"Introduction to IT Governance with CobiT 4.1 and CobiT Quickstart"

ISACA

Joint Session

San Francisco Chapter and Silicon Valley Chapter

April 23, 2008

Debra Mallette

CISA (Information Systems Audit and Control Association Certified Information Systems Auditor)

CSSBB (American Society of Quality Certified Six Sigma Black Belt)

ITIL V2.0 Foundation Certified

Managed Change ™ Master (LaMarsh and Associates)

Agenda

Time	Topic
8:00-8:30	Registration
8:30 – 10:00	Introductions, Overview, Navigation, Exploration of Differences
10:00-10:15	Break
10:15 – 12:00	IT Governance & Management Control Flows –
12:00 – 1:00	Lunch
1:00 – 1:45	Group Exercises – Using CobiT Quickstart to Identify IT Governance & Management Control Flow
1:45 – 2:30	Translating Audit Findings into Persuasive Management Communications – Reversing the Control Flows
2:30 – 2:45	Break
3:00 – 4:00	Systematic Approach to Implementing & Improving IT Governance & Management Control Flows
4:00 – 4:30	Review with Burning Questions
4:30 – 5:00	Course Evaluations, Certificates

Introductions

- Your name
- ISACA involvement
- Governance, Management and/or Audit responsibilities
  - (Auditor, IT manager, consultant/professional services)
- Why are you here? What would you like to get out of the class?
- Burning question?

COBIT 4.1

Please Label your materials!

Guided Tour

- COBIT 4.1 Contents (Cover)
- IT Governance Institute ™
- Table of Contents (p 4)
- How to Use your book – Framework navigation (p 26 & 27)
  - Tabs – Framework
  - Relationship to Job Aid
- Executive Overview (p 5)
  - COBIT ® *Control Objectives for Information and related Technology* (P 5, Executive Overview, about half-way down)
  - Management need for Control Objectives: (bottom of page):
    - Business Objectives are achieved
    - Undesired events are prevented or detected and corrected
  - Analogy to Brakes on the car: Go fast, safely
  - IT Governance Focus areas (Figure 2, p 6 – next slide):
    - Strategic alignment: IT is aligned with the business
    - Value Delivery IT enables the business and maximizes benefits
    - Resource Management: IT resources are used responsibly
    - Risk Management: IT risks are managed appropriately
    - Performance Measurement: objective feedback

Questions and Answers

- What does the acronym CobiT stand for?
  - *Control Objectives for Information and related Technology*
- What are the objectives for IT Governance?
  - IT is aligned with the business
  - IT enables buesiness and mximizes benefits
  - IT resources are used responsibly
  - IT risks are managed appropriately
- What are the IT Governance Focus areas?
  - Strategic alignment, Value delivery, Resource Management, Risk management and Performance Measurement
- What are the CobiT Domains?
  - Plan & Organize
  - Acquire & Implement
  - Deliver & Support
  - Monitor and Evaluation
- How many processes are in each Domain?
  - Plan & Organize = 10
  - Acquire & Implement = 7
  - Deliver & Support = 13
  - Monitor & Evaluate = 4
- What are the IT resources controlled?
  - Applications
  - Information
  - Infrastructure
  - People

Questions and Answers

- Which Domains contain processes that control the majority of the IT resources?
  - Acquire & Implement
  - Deliver & Support

- What are the CobiT Information criteria?
  - Effectiveness,
  - Efficiency,
  - Confidentiality,
  - Integrity,
  - Availability,
  - Compliance &
  - Reliability

- Which processes might the organization focus on improving if Availability is of concern?
  - PO9: Assess & Manage IT Risks
  - AI7: Manage Change
  - DS4: Ensure Continuous Service
  - DS12: Manage the physical environment

- Which processes might the organization focus on for achieving Sarbanes/Oxley (COSO) compliance?
  - See Table: Mapping IT Processes to IT Governance Focus Areas, COSO, CobiT IT Resources and CobiT Information Criteria: Appendix II.

Questions & Answers

- Which of the COBIT Processes addresses:
  - Strategic Planning and Portfolio Management: PO1
  - Risk Management: PO9
  - Financial Management: PO5 & DS6
  - Policy and Process Definition and Implementation: PO6
  - Regulatory Compliance: ME3
  - Project Management: PO10
  - System Test: AI7
  - Managing Change to the Production Environment: AI6
  - Contract and Vendor Management: AI5 & DS2
  - Help Desk: DS8
  - Business Continuity: DS4
  - Disaster Recovery: DS4
  - Configuration Management: DS9 (for production environment)
  - Asset Management: Unclear – usually combination of DS9 & DS6
  - Security: DS5
  - Performance Measurement: DS3
  - Internal Audit: ME2
  - IT Governance: ME4
  - Training: DS7
  - Roles & Responsibilities: All Processes
  - Access management: DS12 for Physical Access, DS11 for Data/Information Access, DS 5 for User Access and Identity Management

COBIT Quickstart

Please Label your materials!

COBIT® and *COBIT® Quickstart*

Business Objectives

Governance Objectives

PO1 Define a Strategic IT Plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define IT Processes, Org. & Relationships
PO5 Manage the IT investment
PO6 Communicate Mgmt aims and direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Information Criteria

- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

PLAN AND ORGANISE

ACQUIRE AND IMPLEMENT

DELIVER AND SUPPORT

MONITOR AND EVALUATE

ME1 Monitor and Evaluate IT Performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance
ME4 Provide IT Governance

IT RESOURCES

- Applications
- Information
- Infrastructure
- People

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
AI5 Manage Changes
AI6 Install and Accredit Solutions and Changes

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

COBIT Quickstart Questions

1. Which processes are in CobiT 4.1, and not *CobiT Quickstart*?
    1. (DS6 : Identify and Allocate Costs
    2. (DS7: Educate and Train Users

2. Processes are further subdivided into ___*detailed control objectives*_____. There are 210 in CobiT and 59 in *CobiT Quickstart*.

3. There are overarching Generic Process Controls that should be considered together with the process control objectives to have a complete view of control requirements are: (See page 14 in CobiT 4.1)

- PC1:__Process Goals and Objectives_____
- PC2:__Process Ownership
- PC3: Process Repeatability
- PC4:_Roles & Responsibilities
- PC5:_Policy, Plans and Procedures
- PC6:__Process Performance Improvement
- List 5-7 observations about the differences between COBIT 4.1 and COBIT Quickstart based on DS5: Ensure Systems Security.
    1. See next page

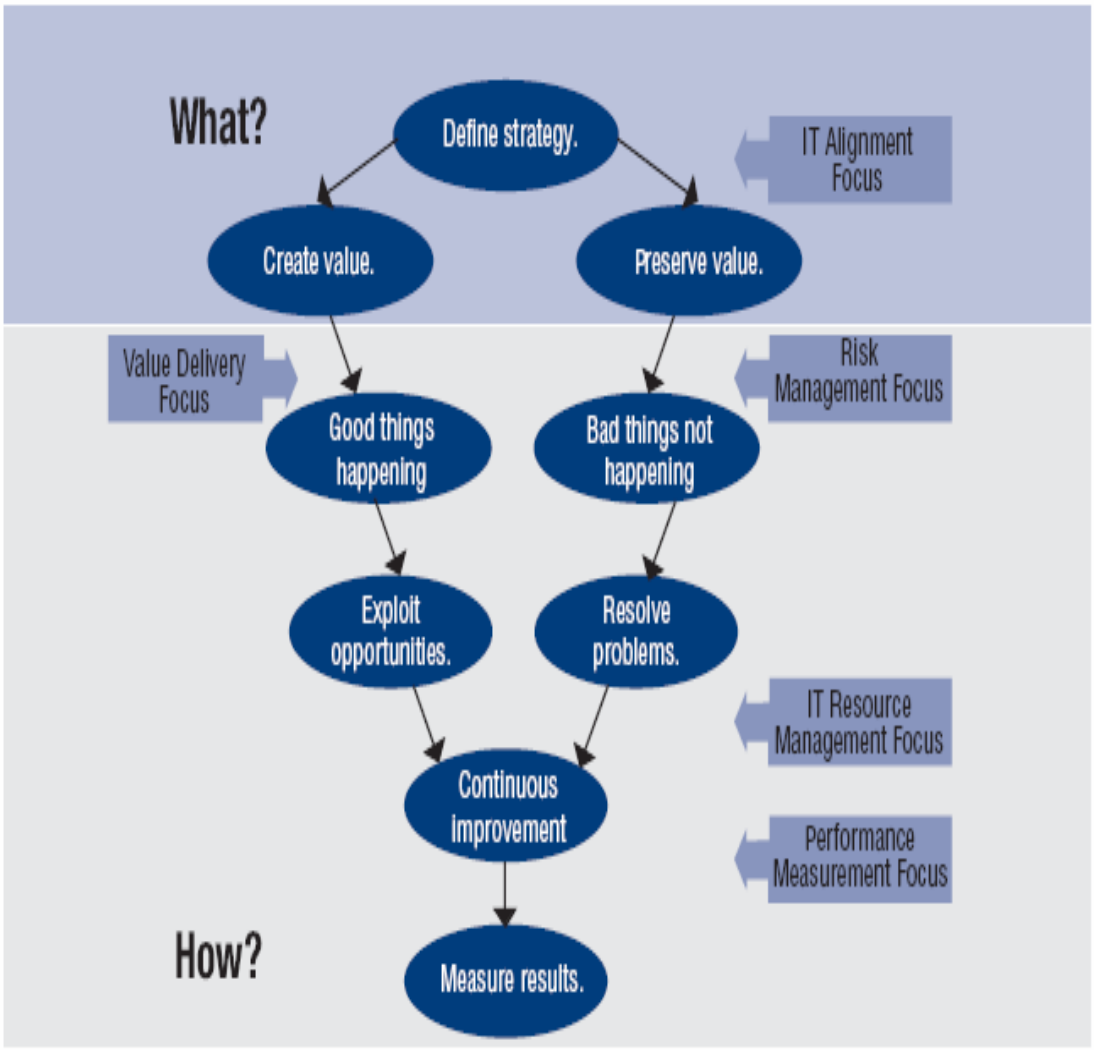
Differences between CobiT 4.1 & Cobit Quickstart

- Quickstart does not list all Control Objectives
- Quickstart is “missing” the maturity model
- 4.1 Doesn’t call out Application Controls as critical supporting reference.
- 4.1 had more metrics
- 4.1 talks about inputs and outputs
- Quickstart shows less detail in the RACI chart (includin what RACI means)
- Quickstart combines Implementation with the Model and 4.1 does not. (Can we download Implementing IT Governance from the site?)
- Quickstart uses the term “Good Practices” rather than “Control Objectives” listed in the manual.
- Quickstart isn’t targeted toward auditors – targeted management
- Quickstart seems to be based on the size/complexity criteria. May be organizations that meet the size/complexity criteria that still need to go to “full CobiT” and beyond.
- Quickstart self-assessment takes a different approach than Implementation Guidelines for “full” CobiT.

Management Control Flows

Control Flows for Enterprise IT Governance and Management:

Connecting IT Alignment Focus on Creating and Preserving Value to Measured Results



Flow is Top Down
2 Paths: Value-Delivery and Risk Management

Ref. IT Governance Implementation Guide, 2nd edition, Page 14

COBIT Quickstart
DS5: Ensure Systems Security (p45)

Processes and Good Practices				Key Metrics	
DS5 Ensure systems security.					
***COBIT Quickstart* Process**		***COBIT Quickstart* Management Practices**	**CO Ref**	Control Objective Metric	IT Process Metrics
Define IT security principles and procedures, and monitor, detect, report and resolve security vulnerabilities and incidents.	42	Implement procedures to control access based on the individual's need to view, add, change or delete data. Especially consider access rights by service providers, suppliers and customers, and change passwords of standard users.	DS5.3 DS5.4	- Elapsed time to grant, change and remove access rights	- Number of incidents due to unauthorised access - Number of security violations
	43	Make sure one person is responsible for managing all user accounts and security tokens (passwords, cards, devices, etc.) and that appropiate emergency procedures are defined. Periodically review/confirm his/her actions and authority.	DS5.4 DS13.4	- Number of violations during emergency situations.	
	44	Log important security violations (system and network, access, virus, misuse, illegal software). Ensure they are reported immediately and acted upon in a timely manner.	DS5.5 DS5.6	- Time since last update of violations log.	
	45	Ensure that all users (internal, external and temporary) and their activity on I T Systems are uniquely identifyable.	DS5.3 AC6	- Number of generic accounts	
	46	Implement virus protection, update security patches, enforce use of legal software. Put preventive, detective and corrective measure to protect from malware. Install and configure firewalls to control network access and information flow.	DS5.9 DS5.10	- Time since last security patch - Number of preventive and detective measures per month	

Diagram the Control Flows

- Top => Strategic Objective
- Bottom => Performance Measurement
- IT Objective is Process Objective
- Management Practices
  - Deliver Value
  - Manage Risk
  - Manage Resources
  - Improve Performance & Process

COBIT Quickstart's DS5: Ensure Systems Security (Page 45 in *Quickstart*)

Define Strategy

Objective (Goal)

Ensure IT Security

Process Objectives

Create Value

Preserve Value

Management Practices)

Good Things Happening

Bad Things Not Happening

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- ***Number of incidents due to unauthorized access***
- ***Number of security violations***

COBIT Quickstart's DS5: Ensure Systems Security (Page 45 in book)

Define Strategy

Ensure IT Security

Objective (Goal)

Create Value

Define IT security principles and procedures

Preserve Value

Monitor, detect, report and resolve security vulnerabilities and incidents

Process Objectives

Good Things Happening

Bad Things Not Happening

Management Practices)

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- ***Number of incidents due to unauthorized access***
- ***Number of security violations***

COBIT Quickstart's DS5: Ensure Systems Security (Page 45 in book)

Define Strategy

Ensure IT Security

Objective (Goal)

Process Objectives

Create Value

Define IT security principles and procedures
Repeatable, low cost onboarding
Reduce time to implementation
to adopt process improvements

Preserve Value

Monitor, detect, report and resolve security vulnerabilities and incidents

Management Practices)

Good Things Happening

A Person is Managing user accounts and security tokens

Bad Things Not Happening

Report and immediately act on important security violations

Exploit Opportunities

All users and their activity are uniquely identifiable

Resolve Problems

Implement virus protection, update security patches, enforce use of legal software, install firewalls

Continuous Improvement

Log important security violations, identify preventive actions

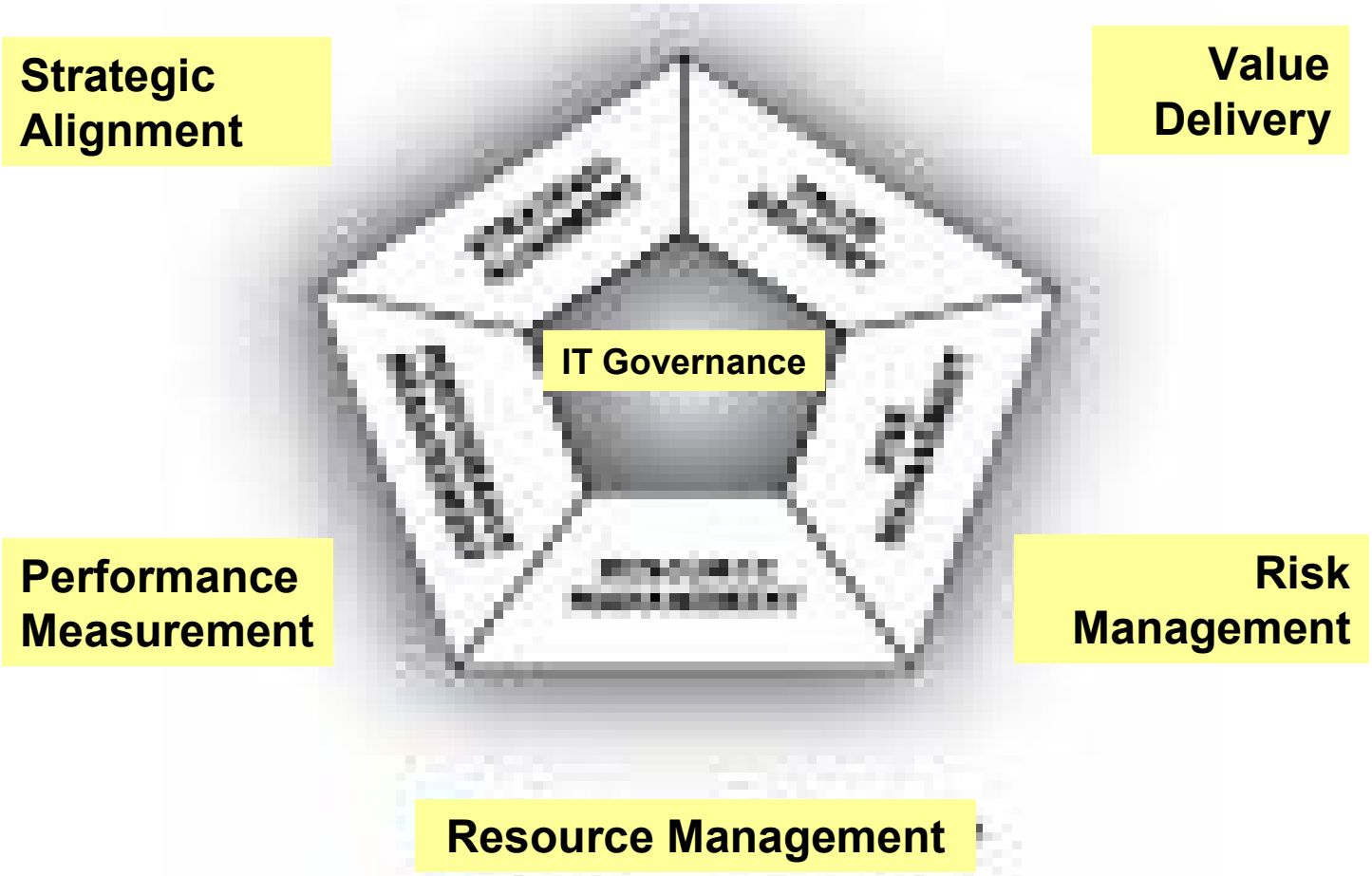
Measure Results

- ***Number of incidents due to unauthorized access***
- ***Number of security violations***

Now let's do this with CobiT 4.1

IT Governance Focus Areas

IT Governance Focus Areas:

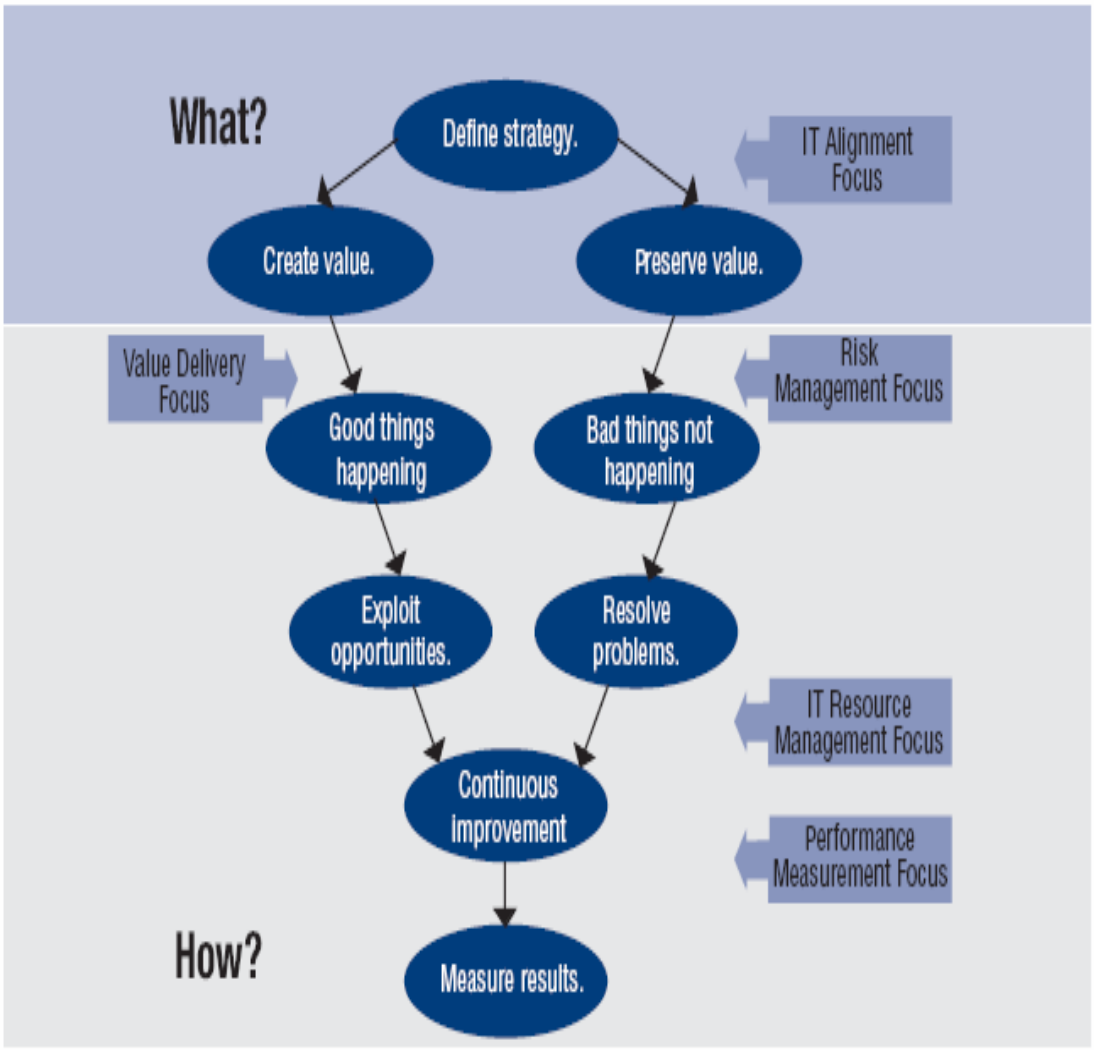


Ref. COBIT© 4.1 Page 6 and Page 26

Control Flows Connecting IT Governance Focus Areas

Control Flows for Enterprise IT Governance and Management:

Connecting IT Alignment Focus on Creating and Preserving Value to Measured Results



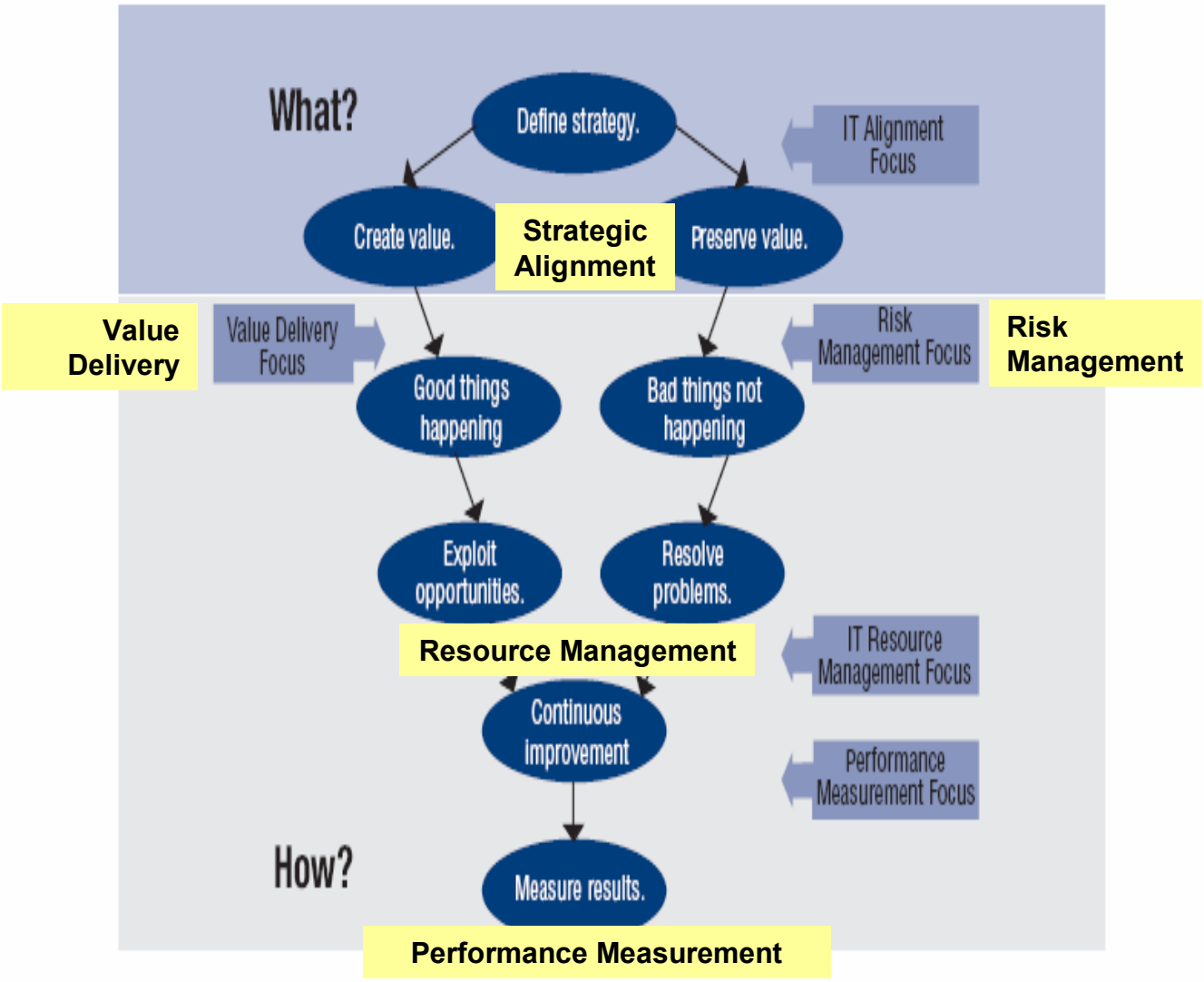
Flow is Top Down
2 Paths: Value-Delivery and Risk Management

Ref. IT Governance Implementation Guide, 2nd edition, Page 14

Control Flows Connecting IT Governance Focus Areas

Control Flows for Enterprise IT Governance and Management:

Connecting IT Alignment Focus on Creating and Preserving Value to Measured Results



Flow is Top Down

2 Paths: Value-Delivery and Risk Management

Ref. IT Governance Implementation Guide, 2nd edition, Page 14

Aligning Business Strategy with Performance Measurement

Business Objective (Goal)

Define Strategy

Strategic Alignment

IT Objective (Goal)

Create Value

Preserve Value

Value Delivery

Risk Management

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

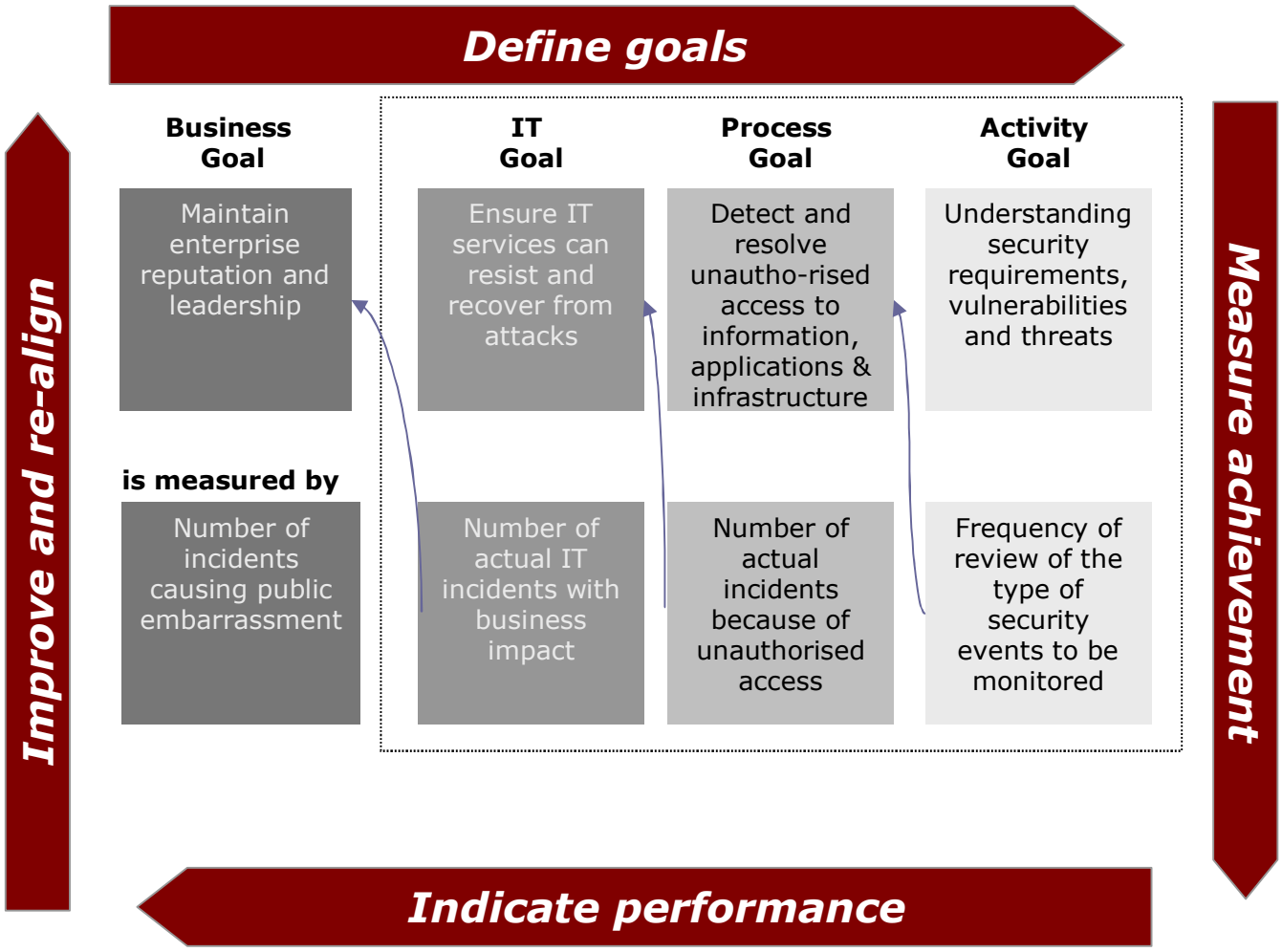
Resource Management

Continuous Improvement

Measure Results

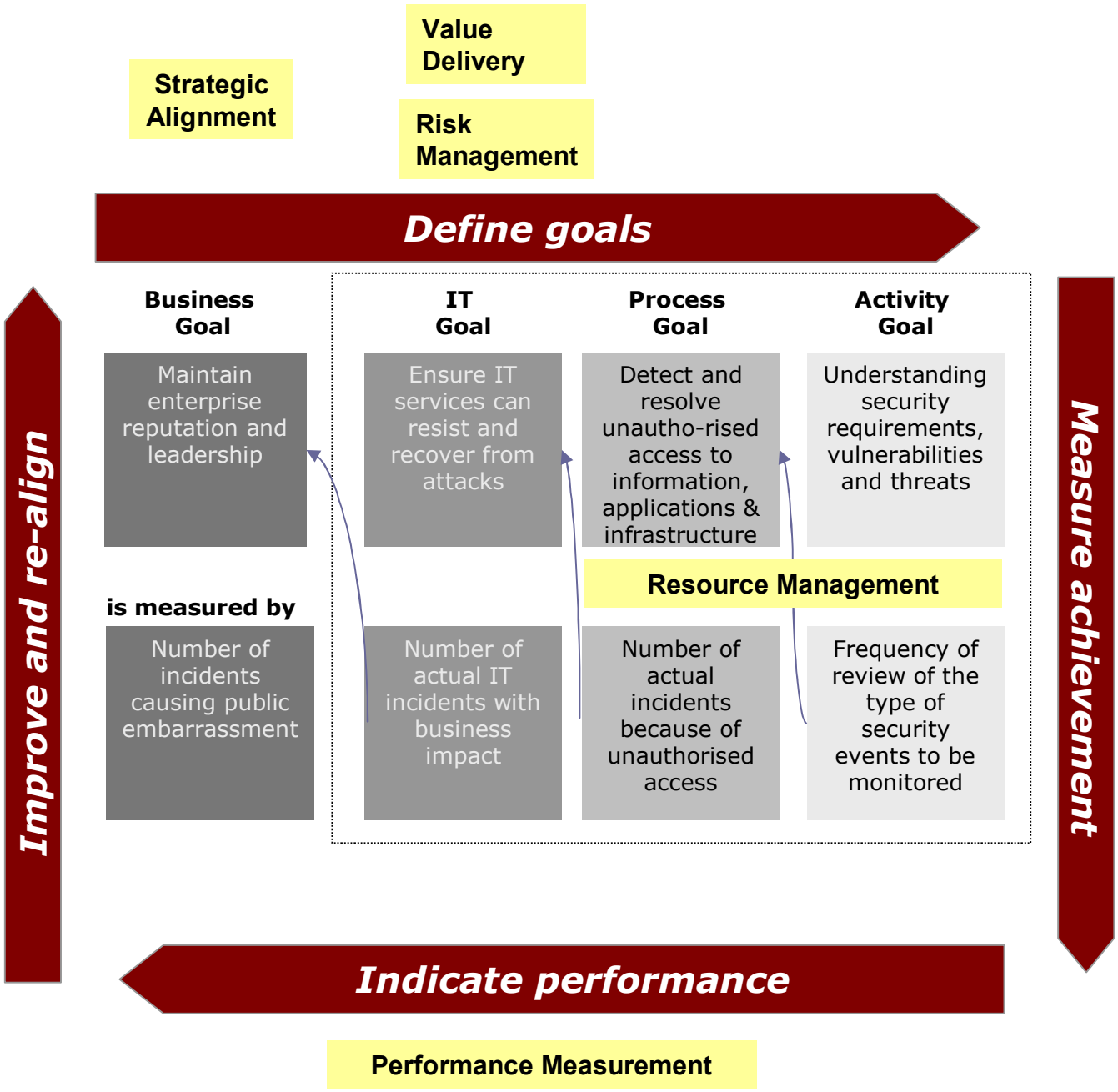
Performance Measurement

Relationship Amongst Process, Goals and Measures*



*** This is figure 19 in COBIT 4.1. The Example is based on DS5 Ensure Systems Security**

Leveraging the Relationship Amongst Process, Goals and Measures*



*** This is figure 19 in COBIT 4.1. The Example is based on DS5 Ensure Systems Security**

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Preserve Value

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- *# of incidents causing public embarrassment*

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- *# of actual IT incidents with business impact*

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

Detect & Resolve Unauthorized access to information, applications and infrastructure

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- *# and type of suspected and actual access violations*

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

Detect & Resolve Unauthorized access to information, applications and infrastructure

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

Gap

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Optimize authorized access to information, applications & infrastructure

Bad Things Not Happening

Detect & Resolve Unauthorized access to information, applications and infrastructure

IT Activity Goal or Control Objective

Exploit Opportunities

Resolve Problems

Continuous Improvement

Measure Results

- *Time to grant, change and remove access privileges*
- *# and type of suspected and actual access violations*

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Optimize authorized access to information, applications & infrastructure

Bad Things Not Happening

Detect & Resolve Unauthorized access to information, applications and infrastructure

IT Activity Goal or Control Objective

Exploit Opportunities

Effective, Efficient & Standardized User Identity and Authorization Management

Resolve Problems

Emergency Response to Malware (viruses, worms, Spyware, spam) attacks

Continuous Improvement

Measure Results

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Optimize authorized access to information, applications & infrastructure

Bad Things Not Happening

Prevent, Detect & Resolve Attacks through Unauthorized access

IT Activity Goal or Control Objective

Exploit Opportunities

Effective, Efficient & Standardized User Identity and Authorization Management

Resolve Problems

Emergency Response to Malware (viruses, worms, Spyware, spam) attacks

Continuous Improvement

Measure Results

- *Number of access rights authorized, revoked, reset or changed*
- *Number and type of malicious code prevented*

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Optimize authorized access to information, applications & infrastructure

Bad Things Not Happening

Prevent, Detect & Resolve Attacks through Unauthorized access

IT Activity Goal or Control Objective

Exploit Opportunities

Effective, Efficient & Standardized User Identity and Authorization Management

Resolve Problems

Emergency Response to Malware (viruses, worms, Spyware, spam) attacks

Continuous Improvement

- *Monitor User Identity and Authorization Process*
- *Post incident response reviews*

Measure Results

Example
DS5: Ensure Systems Security

Business Objective (Goal)

Define Strategy

Maintain Enterprise reputation and Leadership

IT Objective (Goal)

Create Value

Trusted automated business Transactions and Information exchanges

Preserve Value

Ensure that IT services can resist and recover from attacks

IT Process Objective (Goal)

Good Things Happening

Optimize authorized access to information, applications & infrastructure

Bad Things Not Happening

Prevent, Detect & Resolve Attacks through Unauthorized access

IT Activity Goal or Control Objective

Exploit Opportunities

Effective, Efficient & Standardized User Identity and Authorization Management

Resolve Problems

Emergency Response to Malware (viruses, worms, Spyware, spam) attacks

Continuous Improvement

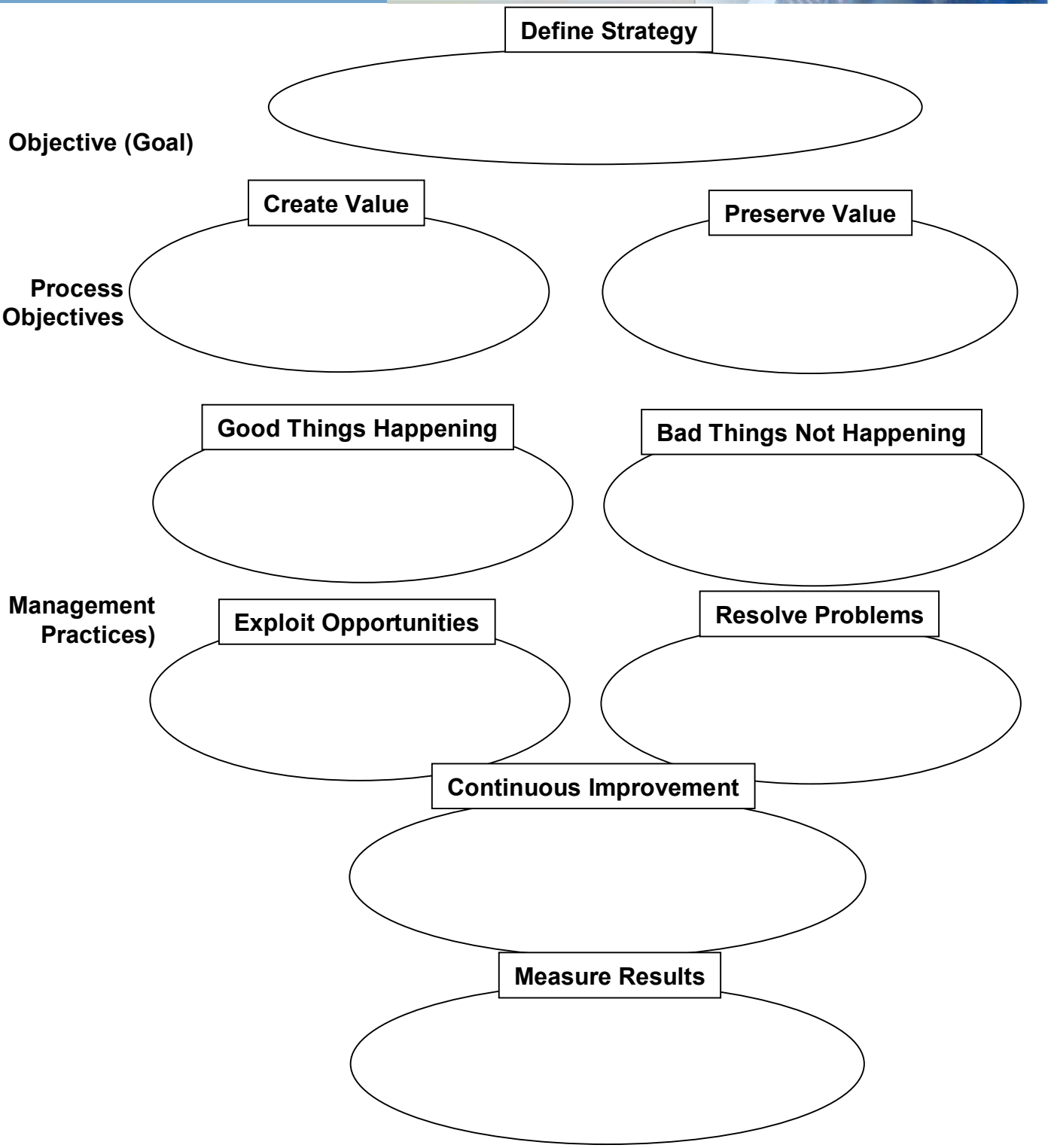
- *Monitor User Identity and Authorization Process*
- *Post incident response reviews*

Measure Results

- *Time to grant, change or remove access privileges*
- *# of incidents with business impact*

Now it is your turn

- Start with CobiT Quickstart
- Expand focus and direction with CobiT 4.1


Define Strategy
Objective (Goal)
Create Value
Preserve Value
Process Objectives
Good Things Happening
Bad Things Not Happening
Management Practices)
Exploit Opportunities
Resolve Problems
Continuous Improvement
Measure Results

(PO5 Manage the IT Investment)

Business Objective (Goal)

Define Strategy

Provide transparency and accountability into Total-cost-of-ownership to realize business benefits

IT Objective (Goal)

Create Value

Create measurable benefits and metrics

Preserve Value

Availability of the service defined by the business need
Prevent unauthorized spending

IT Process Objective (Goal)

Good Things Happening

Monitoring, tracking and Improving IT strategy and Investment decisions

Bad Things Not Happening

No interruption of service

IT Activity Goal or Control Objective

Exploit Opportunities

Prioritize Investment decisions

Resolve Problems

Continuous Improvement

Impact of prioritized Investment decisions can be Continuously improved through Cost and investment management

Measure Results

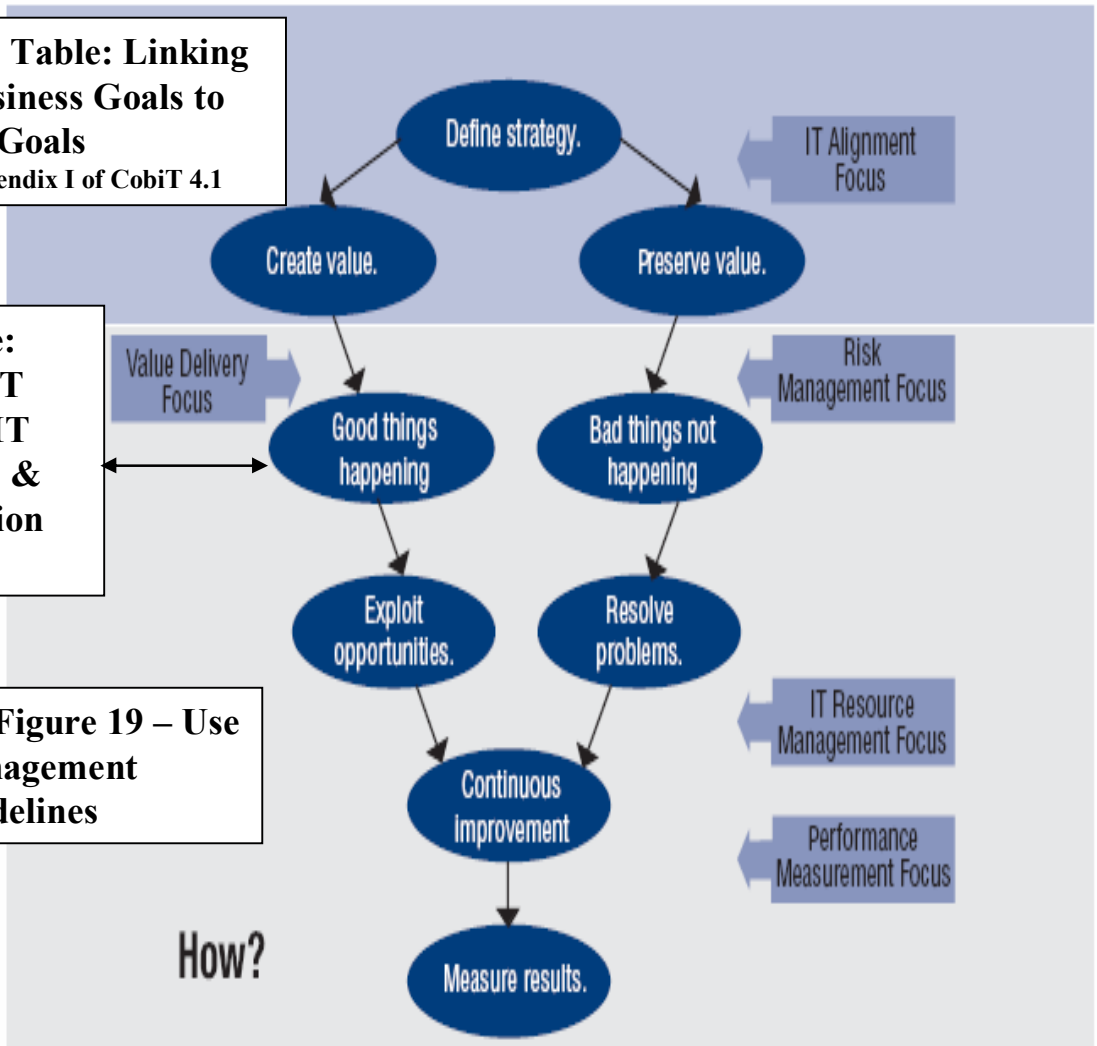
Quantitatively tracked variances Of costs and benefits

References

See Table: Linking Business Goals to IT Goals
Appendix I of CobiT 4.1

See Table: Linking IT Goals to IT Processes & Information Criteria

See Figure 19 – Use Management Guidelines



Linking Business Goals to IT Goals & Information Criteria

			IT Goals						Information Criteria						
	BUSINESS GOALS								Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial perspective	1 Expand the customer base	25	28						✓	✓					
	2 Increase revenue	25	28						✓	✓					
	3 Improve investment return	24								✓					
	4 Optimise asset utilisation	14							✓	✓					
	5 Manage business risk	2	17	17	18	20	20	21 22			✓	✓	✓		
Customer perspective	6 Improve customer orientation and service	3	20						✓						
	7 Offer continuously improved products and services	5	24						✓	✓					
	8 Service availability	10	16	22	23								✓		
	9 Agility in responding to changing business requirements (time to market)	1	5	25					✓	✓					
	10 Cost optimisation of service delivery	7	8	10	24					✓					
Internal perspective	11 Automation of business processes	6	7	8	11				✓	✓					
	12 Improve and maintain business process functionality	6	7	11					✓						
	13 Lower process costs	7	8	13	15	24				✓					
	14 Compliance with external laws and regulations	2	19	20	21	22	26	27			✓			✓	
	15 Transparency	2	18												✓
	16 Compliance with internal policies	2	13								✓			✓	
	17 Improve and maintain operational and staff productivity	7	8	11	13				✓	✓					
Learning and growth perspective	18 Product/business innovation	5	25	28					✓						
	19 Obtain reliable and useful information for strategic decision making	2	4	12	20	26									✓
	20 Acquire and maintain skilled and motivated personnel	9							✓	✓					

Linking IT Goals to COBIT Processes & Information Criteria

	IT GOALS	Processes								Information Criteria					
										Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Position IT as business-driven and aligned with the business strategy	PO1	PO2	PO3 PO10	AI1	AI2 AI7 DS1	DS9	Val1		✓			✓	✓		
2	Respond to governance requirements in line with board direction	PO1	PO4	PO17 ME1	ME3					✓	✓	✓			✓	✓
3	Ensure satisfaction of end users with service offerings and service levels	PO1	AI4	DS1 DS2	DS7	DS8 DS10 DS11				✓						
4	Optimise use of information	PO2	DS11								✓		✓			
5	IT agility	PO2	PO4	PO7 AI2							✓					
6	Define how business functional and control requirements are translated in effective and efficient automated solutions	AI1	AI2	AI6						✓	✓					
7	Acquire and maintain integrated and standardised application systems	PO3	AI2	AI5		AI3	AI5			✓	✓		✓			
8	Acquire and maintain an integrated and standardised IT infrastructure	AI3	AI5							✓	✓		✓			
9	Acquire and maintain IT skills that respond to the IT strategy	PO7	AI5							✓	✓		✓			
10	Ensure mutual satisfaction of third-party relationships	DS2								✓	✓					
11	Seamlessly integrate applications and technology solutions into business processes	PO3	AI4	AI7						✓			✓	✓		
12	Transparency and understanding of IT cost, benefits, strategy, policies and service levels	PO5	PO6	DS1 DS2	DS6	ME1 ME3				✓	✓			✓	✓	
13	Ensure proper use and performance of the applications and technology solutions	PO1	AI4	AI7 DS7	DS8					✓	✓		✓	✓		
14	Account for and protect all IT assets	PO9	DS5	DS9 DS12	ME2						✓			✓		
15	Optimise the IT infrastructure, resources and capabilities	PO3	AI3	DS1 DS7	DS9						✓					
16	Reduce solution and service delivery defects and rework	PO2	AI4	AI6 AI7	DS10					✓	✓		✓	✓		
17	Enhance the achievement of IT objectives	PO1	D-III	P-II						✓	✓	✓	✓	✓	✓	✓
18	Establish clarity of business impact of risks to IT objectives and resources	PO9								✓		✓	✓	✓		
19	Ensure critical and confidential information is withheld from those who should not have access to it	PO7	DS5	DS11 DS12								✓			✓	
20	Ensure automated business transactions and information exchange can be trusted	PO8	AI7	DS5									✓			
21	Ensure IT services and the IT infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster	PO9	DS4	DS5 DS12	DS13	ME2				✓				✓		
22	Ensure minimum business impact in the event of an IT service disruption or change	PO7	AI6	DS4 DS10						✓				✓		
23	Make sure that IT services and infrastructure are available as required	DS3	DS4	DS8 DS13	DS15					✓				✓		
24	Improve IT cost-efficiency and its contribution to business profitability	PO5	AI5	DS7							✓					
25	Deliver projects on time and on budget, meeting quality standards	PO8	PO10							✓	✓					
26	Maintain the integrity of information and processing infrastructure	AI3	DS5										✓			
27	Ensure IT compliance with laws and regulations	DS11	ME2	ME3 ME4											✓	
28	IT demonstrated cost and efficiency savings driven by continuous improvement and readiness for future change	PO5	DS6	DS1 ME3												✓

Recap – Report out

Lunch

- Look to the IT Archetype? Yes!
- Google search on IT archetypes.

Closing the Loop from Audit findings to Strategic Action

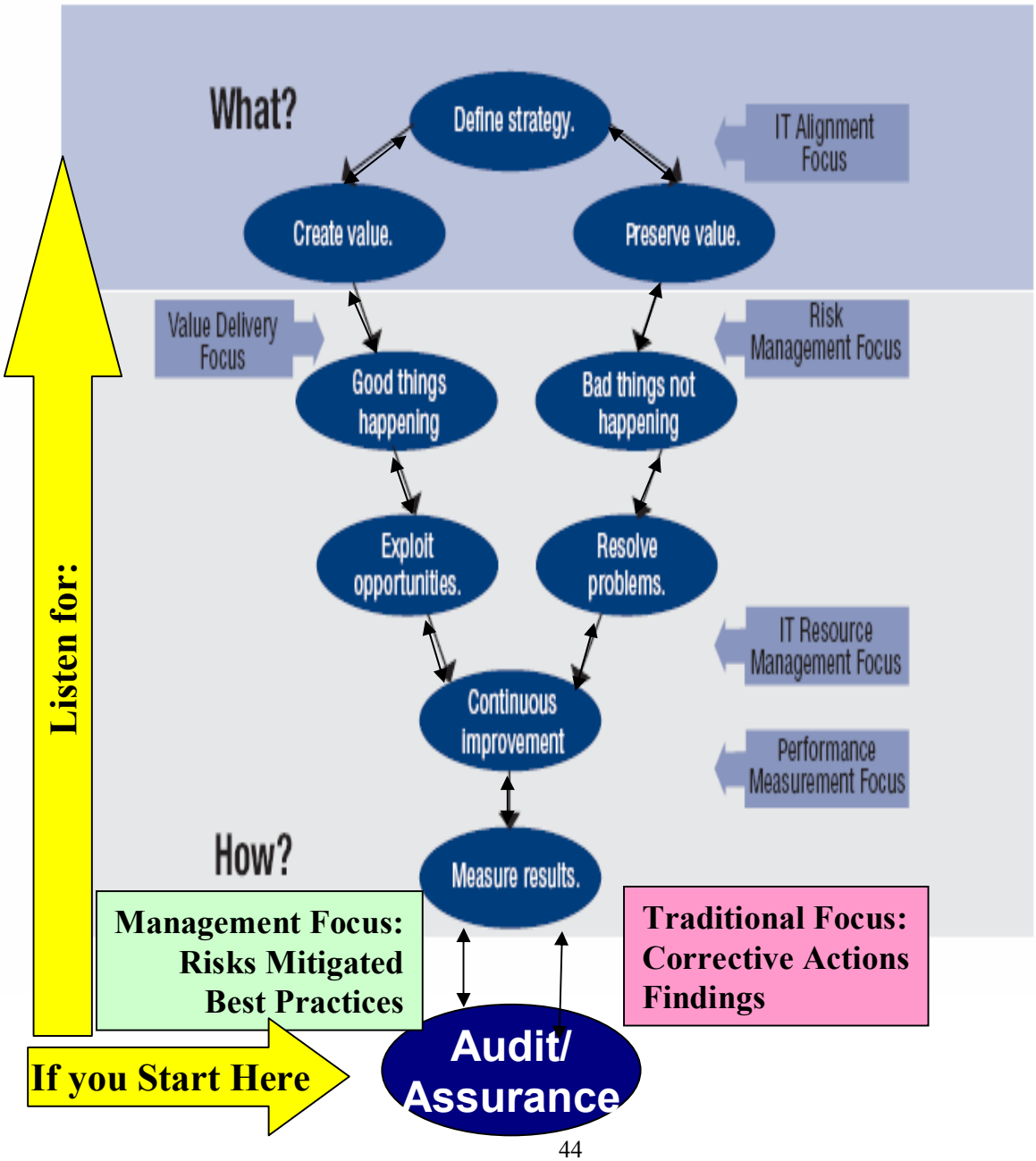
Reversing the Control Flows

When performing Audit/Assurance, connect findings with observed Measured Results and Continuous Improvement Successes. Add Value Delivered to Risks Managed Messages

Translating Observations into persuasive Communications

Value Delivery (Value Creation)

Figure 7—Two Views of Control



Use CobiT to translate Audit Findings & Observations into Persuasive Communications

Management Messages
Risks Mitigated
Best Practices

Audit/Assurance Messages
Corrective Actions
Findings

Listen/Look for:

- Business & IT Objectives
  - Resources
  - Information Criteria
- Quality Objectives
- Risk Management Objectives
- CobiT Control Objectives
- Improvement Initiatives

Continuous Improvement

Measure Results

Strategy & Tactics
Plans & Objectives
Role/Responsibilities
Policy/Process/SOP's

Monitor and Evaluate

Plan & Organize

Metrics

Control +/- 80% IT resources

Deliver and Support

Acquire and Implement

PMBOK Prince2

ITIL

CMMI

Risks Mitigated
Best Practices

Corrective Actions
Findings

Audit/ Assurance

Template to collect Management Messages in Audit/Assurance Visit:

Business Objective (Goal)

Define Strategy

IT Objective (Goal)

Create Value

Preserve Value

IT Process Objective (Goal)

Good Things Happening

Bad Things Not Happening

IT Activity Goal or Control Objective

Exploit Opportunities

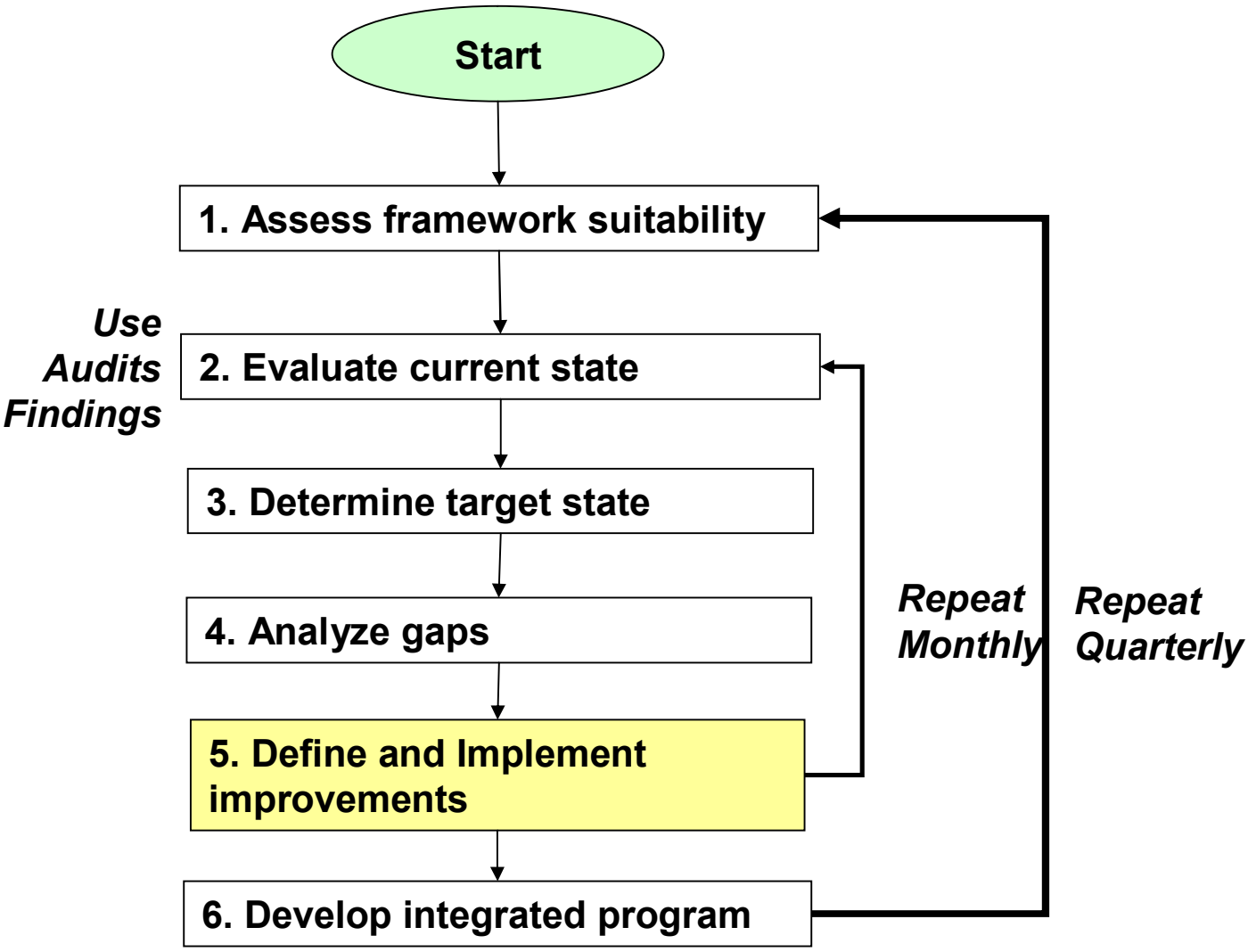
Resolve Problems

Continuous Improvement

Measure Results

Audit/Assurance Scope

Systematic approach to Implementing Improvement



See Quickstart Page 21

For more robust guidance see
IT Governance Implementation Guide, 2nd edition

Quickstart on Assessing Suitability

- CD & see pgs 17 & 18

Evaluate current state Self-Assessment

- CD – CobiT Quickstart see page 19 & 20 for instructions

Review with Burning Questions

- What's after SOX?
  - ISO 9001 + Privacy/Security + Financial Controls
- Global/International Standard for a framework?

Thank You

For more information, please see

www.isaca.org

www.itgi.org

Speaker Contact information

debra.mallette@kp.org

Cell phone: 510-295-3217