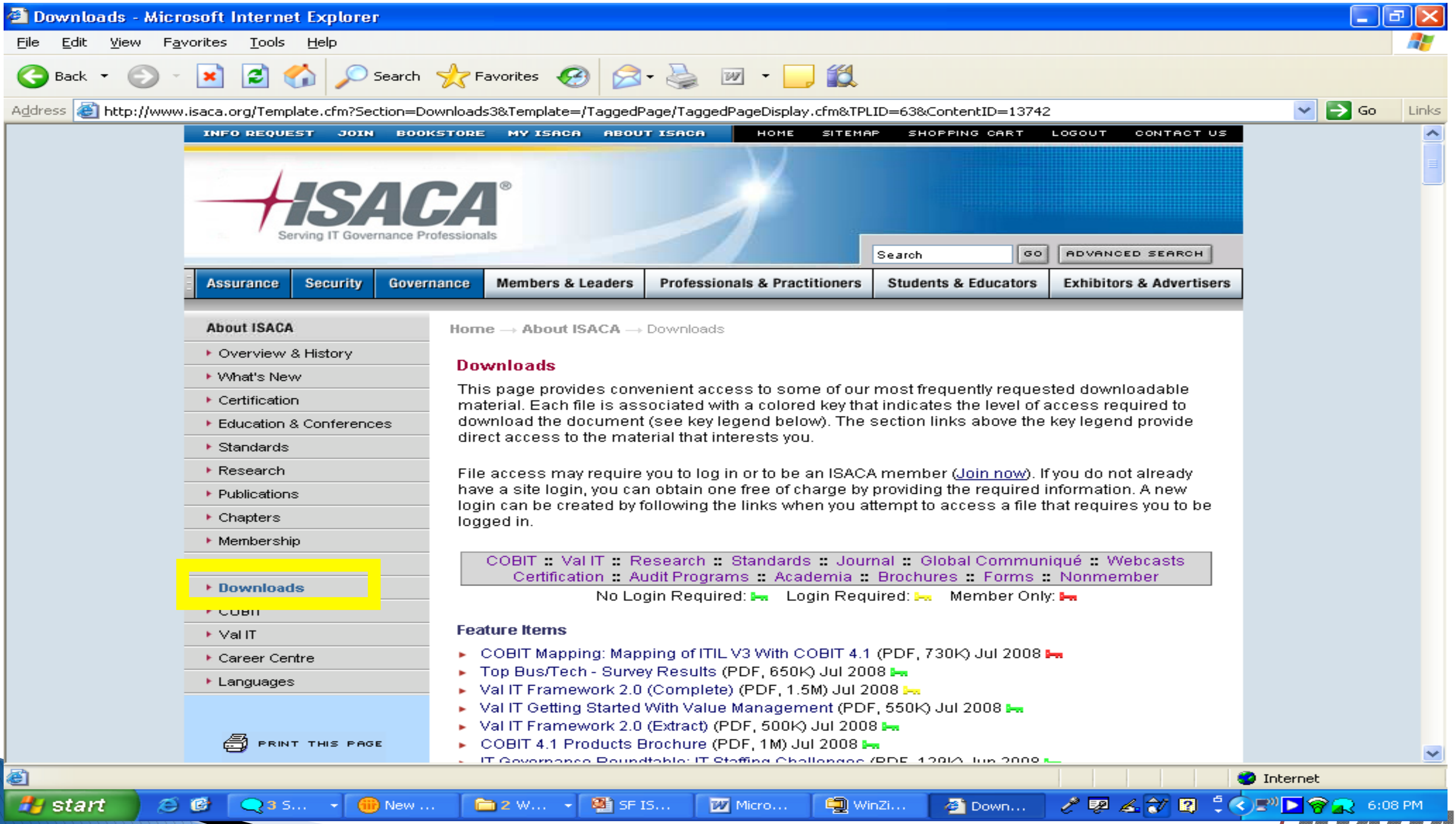
- Set a Target – improve Customer Satisfaction
- Look at Survey results for options:
  - Remove sources of disagreement with source
  - Build on sources of agreement
  - Look to comments!
- Check for impact in:
  - Inputs and outputs
  - Activities
  - Role/Responsibilities
- Make a hypothesis –
  - **"If we use the IT Assurance Guide: Risk Drivers and Value Drivers to summarize the Risks and show alignment, we expect to improve "Summarized Risks and Importance" and "Giving the reason the finding and the corrective action is important"**
- Change the Process:
  - IT Assurance Guide is an input
  - Auditors need training on how to use
- Repeat – Test improvement

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Session Summary

- Better Audits with Process Focus:
  - Process Definition
  - Process Controls
  - Customer and Stakeholder Value
  - Lean
  - Six Sigma
  - Using data from a Customer Satisfaction Survey
- Better Audits with COBIT®
  - Planning
  - Executing
  - Customer Focused Reports and Communications

www.isaca.org
(Members only) IT Assurance guide download


Downloads - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
INFO REQUEST JOIN BOOKSTORE MY ISACA ABOUT ISACA HOME SITEMAP SHOPPING CART LOGOUT CONTACT US
ISACA® Serving IT Governance Professionals
Search GO ADVANCED SEARCH
Assurance Security Governance Members & Leaders Professionals & Practitioners Students & Educators Exhibitors & Advertisers
About ISACA
Overview & History
What's New
Certification
Education & Conferences
Standards
Research
Publications
Chapters
Membership
Downloads
COBIT
Val IT
Career Centre
Languages
PRINT THIS PAGE
Internet
start
6:08 PM

http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742

Home → About ISACA → Downloads

Downloads

This page provides convenient access to some of our most frequently requested downloadable material. Each file is associated with a colored key that indicates the level of access required to download the document (see key legend below). The section links above the key legend provide direct access to the material that interests you.

File access may require you to log in or to be an ISACA member (Join now). If you do not already have a site login, you can obtain one free of charge by providing the required information. A new login can be created by following the links when you attempt to access a file that requires you to be logged in.

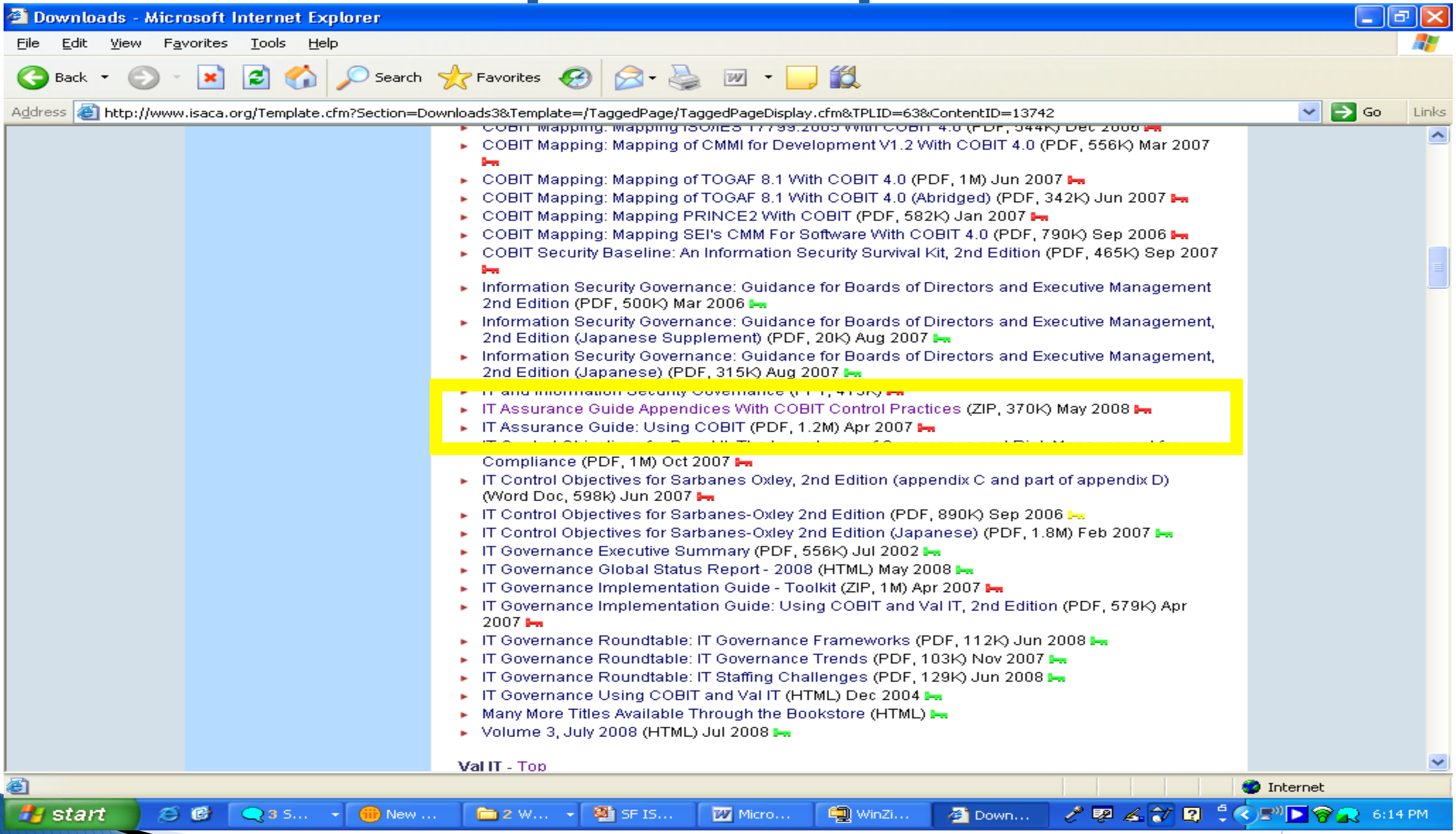
COBIT :: Val IT :: Research :: Standards :: Journal :: Global Communiqué :: Webcasts
Certification :: Audit Programs :: Academia :: Brochures :: Forms :: Nonmember

No Login Required: 🟩 Login Required: 🟨 Member Only: 🟥

Feature Items

- COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1 (PDF, 730K) Jul 2008 🟥
- Top Bus/Tech - Survey Results (PDF, 650K) Jul 2008 🟩
- Val IT Framework 2.0 (Complete) (PDF, 1.5M) Jul 2008 🟨
- Val IT Getting Started With Value Management (PDF, 550K) Jul 2008 🟩
- Val IT Framework 2.0 (Extract) (PDF, 500K) Jul 2008 🟩
- COBIT 4.1 Products Brochure (PDF, 1M) Jul 2008 🟩
- IT Governance Roundtable: IT Staffing Challenges (PDF, 120K) Jun 2008 🟩

Two files – pdf & zip archive



http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742

- COBIT Mapping: Mapping ISO/IEC 17799:2005 With COBIT 4.0 (PDF, 544K) Dec 2006
- COBIT Mapping: Mapping of CMMI for Development V1.2 With COBIT 4.0 (PDF, 556K) Mar 2007
- COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0 (PDF, 1M) Jun 2007
- COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0 (Abridged) (PDF, 342K) Jun 2007
- COBIT Mapping: Mapping PRINCE2 With COBIT (PDF, 582K) Jan 2007
- COBIT Mapping: Mapping SEI's CMM For Software With COBIT 4.0 (PDF, 790K) Sep 2006
- COBIT Security Baseline: An Information Security Survival Kit, 2nd Edition (PDF, 465K) Sep 2007
- Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition (PDF, 500K) Mar 2006
- Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition (Japanese Supplement) (PDF, 20K) Aug 2007
- Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition (Japanese) (PDF, 315K) Aug 2007
- IT and Information Security Governance (PPT, 413K)
- IT Assurance Guide Appendices With COBIT Control Practices (ZIP, 370K) May 2008
- IT Assurance Guide: Using COBIT (PDF, 1.2M) Apr 2007
- IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance (PDF, 1M) Oct 2007
- IT Control Objectives for Sarbanes Oxley, 2nd Edition (appendix C and part of appendix D) (Word Doc, 598k) Jun 2007
- IT Control Objectives for Sarbanes-Oxley 2nd Edition (PDF, 890K) Sep 2006
- IT Control Objectives for Sarbanes-Oxley 2nd Edition (Japanese) (PDF, 1.8M) Feb 2007
- IT Governance Executive Summary (PDF, 556K) Jul 2002
- IT Governance Global Status Report - 2008 (HTML) May 2008
- IT Governance Implementation Guide - Toolkit (ZIP, 1M) Apr 2007
- IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition (PDF, 579K) Apr 2007
- IT Governance Roundtable: IT Governance Frameworks (PDF, 112K) Jun 2008
- IT Governance Roundtable: IT Governance Trends (PDF, 103K) Nov 2007
- IT Governance Roundtable: IT Staffing Challenges (PDF, 129K) Jun 2008
- IT Governance Using COBIT and Val IT (HTML) Dec 2004
- Many More Titles Available Through the Bookstore (HTML)
- Volume 3, July 2008 (HTML) Jul 2008

Val IT - Top

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Survey:

Course Objective Statements:	Strongly Agree	Agree	Disagree	Strongly Disagree	No Opinion
As a result of this session, I have a better understanding of how to make my audits more effective through process controls with COBIT and some very simple Lean and Six Sigma process improvement techniques.					
As a result of this session, I have a better understanding of how COBIT components support IT Assurance activities and the particular COBIT components that provide the most benefit.					
As a result of this session, I have a better understanding of how to using COBIT for more Effective Communications with Responsible Parties and Stakeholders					

If to do were as easy as to know what were good to do, chapels had been churches, and poor men's cottages princes' palaces

The Merchant of Venice, Act I, Scene 2

Success unites knowledge and action.

Thank You for your kind attention!

KAISER PERMANENTE®

Debra Mallette, CGEIT, CISA, CSSBB
Senior Project Manager Consultant Specialist

Kaiser Foundation Hospitals
2101 Webster St. 17th Floor, 171W11
Oakland, CA 94612
510-627-3626
Cell: 510-295-3217
Debra.mallette@kp.org
www.kp.org