S11 - Implementing IT Governance
An Introduction

Debra Mallette

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

S11 - Introduction to IT Governance Implementation using COBIT® and Val IT®

Speaker:
Debra Mallette, CGEIT, CISA, CSSBB

September 21, 2009 – September 23, 2009

ISACA Serving IT Governance Professionals
San Francisco Chapter

Session Objectives

- Introduction to IT governance, stakeholders and their interests
- An overview of COBIT, *Val* IT and Risk IT
- An overview of the new life cycle for implementing IT governance with COBIT, *Val* IT and Risk IT

Session Objective: Introduction to IT governance, stakeholders and their interests

English Proverbs:

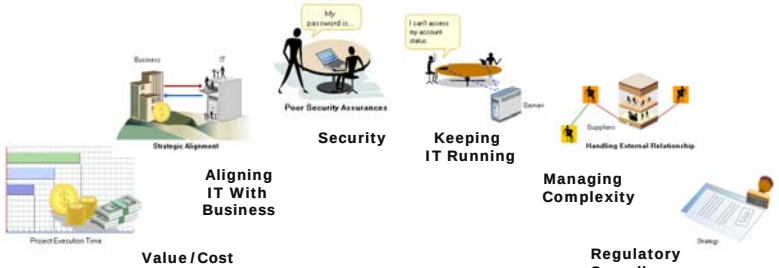
"If a man does not know what port he is steering for, no wind is favorable to him"

"*The ship that will not obey the helm will have to obey the rocks."*

Wikipedia:

The word governance derives from the Greek verb κυβερνάω [kubernáo] which means to steer and was used for the first time in a metaphorical sense by Plato. It then passed on to Latin and then on to many languages.

Need for IT Governance



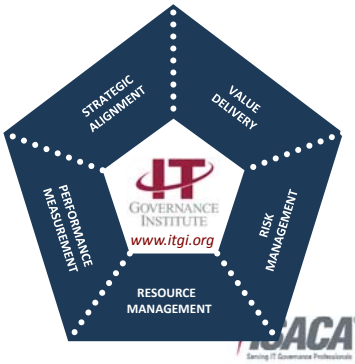
Organisations require a structured approach for managing these and other challenges, to ensure:

- **Agreed objectives for IT**
- **Good management controls**
- **Effective monitoring of performance to keep on track and avoid unexpected outcomes.**

Enterprise Governance – context

Enterprise governance is responsibilities and practices exercised by the board and executive management with goals of:

- Provide strategic direction
- Ensure achieved objectives
- Appropriately managed risk
- Responsible resource use



Enterprise Governance Objective

A Balance of:

- **Performance**
  - Improve profit, efficiency, effectiveness, growth, etc.
- **Conformance**
  - Adhere to legislation, internal policies, audit requirements, etc.

Enterprise governance and IT governance require a balance between performance and conformance goals as directed by the board.

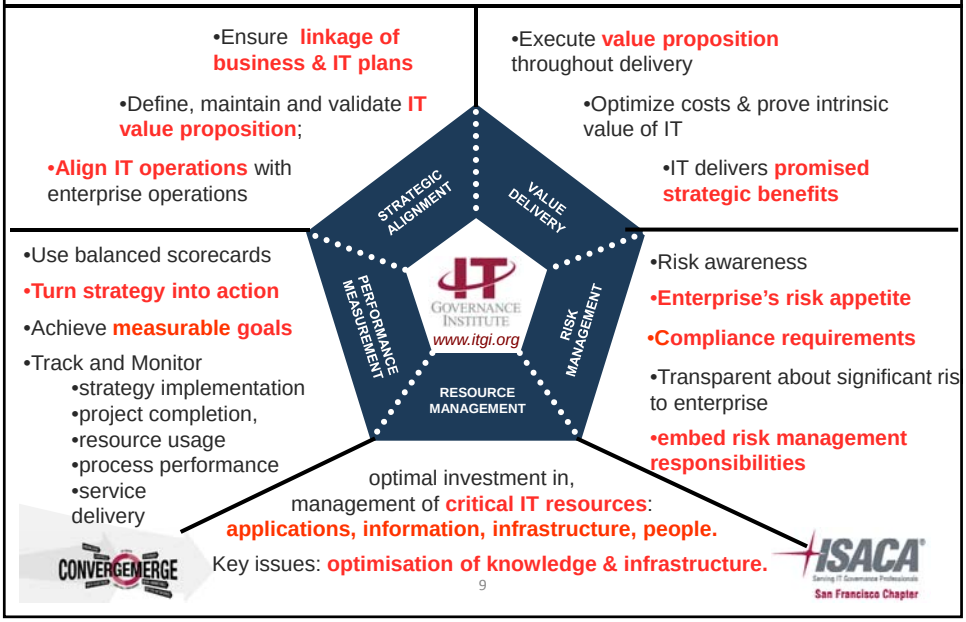
Enterprise and IT Governance

Enterprise governance is responsibilities and practices exercised by the board and executive management with goals of:

- Provide strategic direction
- Ensure achieved objectives
- Appropriately managed risk
- Responsible resource use

IT governance is ***part of enterprise governance***. Consisting of leadership, organisational structures and processes that ensure that the enterprise's IT sustains and furthers the enterprise strategies and objectives

IT Governance Focus Areas Concerned with Value & Risk



9

Governance as 2 views of Control

Ref. Figure 3, pg. 14, Implementing IT Governance, Version 2

10

Governance Stakeholder Responsibilities

Board and Executives — Set direction for IT, monitor results & insist on corrective actions.

Business Management

Define business requirements for IT and ensure that value is delivered and risks are managed.

IT management

Deliver and improve the IT services as required by the business.

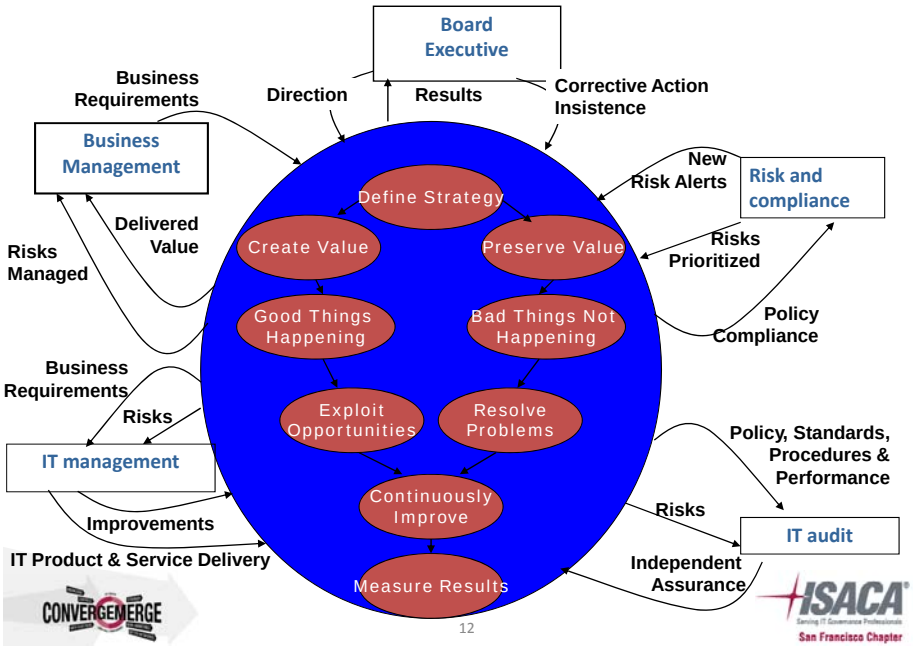
Risk and compliance

Monitor whether policies are complied with and focus on alerts to new risks.

IT audit

Provide independent assurance to demonstrate that IT delivers what is needed.

Stakeholders provide Inputs and expect Outputs



Summary of Introduction to IT governance, stakeholders and their interests

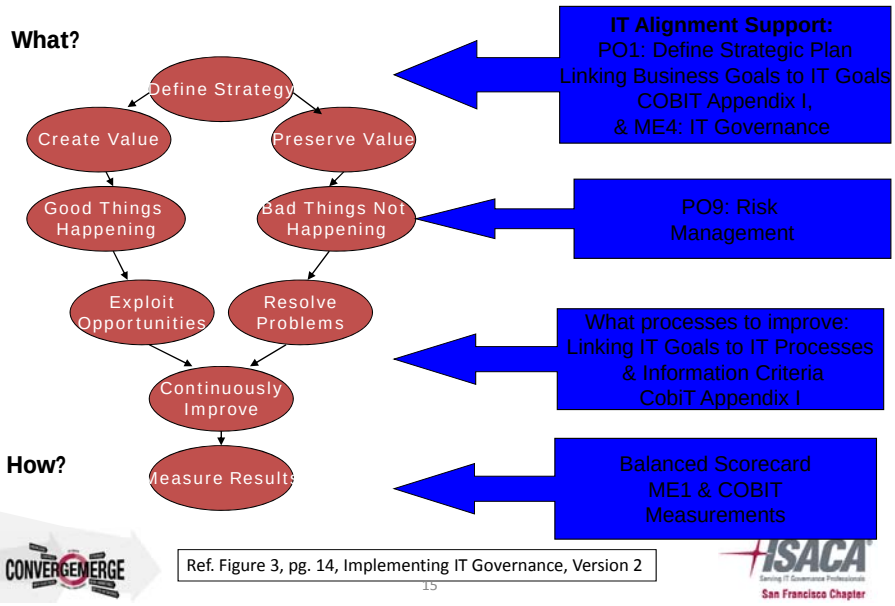
- IT Governance is part of Enterprise Governance.
- Governance Focus Areas:
  - Strategic Alignment
  - Value Delivery
  - Risk Management
  - Resource Management
  - Performance Measurement
- Governance objective is balance of
  - Performance – Value Delivery
  - Conformance – Risk Management
- Governance Stakeholders include:
  - Board & Executives
  - Business & IT Management
  - Risk and Compliance & IT Audit
- Stakeholders:
  - Have Governance Role & Responsibilities
  - Expect Inputs and Deliver Outputs to Governance Process

Session Objective: An overview of COBIT®, Val IT® and Risk IT®

Question: Why do we need an overview of the 3 ITGI Frameworks?

Answer: Because they represent an evolution of ISACA/ITGI's thinking about Governance that are being brought together in the new version of the IT Governance Implementation Guide.

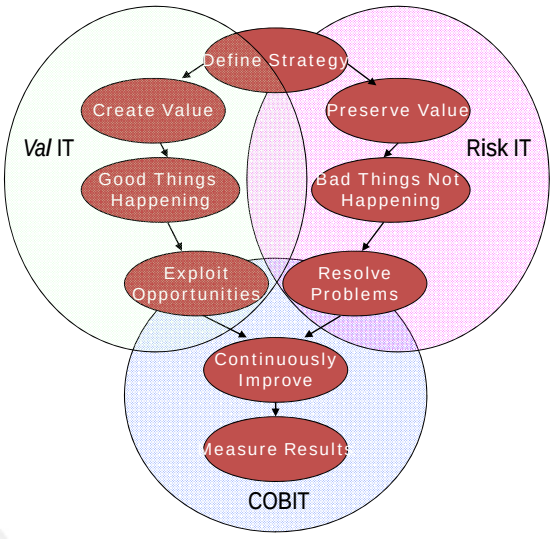
Governance Support with COBIT before introduction of ValIT and RISK IT



Ref. Figure 3, pg. 14, Implementing IT Governance, Version 2

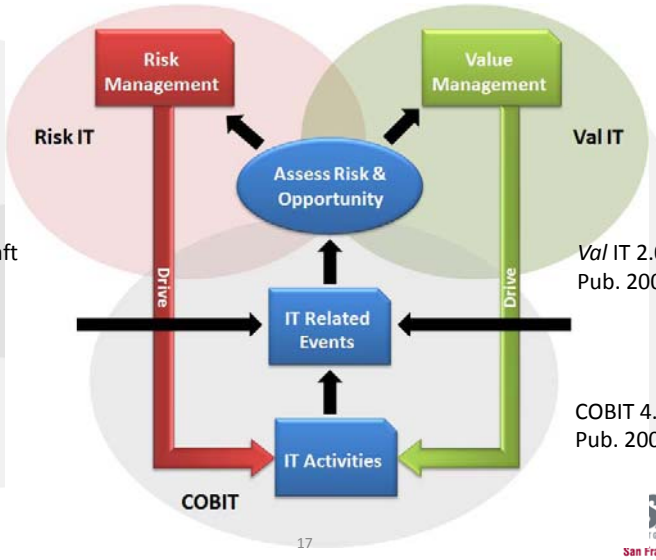
15

Governance Support with COBIT + Val IT and RISK IT



16

Brave New world of Governance: Managing Risk and Opportunity with COBIT, VAL IT and RISK IT



Risk IT Exp. Draft
Pub. 2009

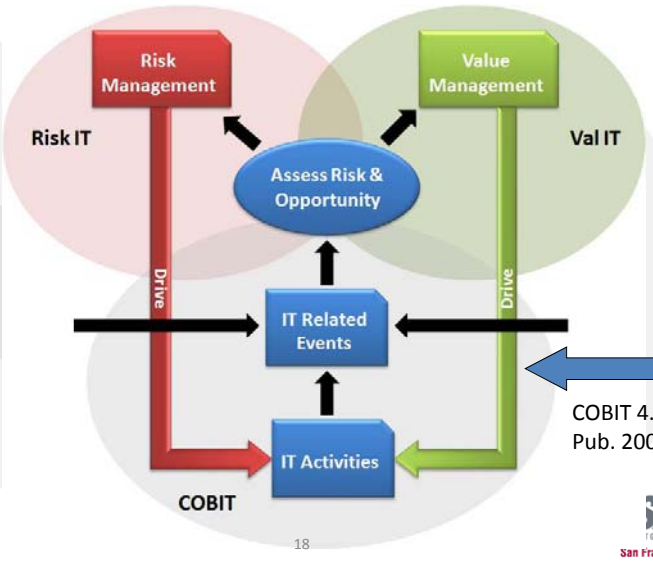
Val IT 2.0
Pub. 2008

Ref. RiskIT
Figure 9, Page 24

COBIT 4.1
Pub. 2007

17

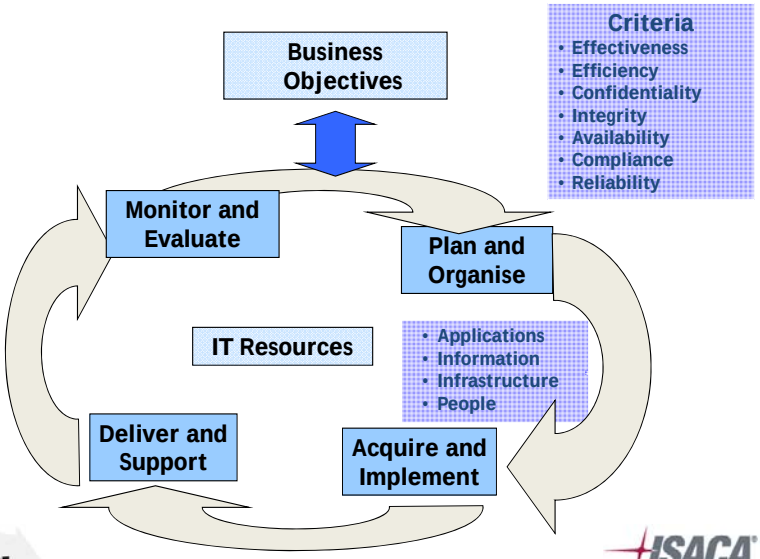
Starting with COBIT " Control Objectives for IT"



COBIT 4.1
Pub. 2007

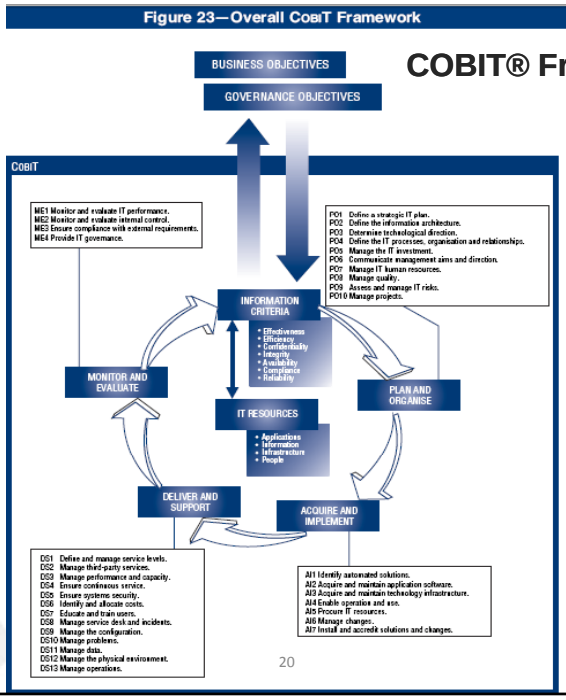
18

COBIT® Framework



19

COBIT® Framework



20

COBIT® Processes by Domain

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 by Domain

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

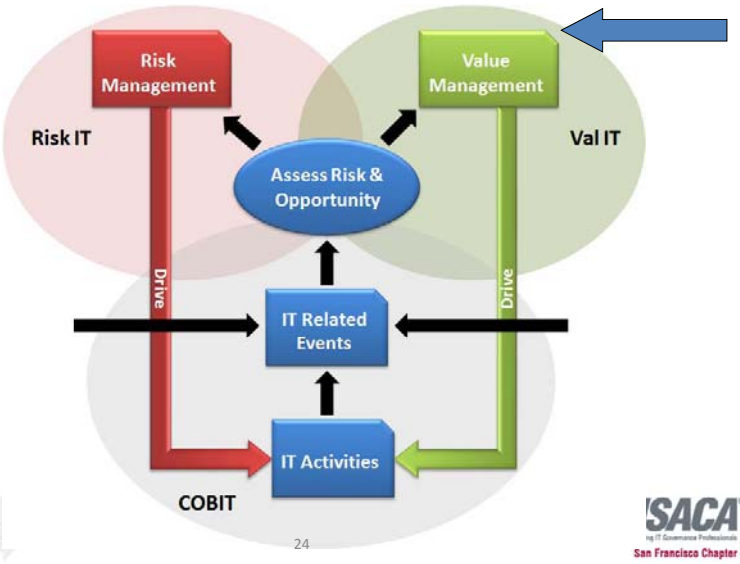
ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance With External Requirements
ME4	Provide IT Governance

Content Overview

For Framework
- Process Controls
- Application Controls
- Maturity Attributes

For each Process:
- Description, linkage to business goal, …
- Detailed Control Objectives
- Management Guidelines
  - Process Inputs and Outputs
  - Process Activities and RACI
  - Measurements
  - Maturity Model

Val IT Vers. 2.0 – Value Management



Val IT

- ***Val* IT supports the enterprise goal of**
  - creating optimal value from IT-enabled investments at an affordable cost, with an acceptable level of risk
  - **and is guided by**
    - a set of principles applied in value management processes
    - **that are enabled by**
      - key management practices
      - **and are measured by**
        - performance against goals and metrics

25

7 Principles of Val IT

- IT enabled investments will:
  - Be managed as a portfolio of investments
  - Include the full scope of activities that are required to achieve business value
  - Be managed through their full economic life cycle
- Value delivery practices will:
  - Recognise that there are different categories of investments that will be evaluated and managed differently
  - Define and monitor key metrics and will respond quickly to any changes or deviations
  - Engage all stakeholders and assign appropriate accountability to the delivery of capabilities and the realistion of business benefits
  - Be continually monitored, evaluated and improved

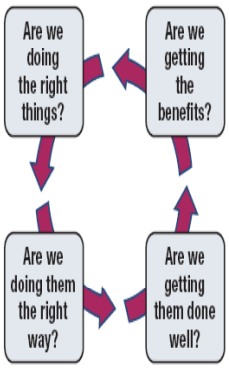
26

Val IT Questions

Figure 3—'Four Ares'

The strategic question. Is the investment:
- In line with our vision
- Consistent with our business principles
- Contributing to our strategic objectives
- Providing optimal value, at affordable cost, at an acceptable level of risk

The architecture question. Is the investment:
- In line with our architecture
- Consistent with our architectural principles
- Contributing to the population of our architecture
- In line with other initiatives



The value question. Do we have:
- A clear and shared understanding of the expected benefits
- Clear accountability for realising the benefits
- Relevant metrics
- An effective benefits realisation process over the full economic life cycle of the investment

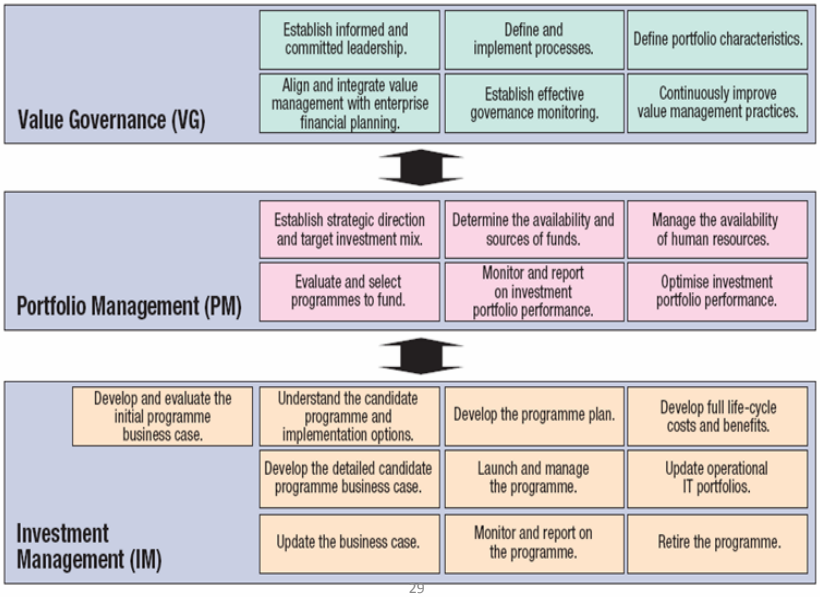
The delivery question. Do we have:
- Effective and disciplined management, delivery and change management processes
- Competent and available technical and business resources to deliver:
  - The required capabilities
  - The organisational changes required to leverage the capabilities

Val IT - Key definitions
Project, Programme & Portfolio

- **Project**—A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient to achieve a required business outcome) to the enterprise based on an agreed upon schedule and budget
- **Programme**—A structured grouping of inter-dependent projects that are both necessary and sufficient to achieve a desired business outcome and create value. These projects could involve, but are not limited to, changes in the nature of the business, business processes, the work performed by people, as well as the competencies required to carry out the work, enabling technology and organisational structure. The investment programme is the primary unit of investment within Val IT.
- **Portfolio**—Groupings of 'objects of interest' (investment programmes, IT services, IT projects, other IT assets or resources) managed and monitored to optimise business value. The investment portfolio is of primary interest to Val IT. IT service, project, asset or other resource portfolios are of primary interest to COBIT.

Val IT Framework

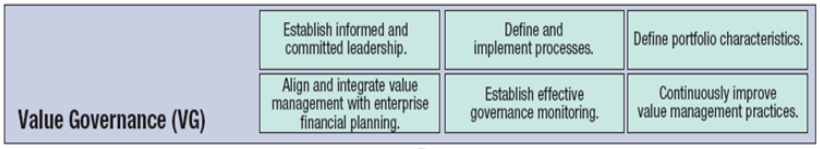
Figure 9—Val IT Domains and Processes



29

Val IT Framework – Value Governance

Figure 9—Val IT Domains and Processes



Value Governance

The goal of value governance (VG) is to ensure that value management practices are embedded in the enterprise, enabling it to secure optimal value from its IT-enabled investments throughout their full economic life cycle. An executive commitment to value governance helps enterprises:

- Establish the governance framework for value management in a manner that is fully integrated with overall enterprise governance
- Provide strategic direction for the investment decisions
- Define the characteristics of portfolios required to support new investments and resulting IT services, assets and other resources
- Improve value management on a continual basis, based on lessons learned

30

Val IT Value Governance (VG) Processes

- **VG1:** Establish informed and committed leadership.
- **VG2:** Define and implement processes.
- **VG3:** Define portfolio characteristics.
- **VG4:** Align and integrate value management with enterprise financial planning.
- **VG5:** Establish effective governance monitoring.
- **VG6:** Continuously improve value management practices.

Val IT Framework – Portfolio Management

Figure 9—Val IT Domains and Processes

Portfolio Management:
The goal of portfolio management (PM)—within the context of the Val IT framework—is to ensure that an enterprise secures optimal value
across its portfolio of IT-enabled investments.

Portfolio Management (PM)	Establish strategic direction and target investment mix.	Determine the availability and sources of funds.	Manage the availability of human resources.
	Evaluate and select programmes to fund.	Monitor and report on investment portfolio performance.	Optimise investment portfolio performance.

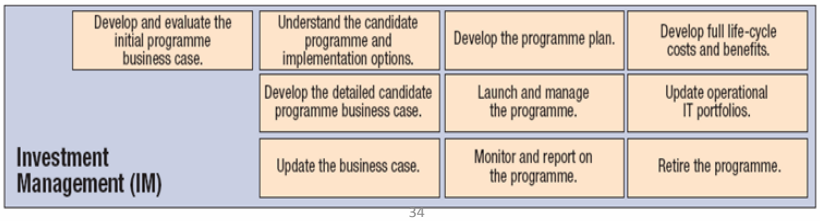
An executive commitment to portfolio management helps enterprises:
- Establish and manage resource profiles
- Define investment thresholds
- Evaluate, prioritise, and select, defer, or reject new investments
- Manage and optimise the overall investment portfolio
- Monitor and report on portfolio performance

Val IT Portfolio Management (PM) Processes

- **PM1** Establish strategic direction and target investment mix.
- **PM2** Determine the availability and sources of funds
- **PM3** Manage the availability of human resources.
- **PM4** Evaluate and select programmes to fund.
- **PM5** Monitor and report on investment portfolio performance.
- **PM6** Optimise investment portfolio performance.

Val IT Framework – Investment Management

Investment Management
The goal of investment management (IM) is to ensure that the enterprise's individual IT-enabled investments contribute to optimal value. When organisational leaders commit to investment management they improve their ability to:
• Identify business requirements
• Develop a clear understanding of candidate investment programmes
• Analyse alternative approaches to implementing the programmes
• Define each programme and document, and maintain a detailed business case for it, including the benefits' details, throughout the full economic life cycle of the investment
• Assign clear accountability and ownership, including those for benefits realisation
• Manage each programme through its full economic life cycle, including retirement
• Monitor and report on each programme's



Val IT Investment Management (IM) Processes

- **IM1** Develop and evaluate the initial programme concept business case.
- **IM2** Understand the candidate programme and implementation options.
- **IM3** Develop the programme plan.
- **IM4** Develop full life-cycle costs and benefits.
- **IM5** Develop the detailed candidate programme business case.
- **IM6** Launch and manage the programme.
- **IM7** Update operational IT portfolios.
- **IM8** Update the business case.
- **IM9** Monitor and report on the programme.
- **IM10** Retire the programme.

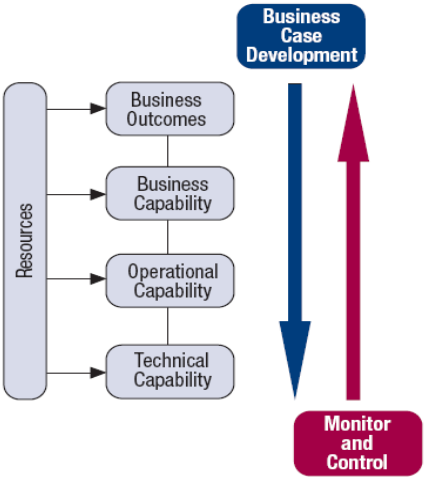
CONVERGEMERGE

35

ISACA San Francisco Chapter

Val IT Cornerstone: Complete, Comparable and Operational Business Cases

Figure 7—The Business Case



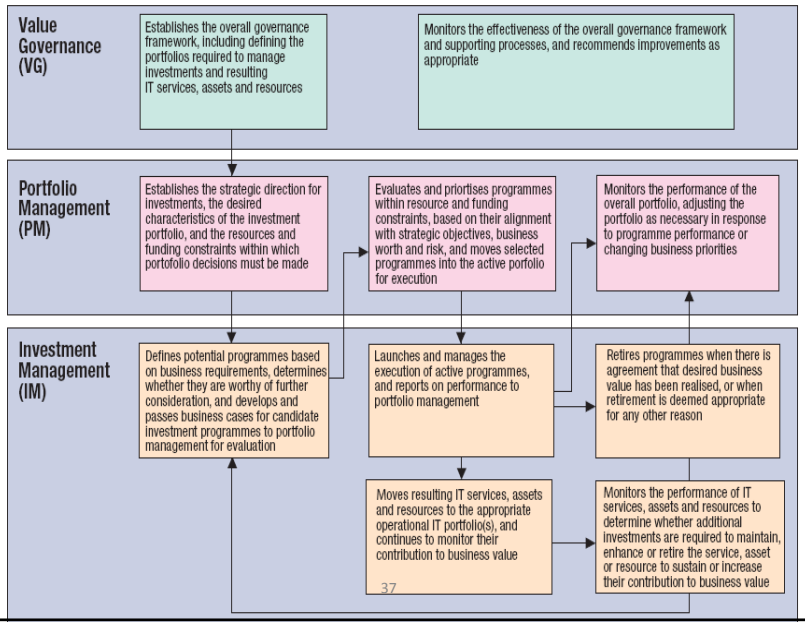
CONVERGEMERGE

36

ISACA San Francisco Chapter

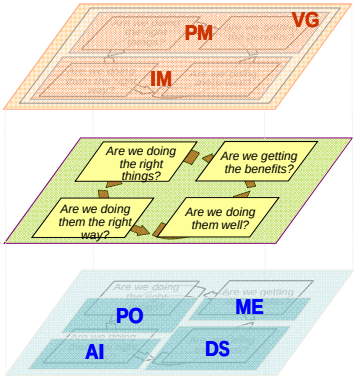
Val IT Framework Relationships (see notes)

Figure 10—Relationship Between the Val IT Domains and Processes



37

Val IT® – "a value lens into COBIT"



Val IT

COBIT

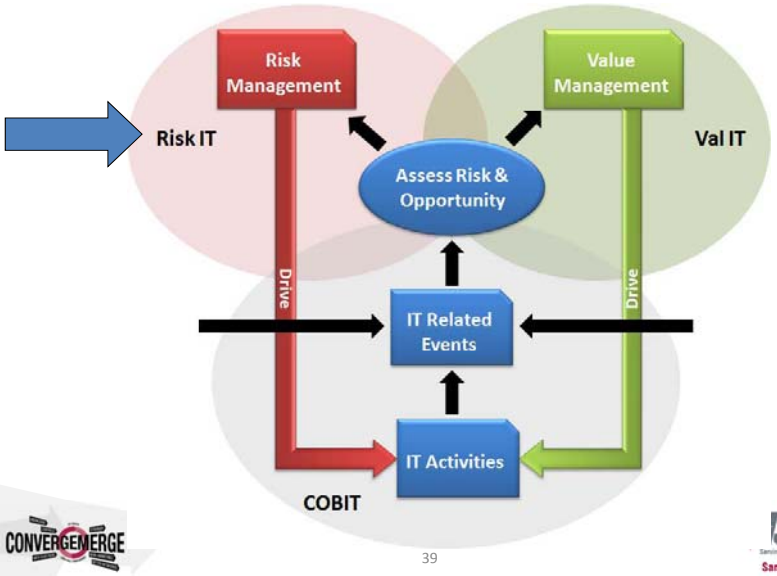
Figure 15—Comparison of Val IT With COBIT

	Governance Focus	Process Focus	Portfolio Focus
Val IT	Enterprise governance of IT	• Programme design and initiation • Benefit realisation • Investment and ongoing value management aspects of all processes	• Manage the investment portfolio • Provide the overall view of portfolio performance
COBIT	IT governance	• IT solution delivery • IT operational implementation • IT service delivery	• Manage the IT project portfolio in support of investment programmes • Manage the IT service, asset and other resource portfolios • Provide information on the performance of the IT service, asset and other resource portfolios

38

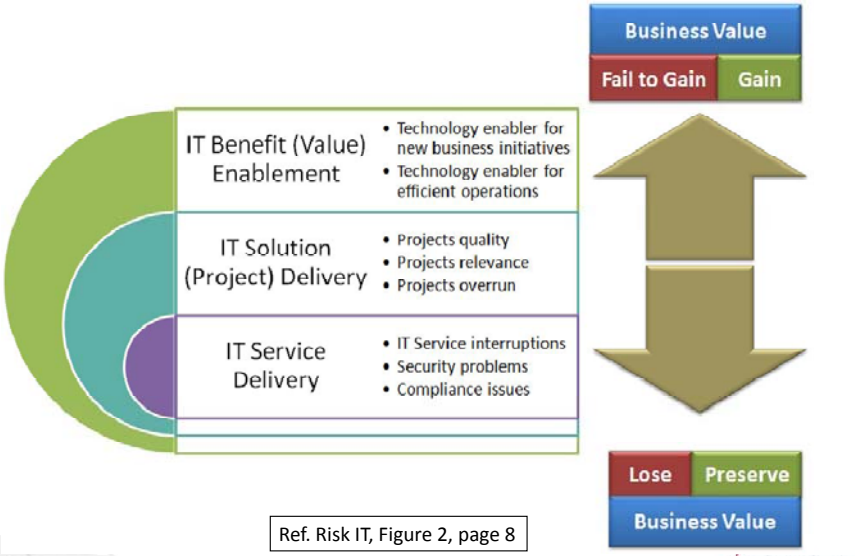
Risk IT

Framework for enterprises to identify, govern and manage IT risk



39

Types of Risk



Ref. Risk IT, Figure 2, page 8

40

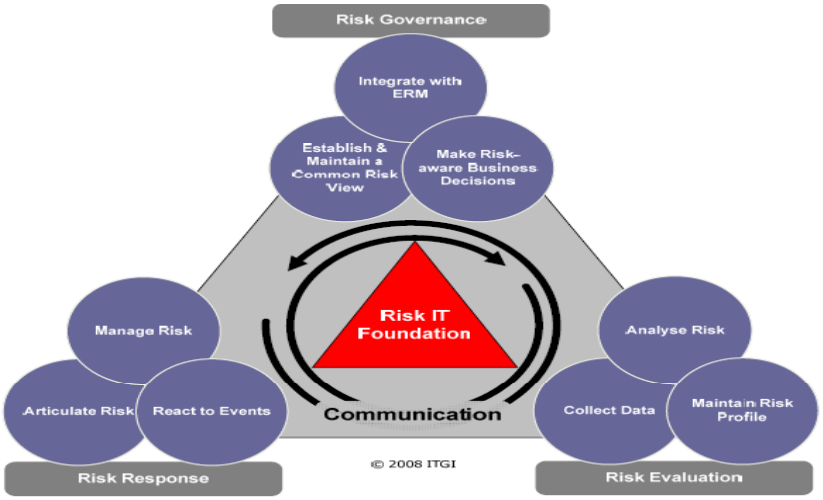
Risk IT Principles

- The Risk IT framework principles are:
  - Effective enterprise governance of IT risk:
  - Always connects to business objectives
  - Aligns the management of IT-related business risk with overall enterprise risk management
  - Balances the costs and benefits of managing risk
- Effective management of IT risk:
  - Promotes fair and open communication of IT risk
  - Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
  - Is a continuous process and part of daily activities

Risk IT Building Blocks

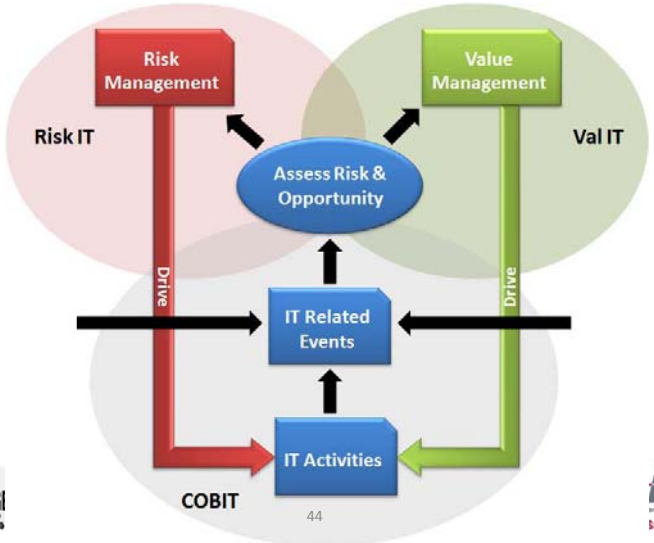
- Key building blocks of good IT risk management are:
- Set responsibility for IT risk management.
- Set objectives and define risk appetite and tolerance.
- Identify, analyse and describe risk.
- Monitor risk exposure.
- Treat IT risk.
- Link with existing guidance to manage risk.

Risk IT Components



43

Summary: COBIT®, *Val* IT® and RiskIT®

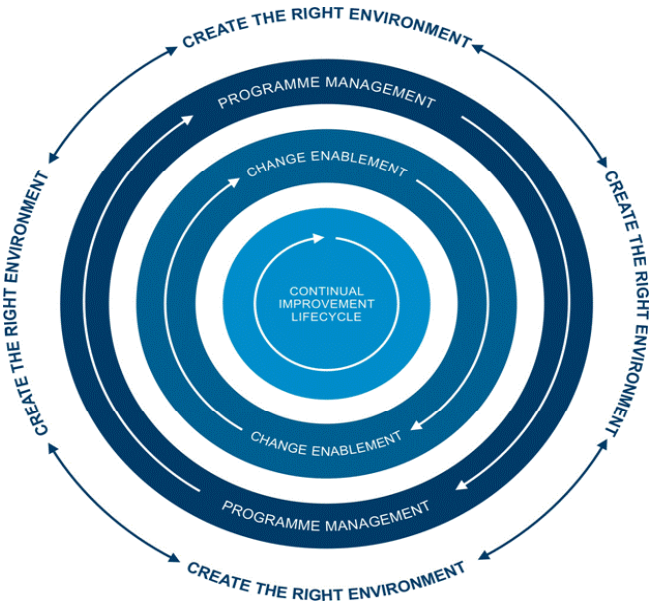


44

Session Objective: An overview of the new life cycle for implementing IT governance with COBIT, VAL IT and RISK IT

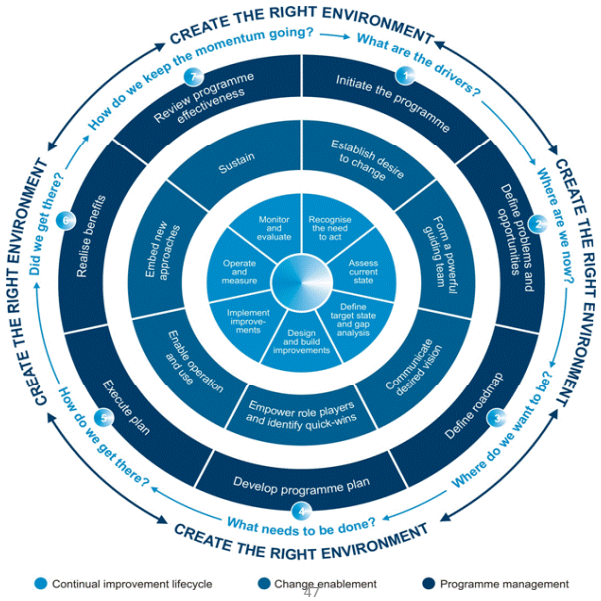
45

Lifecycle Approach

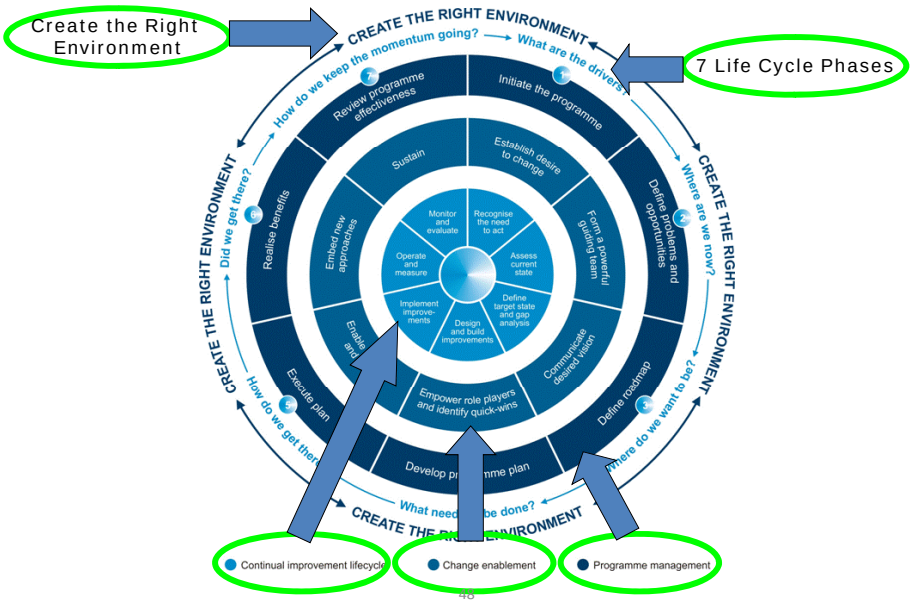


46

Implementing IT Governance Lifecycle



Parts of Lifecycle



Lifecycle Phase Walkthrough

Phases:

- What are the drivers?
- Where are we now?
- Where do we want to be?
- What needs to be done?
- How do we get there?
- Did we get there?
- How do we keep the momentum going?

Lifecycle Phase: What are the drivers?

- Goal of Phase:
  - Outline the business case
  - Identify stakeholders, roles & responsibilities
  - IT Governance programme “wake-up call” and communication kick-ogg
- Need for new or improved IT Governance Organization recognized in Pain Points and/or Trigger events.
- Pain Points analyzed for root cause and opportunities looked for during Trigger events
- Root causes and opportunities provide business case for improved or new IT Governance initiatives

Typical Pain Points

- Failed IT initiatives
- Rising Costs
- Perception of low business value for IT investments
- Significant incidents related to IT risk (e.g. data loss)
- Service Delivery Problems
- Failure to meet regulatory or contractual requirements
- Audit findings for poor IT performance or low service levels
- Hidden and/or rogue IT spending
- Resource waste through duplication or overlap in IT initiatives
- Insufficient IT resources
- IT Staff burnout/dissastisfaction
- IT enabled changes frequently failing to meet business needs (late deliveries or budget overruns)
- Multiple and complex IT assurance efforts
- Board members or senior managers that are reluctant to engage with IT

51

Trigger Events

- Merger, acquisition or divestiture
- Shift in the market, economy or competitive position
- Change in business operating model or sourcing arrangements
- New regulatory or compliance requirements
- Significant technology change or paradigm shift
- An enterprise-wide governance focus or project
- A new CIO, CFO, COO or CEO
- External audit or consultant assessments
- A new business strategy or priority

52

Lifecycle Phase: Where are we now?

- Define the Problems and Opportunities
  - See paint point causes and trigger event opportunities
- Form Powerful Guiding Team
  - Knowledgeable about the business environment
  - Have insight into influencing factors
- Assess the Current State
  - Identify IT goals and their alignment with enterprise goals
  - Identify the most important processes
  - Understand management's risk appetite
  - Understand the maturity of existing governance and related proceses

Lifecycle Phase: Where do we want to be?

- Define the Roadmap
  - Describe the high level change enablement plan and objectives
- Communicate Desired Vision
  - Develop a communication strategy
  - Communicate the vision
  - Articulate the rationale and benefits of the change
  - Set the "tone at the top"
- Define Target State and Perform Gap Analysis
  - Define the target for improvement
  - Analyze the gaps
  - Identify potential improvements

Lifecycle Phase: What Needs to be Done?

- Develop Programme Plan
  - Prioritize potential intitiatives
  - Develop formal and justifiable projects
  - Use plans that include contribution and programme objectives
- Empower Role Players and Identify Quick Wins
  - High Benefit, easy implementation should come first
  - Obtain buy-in by key stakeholders affected by the chagne
  - Identify strengths in existing processes and leverage accordingly
- Design and Build Improvements
  - Plot improvements onto a grid to assist with prioritization
  - Consider approach, deliverables, resources needed, costs, estimated time scales, project dependencies and risks

Lifecycle Phase: How do we Get There?

- Execute the Plan
  - Execute projects according to an integrated programme plan
  - Provide regular update reports to stakeholders
  - Document and Monitor the contribution of projects while managing risks identified
- Enable Operation and Use
  - Build on the momentum and credibility of quick wins
  - Plan cultural and behavioral aspects of the broader transition
  - **Define Measures of Success**
- Implement Improvements
  - Adopt and Adapt best practices to suit the organization's approach to policies and process changes

Lifecycle Phase: Did we Get There?

- Realize Benefits
  - Monitor the overall performance of the programme against business case objectives
  - Monitor and measure the investment performance
- Embed New Approaches
  - Provide transition from project mode to “business as usual”
  - Monitor whether new roles and responsibilites have been taken on
  - Track and assess objectives of the change response plans
  - Maintain communication and ensure communication between appropriate stakeholders continues
- Operate and Measure
  - Set targets for each metric
  - Measure metrics against targets
  - Communciate results and adjust targets as necessary

CONVERGEMERGE

57

ISACA San Francisco Chapter

Lifecycle Phase: How do we Keep Momentum Going?

- Continual Improvements – keeping the momentum is critical to sustainment of the lifecycle
- Review the Programme Benefits
  - Review Programme effectiveness through programme review gate
- Sustain
  - Conscious reinforcement (reward achievers)
  - Ongoing communication campaign (feedback on performance)
  - Continuous top management commitment
- Monitor and Evaluate
  - Identify new governance objectives based on programme experience
  - Communicate lessons learned and further improvement requirements for the next iteration of the cycle.

CONVERGEMERGE

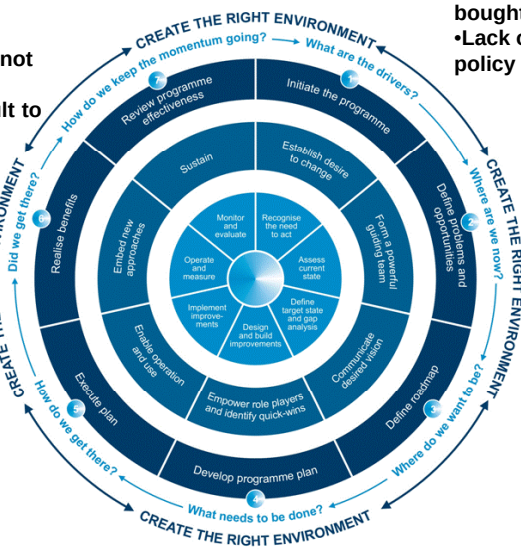
58

ISACA San Francisco Chapter

Challenges

•Improvements are not adopted or applied
•Benefits are difficult to show or prove

•Senior Management not bought-in
•Lack of current enterprise policy and direction



•Cost of improvements outweigh perceived benefits
•Lack of trust and good relations between IT and business

•Trying to do to much at once
•IT in "firefighting" mode, not able to properly prioritize tasks
•Lack of appropriate IT skills in place

•Resistance to change
•Lack of Understanding of IT Governance

Change Enablement

- Guidance provided at each lifecycle phase
- Based on Cotter Model
  - Establish a sense of urgency
  - Form a powerful guiding coalition
  - Create and communicate a clear vision, expressed simply
  - Empower others to act on the vision, identifying and implementing quick-wins
  - Enable use and implement improvements/produce more change
  - Institutionalize new approaches
  - Sustain

Guide Provides for Programme Management

- Guidance provided at each lifecycle phase
  - Initiate programme
  - Define problems and opportunities
  - Define roadmap
  - Develop programme plan
  - Execute plan
  - Realize benefits
  - Review programme effectiveness
- Detailed guidance provided by *Val* IT

How to Use COBIT, Val IT and Risk IT to implement IT Governance

- Guidance is provided for:
  - Integrating IT Governance frameworks
  - IT Governance Frameworks as enablers for Business Value
  - Using COBIT, *VAL* IT and RISK IT components

Time for you to apply what you've heard!

Session exercise

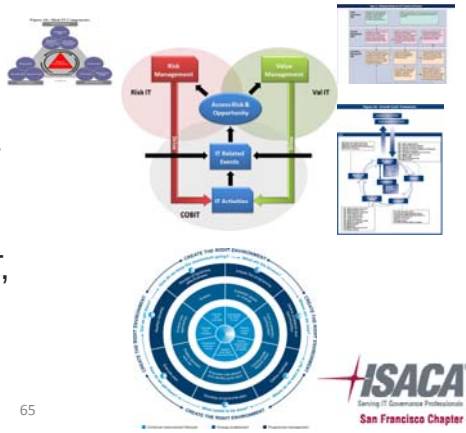
- Split into groups of about 4-5 people – one for each Phase of the Implementation Life Cycle. (see slide 50 for list of 7 phases)
- Take about 10 minutes to review the description of the Phase & identify what you might use from COBIT, RISK IT and/or *VAL* IT in your phase.
- See worksheet on next page
- Choose a spokesperson to report back to the group.

Lifecycle Phase:_____

- Use from COBIT
- Use from *Val* IT
- Use from Risk IT

Session Summary

- Introduction to IT governance, stakeholders and their interests
- An overview of COBIT, *Val* IT and Risk IT
- An overview of the new life cycle for Implementing IT Governance with COBIT, *Val* IT and Risk IT



Links

- See www.isaca.org Downloads for
  - COBIT 4.1
  - RISK IT Exposure Draft
  - Implementing IT Governance Version 3.0
    - Note: Title and content subject to change – not yet published when slides went to press.
- See www.isaca.org *Val* IT for
  - *Val* IT Version 2.0 Framework
  - *Val* IT Webcast (by John Thorp)

Thank You Very Much!

- Questions?
- Please complete a session evaluation. (Thanks)
- My contact information

Debra Mallette, CGEIT, CISA, CSSBB

KAISER PERMANENTE®
4460 Hacienda Dr.
Building D, D-163
Pleasanton, CA 94588-2761
Office Phone: 925 924 5123
Cell: 510-295-3217

CONVERGEMERGE

ISACA
San Francisco Chapter