Kendall Tieck,
Audit Director
Microsoft Corporation

AUDITING IT GOVERNANCE: LEVERAGING COBIT 4.0

9/17/2007

Microsoft
Your potential. Our passion.™

Topics of Discussion

- Why audit IT Governance?
- Is this an IT audit?
- Where to start…
- CobiT 4.0 (A very good place to start)
- Navigating
- Building the approach to the audit

Enterprise Governance

Governance: The method by which an organization is directed, administered or controlled

IT Governance

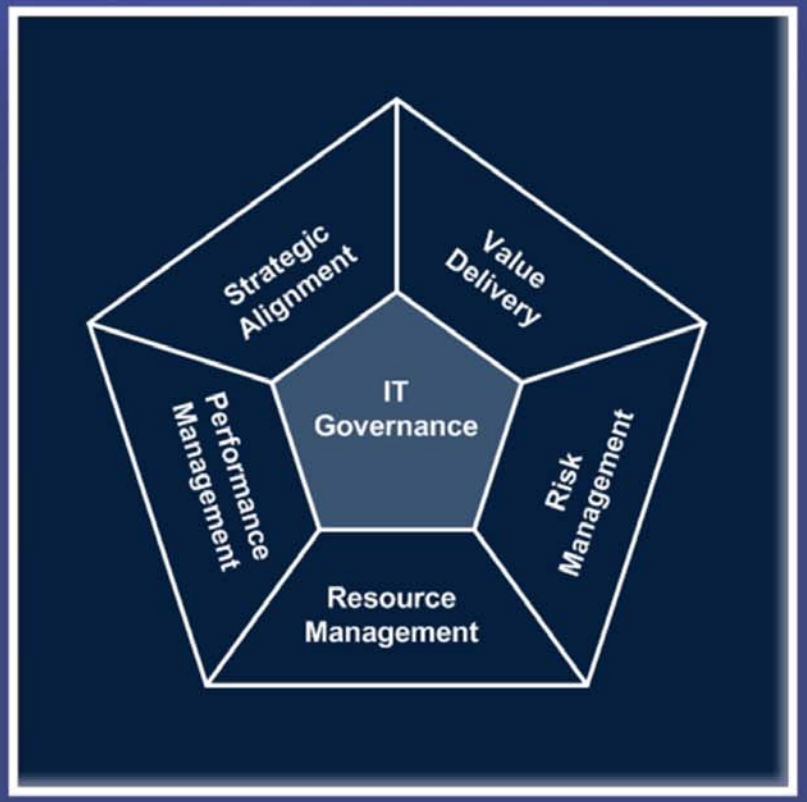
IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

Cobit and IT Governace

CobiT supports IT governance by providing a framework to ensure that:

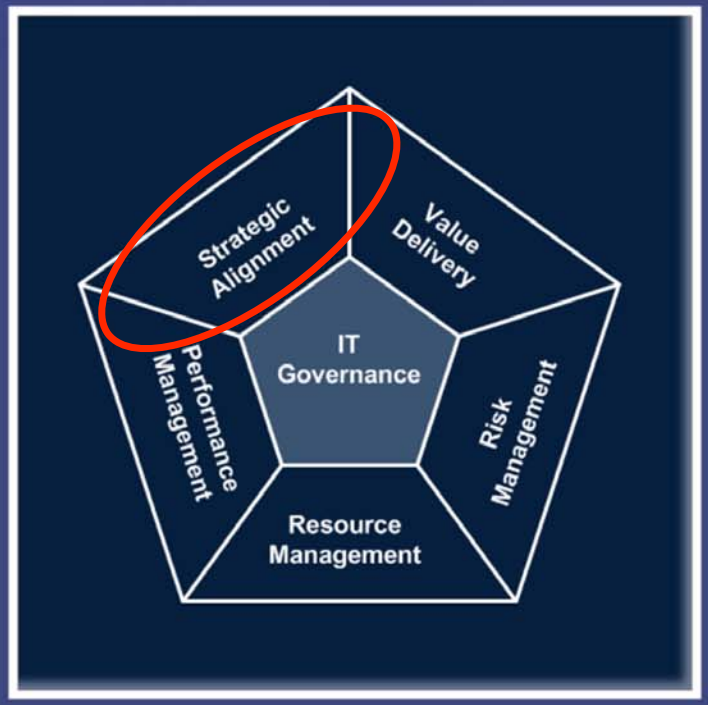
- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

IT Governance Focus Areas



Strategic Alignment

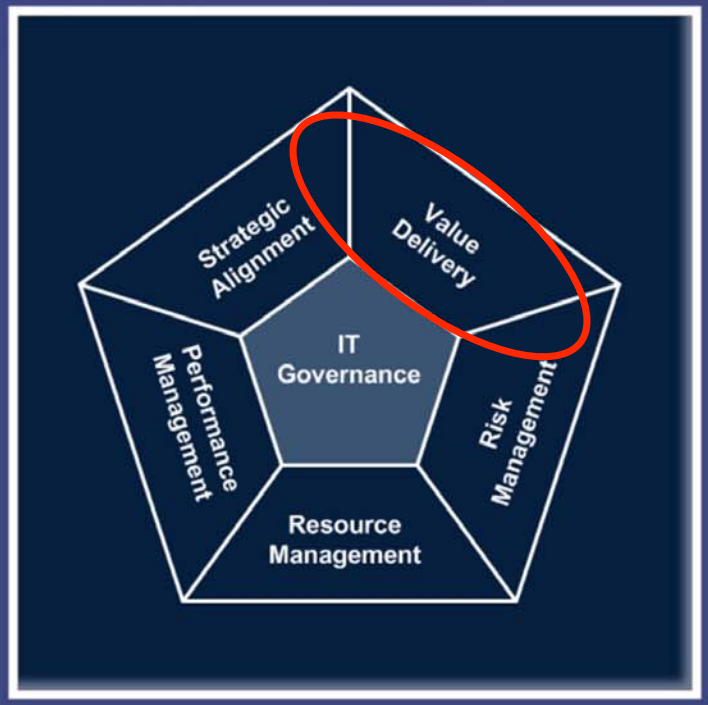
Strategic alignment focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.



Microsoft
Your potential. Our passion.™

Value Delivery

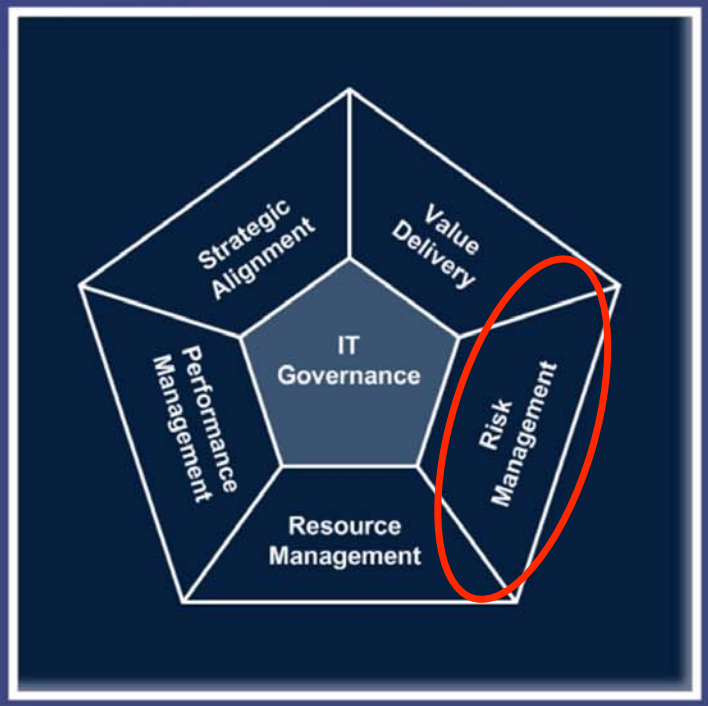
Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.



Microsoft
Your potential. Our passion.™

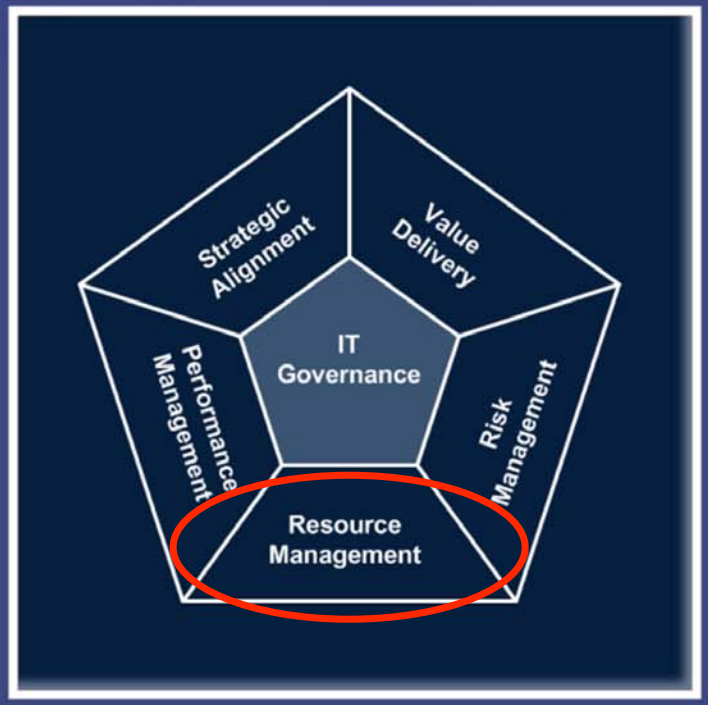
Risk Management

Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.



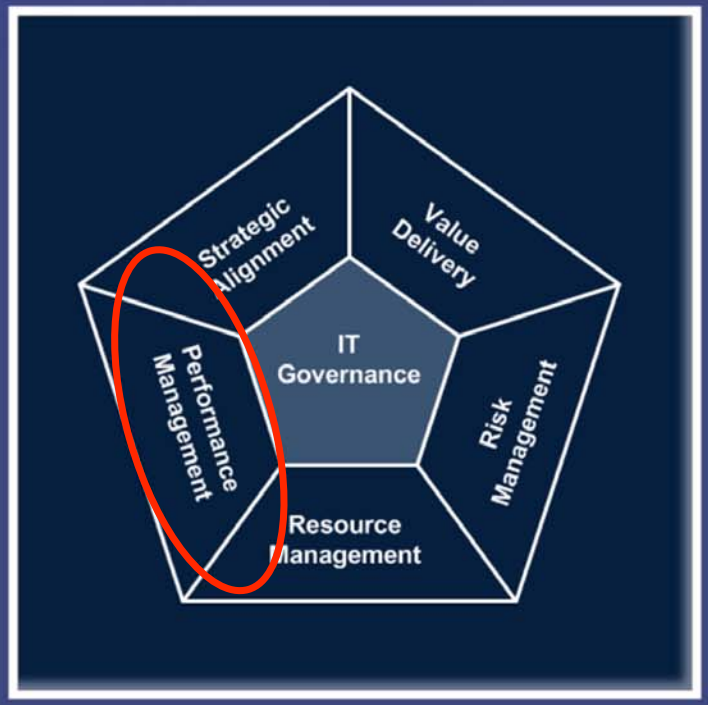
Resource Management

Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.



Performance Management

Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.



Microsoft
Your potential. Our passion.™

CobiT 4.0 Domains

Plan and Organize

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organization as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

Plan and Organize

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organization understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

Acquire and Implement

To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

Acquire and Implement

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

Deliver and Support

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

Deliver and Support

- Are IT services being delivered in line with business priorities?
- Are IT costs optimized?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

Monitor and Evaluate

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

Monitor and Evaluate

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance and performance measured and reported?

CobiT Control Objectives Mapped to IT Governance Focus Areas

		(IMPORTANCE)	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Plan and Organize							
PO 1	Define a strategic plan	H	P		S	S	
PO 2	Define the information architecture	L	P	S	P	S	
PO 3	Determine technological direction	M	S	S	P	S	
PO 4	Define the IT processes, organization, and relationships	L	S		P	P	
PO 5	Manage the IT investment	M	S	P	S		S
PO 6	Communicate management aims and direction	M	P			P	
PO 7	Manage IT human resources	L	P		P	S	S
PO 8	Manage quality	M	P	S		S	
PO 9	Assess and manage IT risks	H	P			P	
PO 10	Manage projects	H	P	S	S	S	S

CobiT Control Objectives Mapped to IT Governance Focus Areas

		(IMPORTANCE)	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Acquire and Implement							
AI 1	Identify automated solutions	M	P	P	S	S	
AI 2	Acquire and maintain application software	M	P	P		S	
AI 3	Acquire and maintain technology infrastructure	L			P		
AI 4	Enable operation and use	L	S	P	S	S	
AI 5	Procure IT resources	M		S	P		
AI 6	Manage changes	H		P	S		
AI 7	Install and accredit solutions and changes	M	S	P	S	S	S

CobiT Control Objectives Mapped to IT Governance Focus Areas

		(IMPORTANCE)	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Deliver and Support							
DS 1	Define and manage service levels	M	P	P	P		P
DS 2	Manage third party services	L		P	S	P	S
DS 3	Manage performance and capacity	L	S	S	P	S	S
DS 4	Ensure continuous service	M	S	P	S	P	S
DS 5	Ensure systems security	H				P	
DS 6	Identify and allocate costs	L		S	P		S
DS 7	Educate and train users	L	S	P		S	
DS 8	Manage service desk and incidents	L	S	P			S
DS 9	Manage the configuration	M		P		S	
DS 10	Manage Problems	M		P		S	
DS 11	Manage data	H		P	P	P	
DS 12	Manage the physical environment	L			S	P	
DS 13	Manage operations	L			P		

CobiT Control Objectives Mapped to IT Governance Focus Areas

		(IMPORTANCE)	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Monitor and Evaluate							
ME 1	Monitor and evaluate IT performance	H					P
ME 2	Monitor and evaluate internal control	M		P		P	
ME 3	Ensure regulatory compliance	H	P			P	
ME 4	Provide IT governance	H	P	P	P	P	P

Strategic Focus

Plan and Organize		
PO 1	Define a strategic plan	P
PO 2	Define the information architecture	P
PO 6	Communicate management aims and direction	P
PO 7	Manage IT human resources	P
PO 8	Manage quality	P
PO 9	Assess and manage IT risks	P
PO 10	Manage projects	P
Acquire and Implement		
AI 1	Identify automated solutions	P
AI 2	Acquire and maintain application software	P
Deliver and Support		
DS 1	Define and manage service levels	P
Monitor and Evaluate		
ME 3	Ensure regulatory compliance	P
ME 4	Provide IT governance	P

Value Delivery

Plan and Organize		
PO 5	Manage the IT investment	P
Acquire and Implement		
AI 1	Identify automated solutions	P
AI 2	Acquire and maintain application software	P
AI 4	Enable operation and use	P
AI 6	Manage changes	P
AI 7	Install and accredit solutions and changes	P
Deliver and Support		
DS 1	Define and manage service levels	P
DS 2	Manage third party services	P
DS 4	Ensure continuous service	P
DS 7	Educate and train users	P
DS 8	Manage service desk and incidents	P
DS 9	Manage the configuration	P
DS 10	Manage Problems	P
DS 11	Manage data	P
Monitor and Evaluate		
ME 2	Monitor and evaluate internal control	P
ME 4	Provide IT governance	P

Resource Management

Plan and Organize		
PO 2	Define the information architecture	P
PO 3	Determine technological direction	P
PO 4	Define the IT processes, organization, and relationships	P
PO 7	Manage IT human resources	P
Acquire and Implement		
AI 3	Acquire and maintain technology infrastructure	P
AI 5	Procure IT resources	P
Deliver and Support		
DS 1	Define and manage service levels	P
DS 3	Manage performance and capacity	P
DS 6	Identify and allocate costs	P
DS 11	Manage data	P
DS 13	Manage operations	P
Monitor and Evaluate		
ME 4	Provide IT governance	P

Risk Management

Plan and Organize		
PO 4	Define the IT processes, organization, and relationships	P
PO 6	Communicate management aims and direction	P
PO 9	Assess and manage IT risks	P
Acquire and Implement		
Deliver and Support		
DS 2	Manage third party services	P
DS 4	Ensure continuous service	P
DS 5	Ensure systems security	P
DS 11	Manage data	P
DS 12	Manage the physical environment	P
Monitor and Evaluate		
ME 2	Monitor and evaluate internal control	P
ME 3	Ensure regulatory compliance	P
ME 4	Provide IT governance	P

Performance Management

Plan and Organize		
PO 5	Manage the IT investment	S
PO 7	Manage IT human resources	S
PO 10	Manage projects	S

Acquire and Implement		
AI 7	Install and accredit solutions and changes	S

Deliver and Support		
DS 1	Define and manage service levels	P
DS 2	Manage third party services	S
DS 3	Manage performance and capacity	S
DS 4	Ensure continuous service	S
DS 6	Identify and allocate costs	S
DS 8	Manage service desk and incidents	S

Monitor and Evaluate		
ME 1	Monitor and evaluate IT performance	P
ME 4	Provide IT governance	P

Two Conceptual Approaches

- **Integrated Audit Approach**: Every audit you conduct addresses key components of IT Governance. Over time you may be able to assess the overall effectiveness of IT Governance.

- **Targeted IT Governance**: Develop a series of targeted audits that together allow a comprehensive assessment of the effectiveness of IT Governance.

Identifying the Approach

Assess Current Audit Knowledge

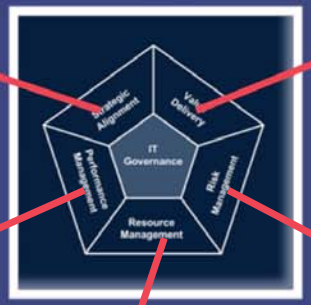
Identify Gaps

Assess the Risk to Business Objectives

Define Scope and Objectives

Is there recent audit work or other data that can inform your assessment of the quality of controls?

Plan and Organize		
PO 1	Define a strategic plan	P
PO 2	Define the information architecture	P
PO 6	Communicate management aims and direction	P
PO 7	Manage IT human resources	P
PO 8	Manage quality	P
PO 9	Assess and manage IT risks	P
PO 10	Manage projects	P
Acquire and Implement		
AI 1	Identify automated solutions	P
AI 2	Acquire and maintain application software	P
Deliver and Support		
DS 1	Define and manage service levels	P
Monitor and Evaluate		
ME 3	Ensure regulatory compliance	P
ME 4	Provide IT governance	P



Plan and Organize		
PO 5	Manage the IT investment	P
Acquire and Implement		
AI 1	Identify automated solutions	P
AI 2	Acquire and maintain application software	P
AI 4	Enable operation and use	P
AI 6	Manage changes	P
AI 7	Install and accredit solutions and changes	P
Deliver and Support		
DS 1	Define and manage service levels	P
DS 2	Manage third party services	P
DS 4	Ensure continuous service	P
DS 7	Educate and train users	P
DS 8	Manage service desk and incidents	P
DS 9	Manage the configuration	P
DS 10	Manage Problems	P
DS 11	Manage data	P
Monitor and Evaluate		
ME 2	Monitor and evaluate internal control	P
ME 4	Provide IT governance	P

Plan and Organize		
PO 5	Manage the IT investment	S
PO 7	Manage IT human resources	S
PO 10	Manage projects	S
Acquire and Implement		
AI 7	Install and accredit solutions and changes	S
Deliver and Support		
DS 1	Define and manage service levels	P
DS 2	Manage third party services	S
DS 3	Manage performance and capacity	S
DS 4	Ensure continuous service	S
DS 6	Identify and allocate costs	S
DS 8	Manage service desk and incidents	S
Monitor and Evaluate		
ME 1	Monitor and evaluate IT performance	P
ME 4	Provide IT governance	P

Plan and Organize		
PO 2	Define the information architecture	P
PO 3	Determine technological direction	P
PO 4	Define the IT processes, organization, and relationships	P
PO 7	Manage IT human resources	P
Acquire and Implement		
AI 3	Acquire and maintain technology infrastructure	P
AI 5	Procure IT resources	P
Deliver and Support		
DS 1	Define and manage service levels	P
DS 3	Manage performance and capacity	P
DS 6	Identifhy and allocate costs	P
DS 11	Manage data	P
DS 13	Manage operations	P
Monitor and Evaluate		
ME 4	Provide IT governance	P

Plan and Organize		
PO 4	Define the IT processes, organization, and relationships	P
PO 6	Communicate management aims and direction	P
PO 9	Assess and manage IT risks	P
Acquire and Implement		
Deliver and Support		
DS 2	Manage third party services	P
DS 4	Ensure continuous service	P
DS 5	Ensure systems security	P
DS 11	Manage data	P
DS 12	Manage the physical environment	P
Monitor and Evaluate		
ME 2	Monitor and evaluate internal control	P
ME 3	Ensure regulatory compliance	P
ME 4	Provide IT governance	P

Microsoft
Your potential. Our passion.™

Assess Current Audit Knowledge

Identify Gaps

Assess the Risk to Business Objectives

Define Scope and Objectives

Is there recent audit work or other data that can inform your assessment of the quality of controls?

CobiT Control Objectives Mapped to IT Governance Focus Areas		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Audit Knowledge
Plan and Organize							
PO 1	Define a strategic plan	P		S	S		
PO 2	Define the information architecture	P	S	P	S		
PO 3	Determine technological direction	S	S	P	S		
PO 4	Define the IT processes, organization, and relationships	S		P	P		
PO 5	Manage the IT investment	S	P	S		S	
PO 6	Communicate management aims and direction	P			P		
PO 7	Manage IT human resources	P		P	S	S	
PO 8	Manage quality	P	S		S		
PO 9	Assess and manage IT risks	P			P		
PO 10	Manage projects	P	S	S	S	S	
Acquire and Implement							
AI 1	Identify automated solutions	P	P	S	S		
AI 2	Acquire and maintain application software	P	P		S		
AI 3	Acquire and maintain technology infrastructure			P			
AI 4	Enable operation and use	S	P	S	S		
AI 5	Procure IT resources		S	P			
AI 6	Manage changes		P	S			
AI 7	Install and accredit solutions and changes	S	P	S	S	S	
Deliver and Support							
DS 1	Define and manage service levels	P	P	P		P	
DS 2	Manage third party services		P	S	P	S	
DS 3	Manage performance and capacity	S	S	P	S	S	
DS 4	Ensure continuous service	S	P	S	P	S	
DS 5	Ensure systems security				P		
DS 6	Identify and allocate costs		S	P		S	
DS 7	Educate and train users	S	P		S		
DS 8	Manage service desk and incidents	S	P			S	
DS 9	Manage the configuration		P		S		
DS 10	Manage Problems		P		S		
DS 11	Manage data		P	P	P		
DS 12	Manage the physical environment			S	P		
DS 13	Manage operations			P			
Monitor and Evaluate							
ME 1	Monitor and evaluate IT performance					P	
ME 2	Monitor and evaluate internal control		P		P		
ME 3	Ensure regulatory compliance	P			P		
ME 4	Provide IT governance	P	P	P	P	P	

Audit Knowledge

Microsoft
Your potential. Our passion.™

Assess Current Audit Knowledge → **Identify Gaps** → Assess the Risk to Business Objectives → Define Scope and Objectives

CobiT Control Objectives Mapped to IT Governance Focus Areas		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Audit Knowledge
Plan and Organize							
PO 1	Define a strategic plan	P		S	S		1
PO 2	Define the information architecture	P	S	P	S		1
PO 3	Determine technological direction	S	S	P	S		2
PO 4	Define the IT processes, organization, and relationships	S		P	P		3
PO 5	Manage the IT investment	S	P	S		S	3
PO 6	Communicate management aims and direction	P			P		2
PO 7	Manage IT human resources	P		P	S	S	4
PO 8	Manage quality	P	S		S		3
PO 9	Assess and manage IT risks	P			P		2
PO 10	Manage projects	P	S	S	S	S	3
Acquire and Implement							
AI 1	Identify automated solutions	P	P	S	S		4
AI 2	Acquire and maintain application software	P	P		S		4
AI 3	Acquire and maintain technology infrastructure			P			4
AI 4	Enable operation and use	S	P	S	S		4
AI 5	Procure IT resources		S	P			3
AI 6	Manage changes		P	S			4
AI 7	Install and accredit solutions and changes	S	P	S	S	S	2
Deliver and Support							
DS 1	Define and manage service levels	P	P	P		P	2
DS 2	Manage third party services		P	S	P	S	2
DS 3	Manage performance and capacity	S	S	P	S	S	2
DS 4	Ensure continuous service	S	P	S	P	S	4
DS 5	Ensure systems security				P		4
DS 6	Identify and allocate costs		S	P		S	2
DS 7	Educate and train users	S	P		S		2
DS 8	Manage service desk and incidents	S	P			S	4
DS 9	Manage the configuration		P		S		4
DS 10	Manage Problems		P		S		4
DS 11	Manage data		P	P	P		4
DS 12	Manage the physical environment			S	P		4
DS 13	Manage operations			P			4
Monitor and Evaluate							
ME 1	Monitor and evaluate IT performance					P	2
ME 2	Monitor and evaluate internal control		P		P		2
ME 3	Ensure regulatory compliance	P			P		4

Highlight the areas that represent gaps in audit knowledge.

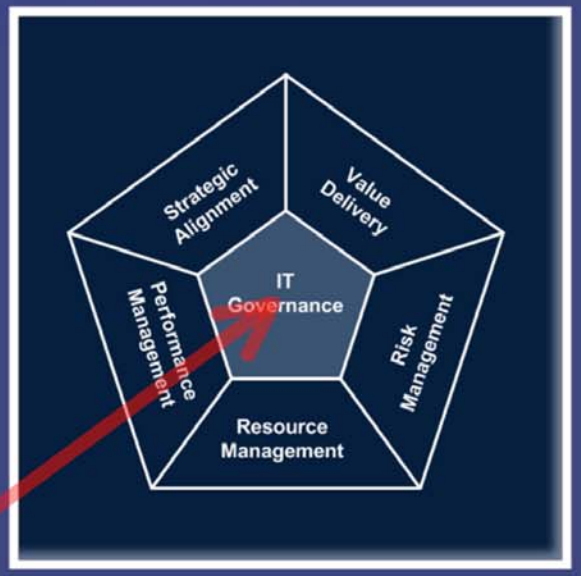
Assess Current Audit Knowledge → Identify Gaps → **Assess the Risk to Business Objectives** → Define Scope and Objectives

CobiT Control Objectives Mapped to IT Governance Focus Areas		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Audit Knowledge	Impact	Likelihood	Total Risk Rating
Plan and Organize										
PO 1	Define a strategic plan	P		S	S		1			
PO 2	Define the information architecture	P	S	P	S		1			
PO 3	Determine technological direction	S	S	P	S		2			
PO 6	Communicate management aims and direction	P			P		2			
PO 9	Assess and manage IT risks	P			P		2			
Acquire and Implement										
AI 7	Install and accredit solutions and changes	S	P	S	S	S	2			
Deliver and Support										
DS 1	Define and manage service levels	P	P	P		P	2			
DS 2	Manage third party services		P	S	P	S	2			
DS 3	Manage performance and capacity	S	S	P	S	S	2			
DS 6	Identify and allocate costs		S	P		S	2			
DS 7	Educate and train users	S	P		S		2			
Monitor and Evaluate										
ME 1	Monitor and evaluate IT performance					P	2			
ME 2	Monitor and evaluate internal control		P		P		2			

Based on the gap analysis, assess the high level risk to the business.

Assess Current Audit Knowledge → Identify Gaps → Assess the Risk to Business Objectives → Define Scope and Objectives

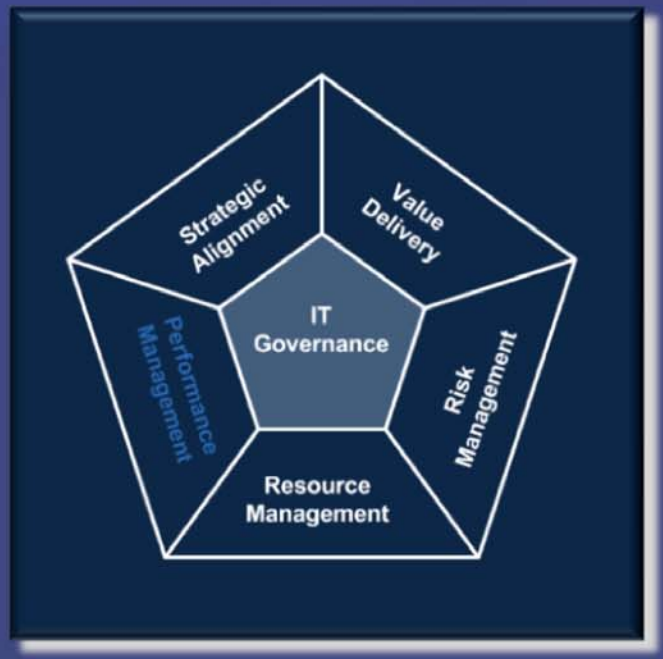
CobiT Control Objectives Mapped to IT Governance Focus Areas		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Audit Knowledge	Impact	Likelihood	Total Risk Rating
Plan and Organize										
PO 1	Define a strategic plan	P		S	S		1			
PO 2	Define the information architecture	P	S	P	S		1			
PO 3	Determine technological direction	S	S	P	S		2			
PO 6	Communicate management aims and direction	P			P		2			
PO 9	Assess and manage IT risks	P			P		2			
Acquire and Implement										
AI 7	Install and accredit solutions and changes	S	P	S	S	S	2			
Deliver and Support										
DS 1	Define and manage service levels	P	P	P		P	2			
DS 2	Manage third party services		P	S	P	S	2			
DS 3	Manage performance and capacity	S	S	P	S	S	2			
DS 6	Identify and allocate costs		S	P		S	2			
DS 7	Educate and train users	S	P		S		2			
Monitor and Evaluate										
ME 1	Monitor and evaluate IT performance					P	2			
ME 2	Monitor and evaluate internal control		P		P		2			
IT Governance Focus Weight		14	14	13	13	7				



Microsoft
Your potential. Our passion.™

Assess Current Audit Knowledge → Identify Gaps → Assess the Risk to Business Objectives → Define Scope and Objectives

CobiT Control Objectives Mapped to IT Governance Focus Areas		Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Total Risk Rating
Plan and Organize							
PO 1	Define a strategic plan	P		S	S		25
PO 2	Define the information architecture	P	S	P	S		22
PO 3	Determine technological direction	S	S	P	S		15
PO 6	Communicate management aims and direction	P			P		18
PO 9	Assess and manage IT risks	P			P		35
Acquire and Implement							
AI 7	Install and accredit solutions and changes	S	P	S	S	S	15
Deliver and Support							
DS 1	Define and manage service levels	P	P	P		P	28
DS 2	Manage third party services		P	S	P	S	12
DS 3	Manage performance and capacity	S	S	P	S	S	32
DS 6	Identify and allocate costs		S	P		S	16
DS 7	Educate and train users	S	P		S		12
Monitor and Evaluate							
ME 1	Monitor and evaluate IT performance					P	20
ME 2	Monitor and evaluate internal control		P		P		25
IT Governance Focus Weight		14	14	13	13	7	



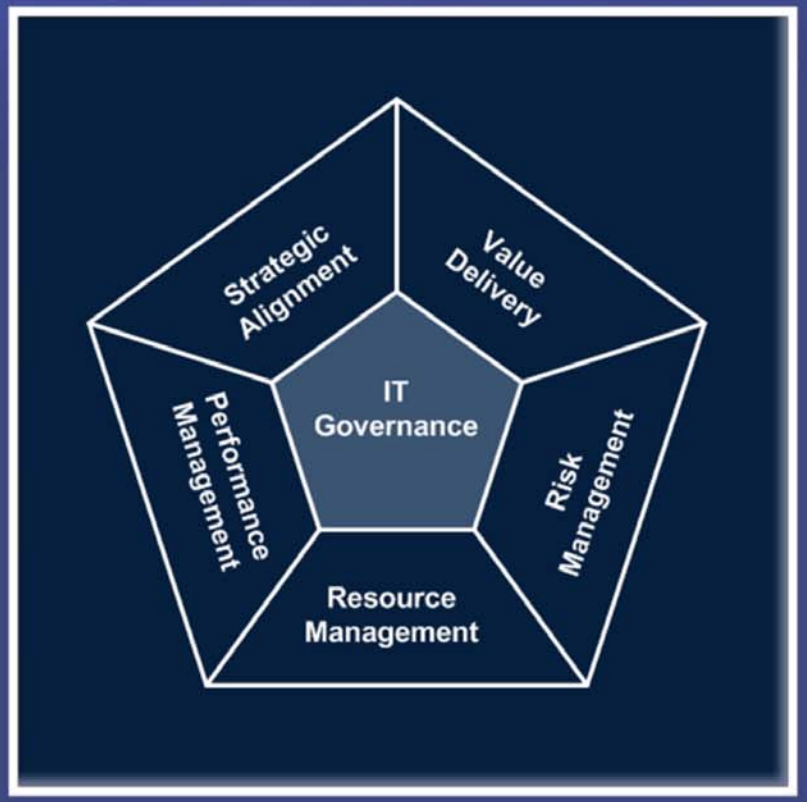
Microsoft
Your potential. Our passion.™

IT Governance Favorites		(IMPORTANCE)	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement
Plan and Organize							
PO 1	Define a strategic plan	H	P		S	S	
PO 2	Define the information architecture	L	P	S	P	S	
PO 3	Determine technological direction	M	S	S	P	S	
PO 5	Manage the IT investment	M	S	P	S		S
PO 6	Communicate management aims and direction	M	P			P	
PO 9	Assess and manage IT risks	H	P			P	
Deliver and Support							
DS 1	Define and manage service levels	M	P	P	P		P
DS 6	Identify and allocate costs	L		S	P		S
Monitor and Evaluate							
ME 1	Monitor and evaluate IT performance	H					P
ME 2	Monitor and evaluate internal control	M		P		P	
ME 3	Ensure regulatory compliance	H	P			P	
ME 4	Provide IT governance	H	P	P	P	P	P

Parting thought…

Leverage Cobit 4.0 to arrive at an approach to audit IT Governance.

We can audit the box to death, but without effective IT Governance the business will not achieve full potential.



Microsoft
Your potential. Our passion.™

Thank you !