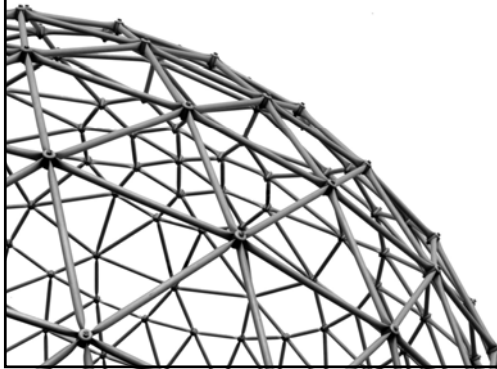


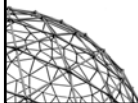
CGEIT Exam Prep: Week1

The CGEIT Exam
IT Governance Foundations

Oct 1, 2009



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.



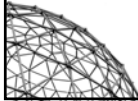
Reminders / Announcement

1. October 7 Registration deadline

- December 09 admin

2. ISACA “CGEIT Review Manual”

- Now being finalized
- Promised publication before year end
- **No assurance of availability for Dec 09 prep**
- Definitely available for June 10 exam prep



Session Agenda

1. Introductions

- Instructors
- Students
- Expectations of the Course

2. The CGEIT Exam

3. Study / Prep Course Strategy

4. Topic: Governance Foundations



Introductions

Instructors



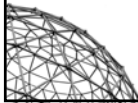
Bill Pankey



Jim Anderson



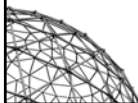
Ann Geyer



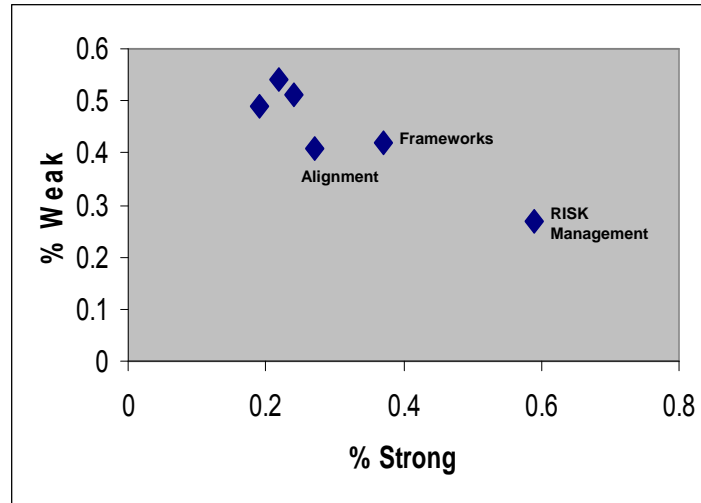
Who are you?

CGET Candidates

- **Quick poll**
 - <http://tinyurl.com/ybu6of9>
 - *OR*
 - 'QUIZ' button on your DimDim console
- **Select and answer each poll question**
 - Profession?
 - Industry Vertical?
 - Region?
 - Credentials?



Student Self Assessment of Competency



Class Expectations

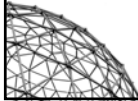
- 1. Not a substitute for IT governance experience**
- 2. Governance from the ITGI perspective**
 - Mostly will use CGEIT basic references
 - Some other ideas when complementary
- 3. Focus on major themes**
- 4. Oriented toward preparing for exam success**
 - Help direct what you need to study
 - Relieve exam prep anxiety
 - Study questions

Disclaimer

No warranty of exam success

- **Materials have been developed by instructors**
- **No ISACA endorsement**
- **No insider knowledge *not* members of the CGEIT test Committee**

- **Quality of experience will be proportional to level of participant effort**



CGEIT Exam: Agenda

- 1. June 2009 Experience**
 - **Expectations**
 - **Reality**
 - **Results**
- 2. Test Challenges**
- 3. Preparation Strategy**



The CGEIT Test Items

CGEIT Item Development: <http://tinyurl.com/qolzxm>

- **ISACA item development protocol requires:**
 - **Reference to a specific CGEIT domain and task**
 - ☀ **Each item is a test of knowledge pertaining to a frameworks [exclusive] or alignment [exclusive] or value delivery [exclusive] or ... related task**
 - **Rationale for the correctness (or not) of each option**
 - **Applicable basic reference *by page***

Our Spring 2009 Expectations

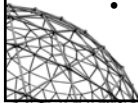
Anticipated questions of objective fact similar to those of CISA or CISM

- **Exam would be a typical ISACA keyword and concept test:**
 - **Which of the following provides the best indicator of IT alignment with enterprise strategic goals?**
 - A. CMM benchmark
 - B. Dashboard
 - C. Balanced Scorecard
 - D. IT metrics
- **Mastery of the CGEIT basic references => Exam success**

Spring 2009 Prep Strategy

Focus on coverage of CGEIT Basic References

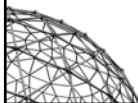
- **Major exam preparation challenge was *editorial*.**
 - Too many pages
 - Too much detail
- **Studied all the material in the basic references +**
 - Assumed that facility with COBIT, ValIT and other branded tools would be critical
 - Assumed that knowledge of important frameworks would be critical
- **Developed 'cheat sheet' summary**
 - Named concepts and terms
 - Basic IT governance themes, *per ITGI*
- **Practice test items**



Reality: What we got

Many questions related to 'best' course of action with only a loose connection to basic references.

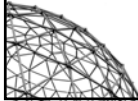
- **Questions similar to:**
 - **To enhance the growth of its ecommerce program, Fortune 50 retailer A acquires a web development firm B. How should the IT departments be merged?**
 - A. B's development organization kept in tact and its management reports to A's IT management
 - B. B managed as an independently operated service provider reporting to A's Sr. Executive.
 - C. A new development organization is create using resources from A and B
 - D. B's human resources assigned to existing functions within A
- **Mastery of the CGEIT basic references \Rightarrow Exam success**



Reality: What we got

No explicit testing of much of the detail found in CGEIT basic references

- **No direct questions regarding details or mechanics of COBIT or ValIT frameworks.**
- **No direct questions regarding the specifics of any of the frameworks listed in the ITSM 'Frameworks' book**



Candidates' Subjective Report

Disappointment that many areas of study apparently were not tested

- **Before posting of Exam results,**
 - **Test different from other ISACA exams**
 - Straightforward questions
 - Little ambiguity
 - Almost 'obvious'
 - **Wished more opportunity to demonstrate their objective knowledge of the domains**
 - **Test was 'too easy'**
 - **High level of confidence in individual answers and overall performance**



Reality: What we got

- **Success was not so easy to achieve**
 - Many bright & experienced persons *who did study* for the exam failed to demonstrate 'minimal competency'
- **Scores were generally lower than expected**
 - Many bright & experienced persons *who did study* for the exam only demonstrated 'minimal competency'
 - Commonly reported disappointment over failure to achieve a higher score

How to Explain

Several (non-exclusive) alternatives

1. **Exam was not 'fair'**
 - Low correlation between competency and test performance?
 - Test is 'immature'?
2. **Candidates studied the 'wrong' material or the 'right material in the wrong way'**
 - Failure to consistently apply a 'CGEIT perspective' to the material?
3. **Candidates used their knowledge incorrectly when writing the exam**
 - E.g., Answered a 'frameworks' question as if it were an 'alignment question'

Prep Strategy #1: Calibrate to the CGEIT Role

The anticipated CGEIT role

- **Performs functions for Board & Sr. Executives**
 - *“Taking a lead role in the establishment and management of information technology infrastructure and processes, individuals playing a role in IT governance provide significant support to the Board of Directors and executive management.”*
- **Is more than IT management and control**
 - Ensures delivery of value and risk management that goes beyond simple IT performance
- ☀ **Determine what Board \ Executive questions are addressed in the reference material.**
 - 1st or 2nd order

Prep Strategy #2: Focus on Responsibilities

CGEIT Job Practice Areas @ <http://www.isaca.org/cgeit>

- **Task responsibilities are defined in the ‘CGEIT job practice’**
- **Most of the key activities are largely ‘non- operational’**
 - *Define and Monitor, Ensure, Enable, Assist, Promote***And are distinct from**
 - *Design, develop, configure, implement, Test*
- **Use understanding of the CGEIT responsibility to determine the required level of knowledge**
 - Procedural vs non-procedural
 - Values & preferences based on experience

Prep Strategy #3: Test understanding by applying knowledge to current industry issues

CGEIT qualification is for governance activity at a high organizational level

- ITGI is not expecting the CGEIT to address long 'settled' issues of IT governance
- Focus of Board and Sr. Executives will be on 'hot' or 'timely' issues for which 'best practice' is not firmly established
- **Important areas to apply CGEIT knowledge include**
 - Appropriate 'sourcing' (e.g., out / off-shoring)
 - Strategic initiatives & partnerships (extended enterprise)
 - Regulatory mandates / legal liability
 - Modernization (e.g. virtualization & cloud computing)
- **ISACA's "Top Business Technology issues Survey" ~ <http://tinyurl.com/n63nmz>**

Prep Strategy #4: Focus on Areas of Weakness

- **Avoid tendency to first answer question from the perspective of area of greatest strength**
 - CGEIT exam questions are associated with only a single domain.



For practice questions:

1st determine the domain from which the question is drawn ... then apply the major themes of that domain

Course Miscellany

- **Prior to online class, lectures will be posted at <http://tinyurl.com/n38o9k>**
 - **Relevant Lectures:**
 - Will remain there for the exclusive use of CGEIT exam prep. No reproduction for other purpose.
 - **Sample test items**
 - Will notify by list serve the availability of items. Target the Monday previous to the class.
 - Review and answer before class. Be prepared for class discussion.
 - **Saturday in-person session**
 - Sponsored by SF ISACA chapter.
 - TBD Date / location TBD
- Address comments / issues to bpankey@tunitas.com**

Introduction to Governance

1. **What is IT governance?**
2. **What problems does IT governance solve?**
3. **How is IT governance achieved?**
4. **Why is IT governance importance**

Enron, Worldcom, TycoGE ...

- **Catastrophic collapse to mere misstatements in financial reports emphasized the need for improved corporate ‘governance’**
 - SOX and other mandates imposed new regimen of ‘control’ over financial reporting
 - Emphasis on importance of IT controls to accuracy in financial reporting (§404)

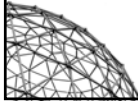
Cedar Sinai, Green Giant, Heartland

- **Colossal IT failure lead to significant losses at otherwise successful companies**
 - Cedar Sinai: decommissions \$70M CPOE application 1 day after mandating its use by all Cedar’s practitioners.
 - Green Giant: trucks 40 railroad car loads of produce to land fill for 30 days due to failures to adequately implement SAP system
 - Heartland: \$30M+ in direct costs, significant loss of business and collapse of stock value due to single information security failure.
 - Name your 3 or 300 examples
- **The IT Governance Institute (ITGI) was established in 1998 in recognition of the increasing criticality of information technology to enterprise success.**

What is IT Governance (short version)

Methods to ensure that the enterprise:

- 1. Makes the right IT investments in the right way (i.e., gets value)**
- 2. Uses information 'responsibly' (i.e., manages risk)**



What is IT Governance (longer version)

- Identification of IT aspects that are strategic to the enterprise**
- Creation of an opportunistic IT strategy**
- Assurance of proper execution of the IT strategy**
- Assurance that costs of non-strategic IT activities are minimized**
- Assurance that information risks appropriately managed**



What is IT Governance (1) Relative to CGEIT Domains

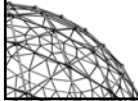
- **Formal mechanism for stakeholder control over IT**
- **Defined by its accomplishments:**
 - Receipt of appropriate value from IT
 - Making the 'right' IT investments
 - "Alignment"
 - "Value Delivery"
 - Maximizing the business benefit from those investments
 - "Performance measurement"
 - "Resource management"
 - Prevention of IT misuse
 - Avoid damage to company assets or reputation
 - "Risk management"

What is IT Governance? (2) Relative to CGEIT Domains

- **Special case of enterprise governance applied to information and IT**
 - ***Arrangement between governing body and management*** that provides the structure through which:
 - Overall objectives are set
 - "strategic alignment"
 - Means of obtaining the objectives are outlined
 - "resource management"
 - "risk management"
 - "value delivery"
 - Performance monitoring is described
 - "performance management"

Broader than COSO Control Concepts

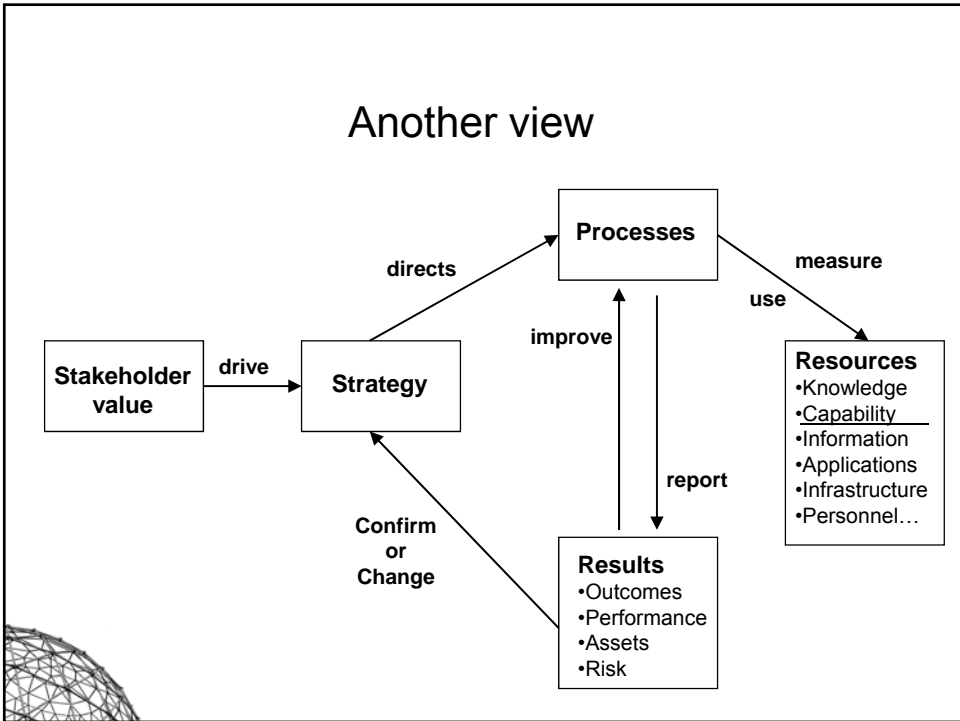
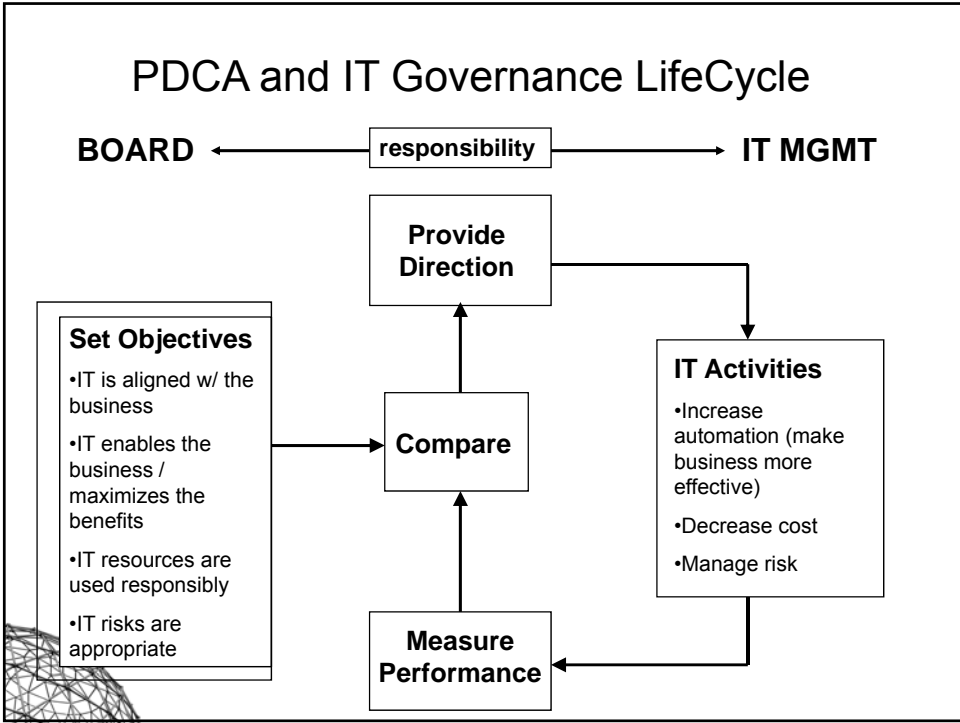
- **COSO focused on risk management**
 - Integrity of financial statements
 - Compliance with laws / regulation
 - Operational efficiency and effectiveness
- **ITGI's IT Governance concept dual focus**
 - results
 - Financial and non-financial
 - Current and future
 - risk management
 - Asset preservation
 - Regulatory compliance



Stakeholder Responsibility

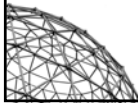
- **OECD, *Principles of Corporate Governance: "responsibilities of boards"***
 - Reviewing and guiding corporate strategy, major plans of action, risk policy
 - Strategic alignment
 - Risk management
 - approving annual budgets and business plans; setting performance objectives;
 - Resource management
 - Value delivery
 - monitoring implementation and corporate performance
 - Performance measurement





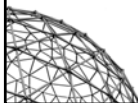
IT Governance Framework How Governance is 'Implemented'

- **Governance process produces**
 - **A set of decisions / questions that must be addressed**
 - **Assignment of specific responsibility for those decisions**
 - **A means to hold decision makers accountable**

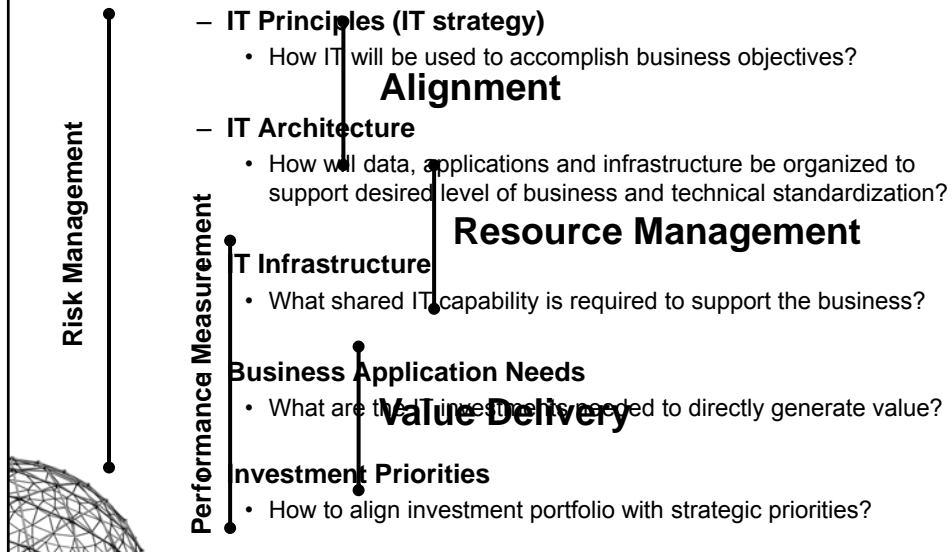


What IT Derives from Governance

- **Board directives drive the following decisions:**
 - **IT Principles (IT strategy)**
 - How IT will be used to accomplish business objectives?
 - **IT Architecture**
 - How will data, applications and infrastructure be organized to support desired level of business and technical standardization?
 - **IT Infrastructure**
 - What shared IT capability is required to support the business?
 - **Business Application Needs**
 - What are the IT investments needed to directly generate business value? How should the need for innovation be balanced with standardization requirements?
 - **Investment Priorities**
 - How to align investment portfolio with strategic priorities?



What IT Derives from Governance / Topics

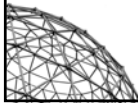


Who makes the decisions?

- **ITGI ‘Board Briefing’ identifies:**
 - Board of Directors
 - IT strategy Committee
 - CEO
 - Business Executives
 - CIO
 - IT Steering Committee
 - Technology Council
 - IT Architectural Review Board
- **COBIT ME4 identifies additional compliance, audit, risk and security roles**

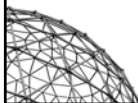
How is accountability maintained?

- **Performance Measurement**
- **IT Governance 'arrangements'**
 - **Business monarchy**
 - **IT monarchy**
 - **Feudal**
 - **Federal**
 - **IT duopoly**
 - **Anarchy**



Why IT Governance important?

- **Stated in the negative:**
 - **Avoid mismatch between Board expectation and Management's delivery**
 - IT solutions with appropriate timeliness, cost and quality
 - Business value
 - Increased productivity
 - **Ineffective IT governance a root cause for:**
 - Lost opportunities
 - Damaged reputation
 - Failure to meet deadlines, cost overruns, quality issues
 - Negative impact on core processes due to poor quality IT services
 - Failure of IT initiative to bring innovation or promised benefits



Why IT Governance important?

- **Industry surveys* show that companies with good IT governance:**
 - Are more profitable
 - Have reduced IT costs
 - Are more likely to find and take advantage of new business opportunity
 - Learn about and adopt new IT faster
 - Make more efficient use of executive resources

* see, for example, Weill & Ross, IT Governance

Question 1.1

<http://www.micropoll.com/akira/mpview/671426-206760>

- **Which is most likely to suffer should the enterprise outsource its IT function?**
 - A. strategic alignment
 - B. value delivery
 - C. risk management
 - D. performance measurement

Question 1.1

- **Which is likely to suffer the most should the enterprise outsource its IT function?**
 - A. strategic alignment**
 - Outsourcing agreements are unlikely to fully anticipate changes in business strategy as outsource obligations are fixed in contractual language.
 - B. value delivery**
 - Value requirements are stated as part of agreed service levels.
 - C. risk management**
 - Risk can be monitored and therefore managed by parties independent of IT
 - D. performance measurement**
 - Performance should be assessed from the perspective of the business and therefore independent of IT.

Results: <http://www.micropoll.com/akira/mpresult/671426-206760>

Question 1.2

<http://www.micropoll.com/akira/mpview/671426-206759>

- **The most important aspect of accountability for IT is?**
 - A. compensation plan**
 - B. performance measurement**
 - C. control processes**
 - D. IT balanced scorecard**

Question 1.2

- **The most important aspect of accountability for IT is?**
 - A. compensation plan**
 - Compensation is only one of the ways to recognize success or failure in meeting objectives
 - B. performance measurement**
 - Executives and managers are accountable for the satisfaction of specific goals as measured by IT performance.
 - C. control processes**
 - Control processes may ensure the accuracy of performance measures but are not the measures of success or failure.
 - D. sanctions**
 - Employee sanctions are only intended to promote compliance with company policy

Results: <http://www.micropoll.com/akira/mpresult/671426-206759>

Question 1.3

<http://www.micropoll.com/akira/mpview/671426-206758>

- **What would typically be the greatest IT governance concern?**
 - A. management of software licenses**
 - B. effective staff recruitment, retention & training program**
 - C. bandwidth reservation**
 - D. thorough and cost effective disaster recovery planning**

Question 1.3

- **What would typically be the greatest IT governance concern?**
 - A. management of software licenses**
 - management of software licenses is too narrow a concern for Board attention
 - B. effective staff recruitment, retention & training program**
 - Staff retention is a persistent requirement needed to ensure availability of the resources needed to execute strategy and delivery value. Failure to retain staff will negatively impact performance
 - C. bandwidth reservation**
 - A 'distracter'
 - D. thorough and cost effective disaster recovery planning**
 - Disaster recovery planning is less important as it is likely that the DRP will never be invoked and in many scenarios a DRP deficiency will not negatively impact performance

Results: <http://www.micropoll.com/akira/mpresult/671426-206758>

Next Class

- **Domain: Governance Frameworks**
 - **Reading**
 - Board Briefing on IT Governance*
 - COBIT 4.1, *but only the following:*
 - ME 4: Provide IT Governance
 - PO 4: Define IT processes, organization and relationships
 - PO 6: Communicate management
- * Most important single CGEIT Basic Reference