

CGEIT Exam Prep: Week 9

Risk Management



Webinar URL: <http://tinyurl.com/cgeitPrep>
Dial IN: 641-715-3635 | CODE: 675-176#

Dec 3, 2009

1

Copyright ©2009 Tunitas Group and Professional Assurance, LLC. All rights reserved.

This presentation and other class material may be used solely by participants in the 2009 CGEIT Preparation Class, given by Tunitas Group and Professional Assurance, for purposes of exam study and preparation. No other use is permitted without express written authorization.



2

Resource Reminders

- **Share questions \ comments with class**
 - Use: cgeit@tunitas.com or wiki
- **Lectures and links**
 - <http://www.tunitas.com/cgeit>
- **Class Wiki for notes and candidate contributions**
 - <http://cgeitexamprep.wikispaces.com/>
- **Weekly sample questions generally found at:**
 - <http://Tinyurl.com/cgeit-wk#> where # is the week number
- **CISA CPE (IT Governance Domain)**
 - 1 CPE hr for each class hr

3

Schedule

- **Dec 11: Review**
 - Test strategy
 - Additional material on value delivery
 - No new concepts
 - Your questions

4

Agenda

- **Practice Test Items**
- **Risk Management**
 - **CGEIT Concepts**
 - **COSO ERM**
 - **Risk IT**
- **Domain Tasks and Competencies**

5

Week 9 Test Scenario

- *Company is a national law firm with offices in many jurisdictions. To save costs and improve security, the Company has begun consolidation of Company IT resources at an enterprise wide data center thru a 10 year contract with an external service provider.*
- **What types of questions could we expect?**
 - **Risk management**
 - What are the security + / - with data consolidation?
 - How is company risk managed with 3rd party provider
 - For a law firm IT may not be strategic, but the protection of privileged information is mission critical.
 - **Alignment (always an issue when outsourcing)**
 - How does the Company ensure that the type and level of provided services are sufficient to support Company growth
 - **Performance measurement**
 - Centralized service to support de-centralized business

Risk Management Question Hints

- Infosec is a subset of risk management in turn a subset of corporate governance
- Executive level responsibility for infosec *governance*. Responsibility for security activities lower in the organization.
- Risk reporting must address potential to adversely effect the accomplishment of strategic objectives
 - Risk reporting must address potential loss of corporate assets
- Select the risk treatment that best supports business objectives
 - Risk acceptance *framework* Board responsibility

Question 9.1

How is the risk of a breach of electronically maintained client confidential information best managed?

1. By the service provider's independently validated compliance with the Firm's security standards.
 - *The Firm's existing security standards may be insufficient for consolidated data center*
2. Service agreement requiring that the Outsource indemnify the Firm for all losses associated with a breach of security.
 - *Damages may be beyond the capability of outsource to satisfy or otherwise cost prohibitive.*
3. Encryption of all data maintained at the data center.
 - *A technical solution such as encryption is not a panacea solution what is a business problem. Furthermore, applications & users must have access to keys which creates vulnerability*
4. Through regular audits of data center operations conducted by the Firm's risk officer
 - *The only alternative that provides flexibility sufficient to respond to a changing risk environment.*

Question 9.2

Individual Courts and Regulators have distinct requirements with respect to the security of electronic filings. What approach should the Firm take to ensure that its Attorneys have the capability to submit electronic filings where ever such are allowed

1. Provision a suite of security services to be used as determined by individual Attorneys
 - *Most cost effective alternative. Allows the Firm to ensure the technical competence of the security implementation, while meeting jurisdictional requirements.*
2. Implement a global security standard that encompasses the security requirements of all jurisdictions
 - *This is likely to be cost inefficient. The filing requirements necessarily involve implementation specifics (ie, filings are transactional).*
3. Allow offices in different jurisdictions to independently implement the appropriate security procedures as required by the relevant Courts and Agencies
 - *This is an inefficient and high risk strategy. Provides little opportunity for standardization ; assumes security competency are separate offices.*
4. Support with a global standard the most common security requirements; defer electronic filings in jurisdictions not supported by that standard.
 - *This may not be an option in some jurisdictions; prevents Firm from taking advantage of cost benefits of electronic filing.*

Question 9.3

One of the Firm's offices has experienced a successful intrusion into its network by hackers, but due to poor incident response is unable to determine what information may have been accessed or modified. What action should immediately be taken?

1. Notify Clients of that office that there may have been a breach of Privileged communication.
 - *Costly alternative. May needless damage Firms reputation. Need to first better understand the specifics of the information losses.*
2. Isolate the office network from the Corporate WAN.
 - *Containment of significant but poorly understood risk is appropriate.*
3. Notify Firm Attorney's that there has been a hack and therefore review any recently prepared documents for unexpected changes.
 - *Costly alternative. May needlessly waste Attorney resource on non-billable activity. Need to first better understand the specifics of the hack.*
4. Have external auditors conduct a forensic analysis to determine the method and scope of the intrusion.
 - *An appropriate activity, but it is not necessarily the first thing to accomplish. Poor incident response procedures may have limited the ability of forensic analyst.*

Question 9.4

Firm Attorneys regularly include client confidential information in unencrypted Internet email. Canons of attorney ethics do not require Attorneys to encrypt email or notify clients that they are using insecure email. What is the Firm's best course of action?

1. **Adopt an enterprise email encryption solution that is only partially effective but easy to implement**
 - *Prevention of relatively low risk events is undoubtedly more cost effective than other risk treatment (avoidance or transfer)*
2. Inform clients of the practice but agree to any client request not to use such insecure communication channels
 - *This is a form of risk transfer. May actually increase risk and cost by preventing attorneys from using standard communication channels.*
3. Confirm that Firm malpractice policies include losses due to unintended breaches of privileged communication
 - *Firm remains at risk to demonstrate how intercepted email caused tangible loss to Firm. Provides the client no protection. Unlikely to compensate for sanctions due to violation of general duty to protect privileged information*
4. Inform clients of the practice and agree not to use such insecure communication channels unless the Client accepts the risk of a confidentiality breach.

See 2 above.

Question 9.5

The Firm is considering deploying a Client portal through which clients can submit required documents, preview filings requiring signature, review billing records, and securely communicate with Attorneys and other staff. What information is the most important to collect when evaluating the risk associated with the portal?

1. Likelihood of intrusion attempts
 - *Although significant, intrusion is just one kind of threat associated with the portal*
2. Level of client use
 - *Risk and risk response is understood relative to value. The value of a client portal is clearly related to the level of utilization.*
3. Impact on Attorney productivity
 - *Distracter response. Attorneys are unlikely to be the parties managing the collection of documents, request response, etc*
4. Cost of appropriate security
 - *'Security' is just one kind of risk response. Security risk is just one kind of risk.*

Agenda

- **Practice Test Items**
- **Risk Management**
 - CGEIT Concepts
 - COSO ERM
 - Risk IT
- **Domain Tasks and Competencies**

13

Information Security Governance: Guidance for Boards

- **Purpose of infosec governance:**
 - Alignment w/ business strategy (avoid focus on past wars)
 - Risk management
 - Efficient use of resources
 - Monitoring and reporting of appropriate risk metrics
 - Optimize value of security investments
- **Roles & responsibilities**
 - **Board**
 - Define 'global risk profile'
 - Set tone
 - Resource infosec
 - Obtain independent assurance from auditors (internal or external)
 - ☼ Insist that management makes security investments measurable & reports on security program effectiveness

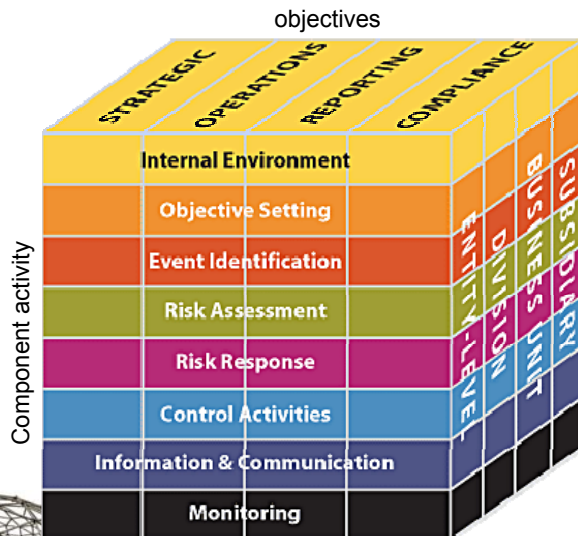
14

Information Security Governance: Guidance for Boards

- **Roles & responsibilities**
 - **Sr. Management**
 - Oversight for security and control framework: policy, standards, practices and procedures, measures
 - Appropriate risk identification
 - Security infrastructure
 - Monitoring
 - Reviews of effectiveness
 - Incorporation into SDLC
- **Questions**
- **Infosec Governance Deliverables (by domain)**
- **Maturity model**
 - *IT focus is associated w/ lower levels of maturity*

15

COSO ERM Framework



- **General framework for management of enterprise risk**
 - Common language & approach
- **Management of IT related risks (eg infosec) should be addressed as special case of ERM**
 - Enterprise context
 - IT risk as 'just another' kind of business risk

16

COSO ERM Component Activity

- **Internal environment**
 - Risk management philosophy / appetite
 - Ethical values
 - Corporate structure / roles & responsibilities
 - HR standards
- **Objective setting**
 - Company purpose / goals
- **Event identification** ← *Top Down!*
 - Listing of significant risk (adverse) events
- **Risk assessment**
 - Likelihood / impact of risk events
- **Risk response**
 - Avoidance | Reduction | Sharing (transfer) | Acceptance
Or combination thereof

17

COSO ERM Component Activity

- **Control activity**
 - Policies and procedures that ensure that risk response activity carried out
 - E.g., (trivial) not the password policy, but the AD & Win logon mechanism that enforces the policy
- **Information and communication**
 - Outputs, indicators, reports that coordinate other component activities
- **Monitoring**
 - Processes needed to determine the effectiveness of all the other ERM components

18

COSO ERM Organizational Objectives

- **Strategic Risks**
 - Big picture, adverse impact on enterprise mission
- **Operations Risk**
 - Adverse impact on company operations
 - Business interruption, project, contract and product liability, information security
- **Reporting Risk**
 - Reliability of the Company's financial & non-financial reporting
- **Compliance Risk**
 - Legal & regulatory exposure



19

COSO ERM Entity & Unit Level Risk

Entity-wide plus unit specific risks

- **Unit-level risk**
 - Risk should be considered and managed at all levels of business
 - Follow organization chart?
- **Entity level risk**
 - Risk impacting multiple business units
 - Roll up of unit level risk with 'material' impact

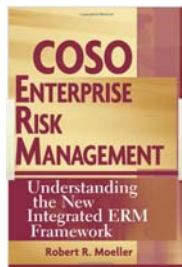


20

COSO ERM: for more info

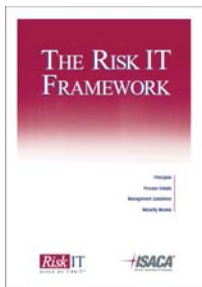
COSO.org

- http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
- http://www.coso.org/documents/COSO_ERM.ppt
- <http://www.coso.org/ERM-IntegratedFramework.htm>



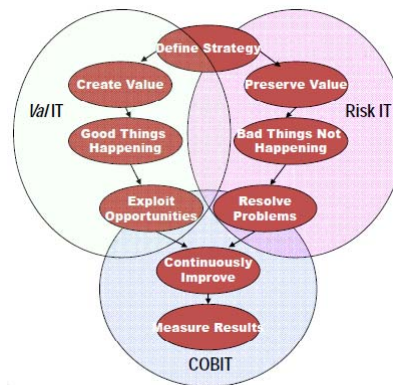
especially recommended for security professionals

21



Risk IT Framework

- **3rd Component of ITGI's IT Governance Framework**
 - Val IT – creation of business value
 - Risk IT – protection of information assets
 - COBIT - control & improve IT



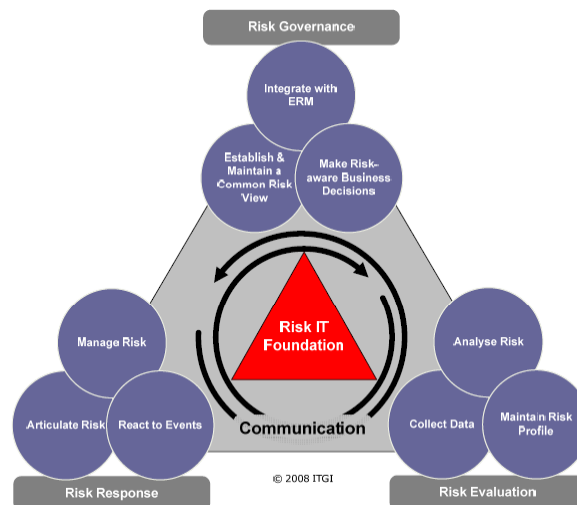
22

Risk IT

- **Goal: ensure enterprise governance of IT risk**
 - **Connects IT risk with business objectives**
 - **Aligns IT-related business risk with overall enterprise risk management**
 - Akin to IT-enabled business investment / value
 - **Framework specializes the COSO ERM framework to IT risk**
 - **Emphasis (but not exclusively) on information security risk**
- **Framework provides:**
 - **Risk management governance practices**
 - **End to end process framework**
 - **Catalog of generic adverse related IT risk**
 - **Tools & techniques**
 - **Roles & responsibilities**

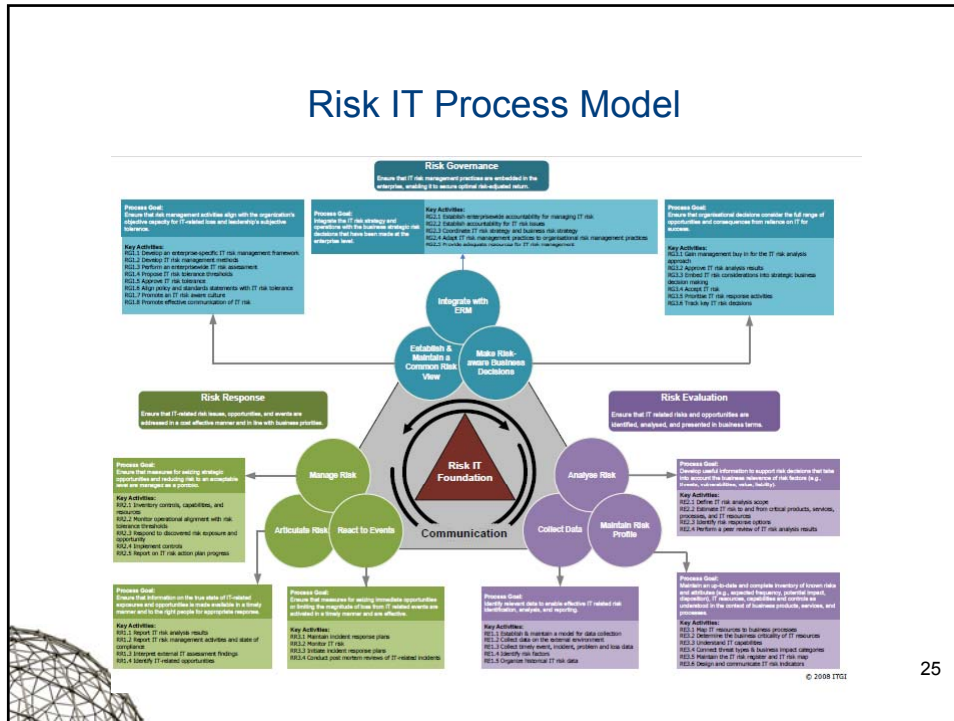
23

Risk IT Components

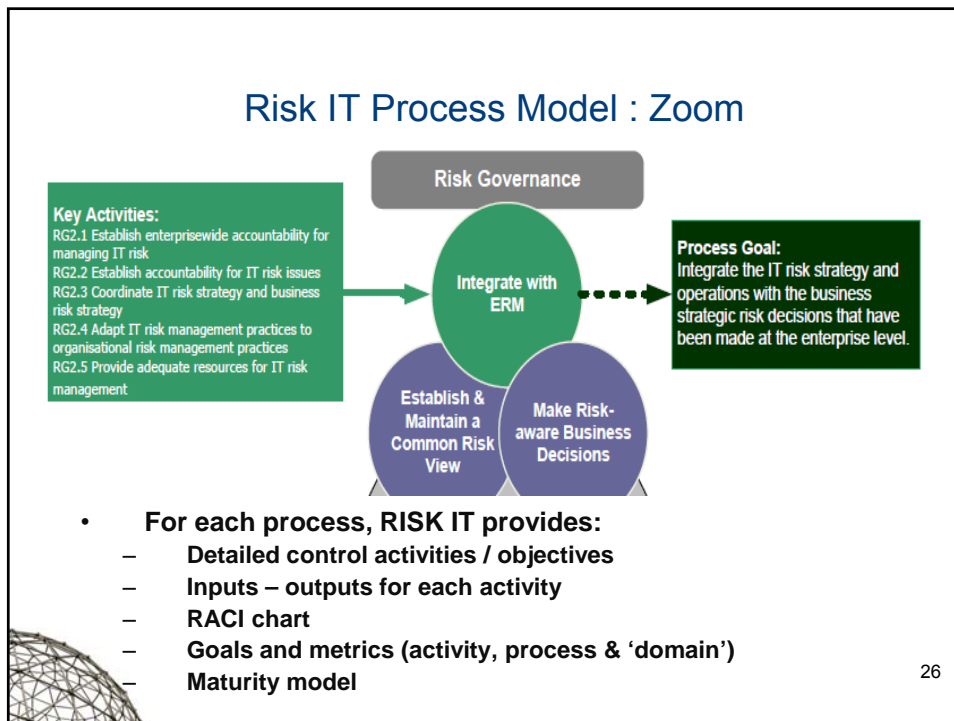


24

Risk IT Process Model








Risk IT Process Model : Zoom



- For each process, RISK IT provides:
 - Detailed control activities / objectives
 - Inputs – outputs for each activity
 - RACI chart
 - Goals and metrics (activity, process & 'domain')
 - Maturity model

Risk IT Companion Document

The Risk IT Practitioner Guide

-  Download (PDF, 5.7M) 
-  Download Toolkit Zip (Zip File, 195K) 
-  Purchase the Book

The Risk IT Framework describes a detailed process model for the management of IT-related risk. In this model, multiple references are made to risk analysis, scenario analysis, responsibilities, key risk indicators and many other risk-related terms. *The Risk IT Practitioner Guide* contains practical, detailed guidance on how to accomplish some of the key activities described in the process model.

[The Risk IT Framework](#)



Domain Task & Knowledge Competencies

What ISACA Tells Us about Risk Management

- Eight Task Statements, 18 Knowledge Statements
- Task Statements are Cross Referenced to COBIT Processes and Control Objectives.
- Domain Statement: *“Ensure that appropriate frameworks exist and are aligned with relevant standards to identify, assess, mitigate, manage, communicate and monitor IT-related business risks as an integral part of an enterprise's governance environment.”*
- Following are Details About Each Task Statement
- Recommendation: Understand each Task Statement in terms of the indicated COBIT Processes and Control Objectives.
- Recommendation: Review Knowledge Statements to make certain you have at least scanned primary references.

29

Risk Management Task Statement #1

- “Ensure that IT risk identification, assessment, mitigation, management, communication and monitoring strategies are integrated into business strategic and tactical planning processes. .”
- Corresponds to COBIT:
 - PO4.8 Responsibility for risk, security and compliance
 - PO9.1 IT risk management framework
 - PO9.4 Risk assessment
 - Key Insight: COBIT is strong on “security risks” and not so strong on “other risks” in this domain. However, all risks are essentially treated the same for CGEIT purposes.

30

Risk Management Task Statement #2

“Align the IT risk management processes with the enterprise business risk management framework (where this exists).”

- Corresponds to COBIT:
 - PO9.1 IT risk management framework
- Key Insights: this is the most important element of the COBIT approach to this domain. By specifying “full spectrum risks” (i.e. beyond those discussed in ISO 27001 Annex) within this framework, full spectrum risks can be monitored for and reported against.



31

Risk Management Task Statement #3

“Ensure a consistent application of the risk management framework across the enterprise IT environment..”

- Corresponds to COBIT:
 - PO4.8 Responsibility for risk, security and compliance
 - PO9.2 Establishment of risk context
 - PO10.9 Project risk management
 - DS5.2 IT security plan
- Key Insight: (1) This task competency is heavily influenced by maturity within the risk management functions and across the organization. (2) Notice (again) that the “IT Security Plan” (DS5.2) does not typically cover “non-security” risks [go to COBIT DS5 for further discussion] but PO10.9 is in place focusing on “project risks.”



32

Risk Management Task Statement #4

“Ensure that risk assessment and management is included throughout the information life cycle.”

- Corresponds to COBIT:
 - PO9.2 Establishment of risk context
 - PO10.9 Project risk management
- Key Insight: (1) COBIT PO10.9 deals with “project risk.” (2) consider how training should be introduced that emphasizes “project risk” within the standard risk assessment process.



33

Risk Management Task Statement #5

“Define risk management strategies, and prioritize responses to identified risks to maintain risk levels within the appetite of the enterprise.”

- Corresponds to COBIT:
 - ME4.5 Risk management
- Key Insights: (1) for a variety of reasons, organizations require A LOT of hand holding in the rational acceptance of risk.



34

Risk Management Task Statement #6

“Ensure that risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels.”

- Corresponds to COBIT:
 - PO9.2 Establishment of risk context
 - PO9.3 Event identification
 - PO9.4 Risk assessment
 - PO9.5 Risk response
- Key Insights: (1) emphasizes the reality that planning it and monitoring it isn't the same as DOING IT. So a separate task competency devoted to adoption of the risk management strategies...



35

Risk Management Task Statement #7

“Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate).”

- Corresponds to COBIT:
 - ME4.5 Risk management
 - AI1.2 Risk analysis report
 - PO9.3 Event identification
 - PO9.6 Maintenance and monitoring of a risk action plan
- Key Insights: (1) Risk reporting is not on the same calendar as audit findings and responses. (2) Event identification and the risk action plan must be matched with the risk impact AND the remediation window.



36

Risk Management Task Statement #8

“Establish monitoring processes and practices to ensure the completeness and effectiveness of established risk management processes.”

- Corresponds to COBIT:
 - PO9.6 Maintenance and monitoring of a risk action plan
 - ME4.5 Risk management
- Key Insights: Means review and refine the risk management plan.

Once we have implemented the COBIT Processes and Control Objectives associated with this domain, we are essentially at maturity level “3.5”

37

Risk Management 18 Knowledge Statements

1. Knowledge of the context of risk management at the strategic, portfolio, program, project and operations level
2. Knowledge of risk management frameworks and standards (e.g., COSO ERM, MoR, OCTAVE, ISO31000, AS/NZ 4360:2004)
3. Knowledge of the enterprise's business objectives
4. Knowledge of the enterprise's risk management framework (including the risk classification model used to support risk identification and assessment)
5. Knowledge of the enterprise's external business environment
6. Knowledge of the enterprise's internal environment

38

Risk Management 18 Knowledge Statements

7. Knowledge of how the enterprise defines and executes business strategies to achieve its goals and objectives
8. Knowledge of how to map business process down to IT process to understand dependencies and root cause
9. Knowledge of the enterprise's risk appetite
10. Knowledge of the enterprise's IT resources (applications, information, infrastructure and people)
11. Knowledge of the threats, vulnerabilities and opportunities inherent in the enterprise's use of IT
12. Knowledge of the types of business risks, exposures and threats that can be addressed using IT resources

39

Risk Management 18 Knowledge Statements

13. Knowledge of quantitative and qualitative methods to determine sensitivity, criticality and maturity of IT-related contributions to business success
14. Knowledge of quantitative and qualitative methods (including enterprise-specific descriptive measurement scales, IT-related asset valuation methods and probability, use of both audit and stream data types, and impact and loss expectancy models/techniques) to assess IT risks
15. Knowledge of methods to discover more rare, but high-impact risk types, such as process analysis techniques
16. Knowledge of risk mitigation strategies in relation to the use of IT in the enterprise
17. Knowledge of risk management techniques that can be applied to affect enterprise risk management, particularly as they relate to IT-related activities
18. Knowledge of methods to effectively manage and report the status of identified risks

40