APMG International

ISACA

TOP TIPS

Mark's COBIT and CGEIT 'hacks'

Mark Thomas, Escoute
CGEIT, CRISC, Certified COBIT Assessor

Mark's COBIT and CGEIT "hacks"

1. What's in it for me? Board/Executive Management.
2. What's in it for me? Middle Management.
3. What's in it for me? Analyst/Individual Contributor.
4. What's in it for me? Program/Project Management.
5. What's in it for me? Risk/Compliance.
6. What's in in it for me? Information Security.
7. Use COBIT as a means of adopting a tailorable governance framework in your organization.
8. Adopting GEIT in an environment that has little to no executive level support.
9. Making GEIT sustainable and continuous in an enterprise.
10. Tips and tricks to studying for the CGEIT and COBIT exams.

Hack #1: What's in it for me? Board/Executive Management

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
Holistic understanding of how all CGEIT domains relate to governing enterprise IT. Ability to recognize the distinction between governance and management. How to organize governing bodies, committees and boards.	Definition and purpose statements for ALL CGEIT domains. Task and knowledge statements relevant to specific roles.	Insights on how to gain value from I&T investments across the enterprise. Ability to identify monitoring and performance requirements for I&T.	Governance System Principles Governance Framework Principles Design Factors Governance Objectives in the EDM domain: EDM01, EDM02, EDM03, EDM04, EDM05 Management Objectives in the MEA domain: MEA01, MEA02, MEA03, MEA04 RACI charts for each objective

Hack #2: What's in it for me? Middle Management

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
Holistic understanding of how all CGEIT domains relate to managing enterprise IT. Ability to recognize the distinction between governance and management and how to organize processes and practices to support organizational goals. Specific tasks associated with each domain that can enhance the adoption of EGIT.	Definition and purpose statements for ALL CGEIT domains. Task and knowledge statements relevant to specific roles.	Guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities.	Governance Framework Principles Design Factors Management Objectives APO01, APO02, APO03, APO04, APO05, APO06, APO07, APO08, APO09, APO10, APO11, BAI01, BAI05, BAI06, BAI11, MEA01, MEA02, MEA03, MEA04 RACI charts for each objective

Hack #3: What's in it for me? Analyst/Individual Contributor

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
What specific tasks and knowledge areas are applicable. How to link specific responsibilities to the overall success of the enterprise.	All domains in CGEIT Task and knowledge statements for each domain	What practices and activities should be executed in order to support the overall value contribution of IT.	Determine the applicable governance or management objective is applicable to your role. Understand all components, practices, and activities in the objectives relevant to your role.

Hack #4: What's in it for me? Program/Project Management

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
How programs and projects fit into the overall strategic plans for the enterprise. How the key to overall benefits realization depends on adequate portfolio, program and project execution. The importance of an I&T investment business case and its lifecycle.	Domain 3, Benefits Realization Domain 4, Risk Optimization Domain 5, Resource Optimization	How to manage programs and projects in alignment with the investment portfolio and enterprise strategy. Develop a standard program and project management approach that results in consistent results. Manage program and project risk in alignment with the overall enterprise risk appetite guidance.	All governance components (focus on process) Management objectives: EDM03, EDM04, APO05, APO06, APO07, APO11, APO12, BAI01, BAI02, BAI05, BAI11

Hack #5: What's in it for me? Risk/Compliance

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
Recognize the enterprise risk appetite and tolerance levels and apply these to risk responses. Understand how to identify risk, analyze and assess risk, respond to risk, and report and monitor risk.	Domain 1, Framework for the governance and management of enterprise IT Domain 4, Risk Optimization	Ensure that the I&T related enterprise risk does not exceed the risk appetite and tolerance levels. Continually integrate the management of enterprise I&T related risk with enterprise risk management and balance the costs and benefits of managing those risks.	All governance components Governance objectives: EDM03 Management objectives: APO10, APO12, APO13, APO14, DSS05, DSS06, MEA01, MEA02, MEA03, MEA04 Design factors: Risk Profile, I&T Related Issues, Threat Landscape, Compliance Requirements Risk scenarios

Hack #6: What's in it for me? Information Security

CGEIT		COBIT	
WIIFM?	*Where to look*	*WIIFM?*	*Where to look*
Relate the enterprise information security posture to the overall risk appetite and tolerance guidance from Domain 4, Risk Optimization	Domain 2, Strategic Management Domain 3, Risk Optimization	Understand how to keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels. Recognize additional frameworks, bodies of knowledge and standards are applicable to the information security role.	All governance components Governance objectives: EDM03 Management objectives: APO10, APO12, APO13, APO14, DSS05, DSS06, MEA01, MEA02, MEA03, MEA04 Design factors: Risk Profile, Threat Landscape Risk scenarios

Hack #7: Use COBIT as a means of adopting a tailorable governance framework in your organization

CGEIT	COBIT
Domain 1, Framework for the governance and management of enterprise IT: Understand the various frameworks, bodies of knowledge and how they can be used in an overarching governance framework.	Governance System Design Workflow (in the COBIT Design Guide): Understand enterprise context and strategy, Determine the initial scope of the governance system, Refine the scope of the governance system, Conclude the governance system
Domain 2, Strategic Management: Understand the organizational strategy and use the goals cascade to determine the appropriate processes and additional governance components that will add value to the enterprise.	COBIT Design Factors (in the COBIT Design Guide): Enterprise Strategy, Enterprise Goals, Risk Profile, I&T Related Issues, Threat Landscape, Compliance Requirements, Role of IT, Sourcing Model for IT, IT Implementation Methods, Technology Adoption Strategy, Enterprise Size
Domain 3, Benefits Realization: Focus on the key processes such as Ensured benefits realization, portfolio management, program management and project management.	COBIT Implementation Model (In the COBIT Implementation Guide): 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?
Domain 4, Risk Optimization: Understand the enterprise risk appetite and tolerance levels and apply these to the risk responses for each risk scenario.	
Domain 5, Resource Optimization: Inventory all resources and determine the demand/supply ratio to make business-based prioritizations.	

Hack #8: Adopting GEIT in an environment that has little to no executive level support

CGEIT	COBIT
Conduct a full stakeholder analysis to understand the relevant stakeholders, their stake and influence. Use the RACI charts to determine appropriate roles. Under Domain 1, Framework for the governance and management of enterprise IT, refer to the section on methods to manage organizational, process and cultural change. This section addresses the Kotter Implementation Lifecycle, the Lewin/Schein Change Theory, and models to establish accountability.	Refer to the COBIT Implementation Guide Chapter 4, Identifying Challenges and Success Factors. In this chapter, each phase of the implementation lifecycle identifies challenges such as this one and suggests potential solutions. Refer to the COBIT Implementation Guide Chapter 5, Enabling Change. This chapter identifies the organizational aspects of adopting EGIT and offers suggestions on gaining the proper support from all levels.

Hack #9: Making GEIT sustainable and continuous in an enterprise

CGEIT	COBIT
Initiate and manage the GEIT implementation as a program, using Domain 3, Benefits Realization as a guide. Identify all relevant risk scenarios and determine the proper responses based on Domain 4, Risk Optimization. Ensure the proper resources are available by using Domain 5, Resource Optimization.	Adopt and adapt the GEIT system as design factors change. For example, if the enterprise strategy or threat landscape encounters major changes, then the selected governance and management objectives may change as well. Refer to the COBIT Design Guide to assist in making changes based on all of the design factors. Download the design guide tool from the ISACA site to assist in determining the most applicable governance and management objectives to focus on. Refer to the COBIT Implementation Guide for a step-by-step methodology for continuously adopting and adapting a GEIT program.

Hack #10: Tips and tricks to studying for the CGEIT and COBIT exams

CGEIT	COBIT
Know the syllabus and download the candidate exam preparation guide from the ISACA site.	Know the syllabus and download the candidate exam preparation guide from the ISACA site.
Understand the intent of each domain. This will assist you in determining the scope of the question and eliminating answers that are part of other domains.	Read the full question and look for key words to determine which module the question is coming from and remove answers that are clearly not correct.
Know the task and knowledge statements. These statements are the basis of how exam questions are written – they seek to test your ability to achieve these tasks based on the appropriate knowledge statements.	Be cautious of absolutes such as always or never.
Be cautious of absolute statements such as always or never.	When you are completely lost, look for the answer that would be the most valuable to the enterprise.
Download and study the CGEIT body of knowledge as well as the practice exam questions.	Download and study the COBIT Introduction and Methodology and Governance and Management Objectives Guides.
Attend an accredited exam preparation course.	Attend an accredited exam preparation course.

Get in touch….

www.apmg-international.com

@APMG_Inter

www.isaca.org

@ISACANews

www.escoute.com

@ESCOUTE1

Mark Thomas: www.linkedin.com/in/markthomas8/

COBIT 2019

TRAINING & CERTIFICATION

www.isaca.org/

apmg-international.com/

CGEIT