

CGEIT Exam Prep: Week 8

Governance in the Extended Enterprise



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

Nov 19, 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

- **Friday, Nov 27 Review**
 - Strategic alignment
 - case study artifacts
 - Strategy maps
 - IT strategy
 - Enterprise architecture
 - IT BSC
 - KGI & KPI
- **Dec 2: “Risk Management”**
 - COSO ERM / ISACA's RiskIT
 - Broader risk context / treatment than CIA
 - Review of CGEIT required task competencies / knowledge
- **Dec 10: Review**
 - Governance responsibilities
 - Control frameworks
 - COBIT navigation
 - Process controls
 - Application controls
 - Value delivery
 - case study artifacts

4

Agenda

- **Practice Test Items**
- **Extended Enterprise**
 - Definitions
 - Key concepts
 - Governance Issues
- **Case Studies**
 - US healthcare
 - INTC-MSFT-DELL-FDX
- **Domain Tasks and Competencies**

5

Week 8 Test Scenario

- *Company A is a 'smart sourcing' company that supplies merchants through the world with consumer goods. Rather than own any product or warehousing facility, it leverages the assets of some 25k other firms possessing specialized production and distribution capabilities. To leverage technology, the Company links all supply chain components through its extranet.*
- **What types of questions could we expect?**
 - Alignment
 - IT is obviously strategic and Company market is competitive.
 - Performance Measurement
 - Company at risk for slow learning. Does not see finished products or directly engage product consumers
 - Risk Management
 - Company position & Scale of partner network limits Company's ability to control use and disclosure of information

Question 8.1

3k of the Company's 14k employees are involved with the development and maintenance of the Company's extranet resources. At a recessionary time, should the Company reduce cost through outsourcing IT to a global service provider?

- *Yes, reduced revenue due to a fall off in consumer discretionary purchasing necessitates cost reduction*
 - Risks Company growth. Outsource arrangement is governed by contract where market dictates needs for change.
- *No, improvements in IT are needed to achieve additional efficiency needed to offset revenue reduction*
 - IT operations are (obviously) essential to Company success and growth. IT must find a way to operate with reduced budget.
- *No, IT is a strategic Company asset*
 - While true, answer does not respond to lower revenue issue
- *Yes, the Company's service oriented architecture infrastructure is easily supported by a global service provider*
 - Whether the outsource is technically easy or hard, is secondary to the strategic question of whether or not it should be done.

Question 8.2

To ensure appropriate timeliness, pricing, and quality, the Company requires greater granular control over supply chain components. Which IT goal and metric best supports this business goal?

- *Reduce the cost of business transactions, measured by % of suppliers receiving bid requests via Company extranet*
 - Relationship between transaction costs and Intranet penetration needs to be established.
- *Improve the timeliness of transaction completion, measured by % of orders filled within specified period*
 - IT goal directly supports the business objective
- *Improve the cost effectiveness of IT, measured by % of business manager satisfaction with service costing model*
 - Very indirect measure of IT cost effectiveness. Relationship between IT cost effectiveness and timing, pricing and quality needs to be established.
- *Improve the utility of the Company extranet, as measured by # of company services available through it*
 - Very indirect measure of extranet utility. Relationship between extranet utility and timing, pricing and quality needs to be established.

Question 8.3

The Company has privileged access to the information resources of more than 7500 firms. What best assures the Company's Board that this access will be used responsibly?

- *Company compliance with ISO 27001*
 - Standard that best encompasses technical plus cultural aspects of information security.
- *A satisfactory SAS70-Type II audit*
 - Possible answer, but likely to be insensitive to individual practices regarding information systems of trading partners. SAS70 is more focused on data center assets.
- *The Company's high ethical standards*
 - 'Tone at the top' is insufficient. Assurance requires a demonstration that such standards are actually met; policy and procedures are in place to enforce such standards.
- *Electronic trading agreements with such trading partners*
 - Scale considerations are such that assessment of compliance with each such agreement is unlikely.

Question 8.4

Due to a manufacturing defect, finished goods made using Supplier B's products need be recalled. Such products may have been re-labeled or otherwise changed as they passed through Company A's supply chain. What previous management activity would ensure that the Company has the information to support such a recall effort?

- *Enterprise information architecture planning and development*
 - EA identifies the IT resource supporting this business requirement, in particular the need to trace movement of good through the supply chain.
- *Security risk management*
 - The product failure may have nothing to do with a failure of enterprise security controls
- *Identification of external legal, regulatory and compliance obligations*
 - May identify a recall requirement; but not how to complete it.
- *Business contracts with supply chain partners*
 - Identifies the obligations of other parties; but does not solve the basic information problem.

Question 8.5

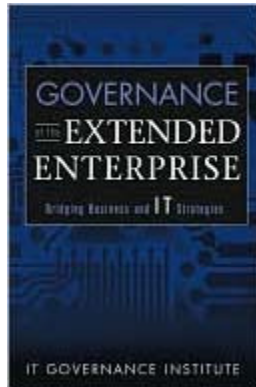
The Company has begun an infrastructure improvement project targeted at revenue growth. Use of what measurement framework is likely to be most effective in achieving these goals?

- **COBIT**
 - Appropriate, but requires substantial effort to reproduce what is provided by industry framework
- **ITIL service management metrics**
 - Relationship between ITIL metrics and revenue needs to be established
- **Capability maturity modeling**
 - Relationship between IT process maturity and revenue growth needs to be demonstrated.
- **An industry group's framework**
 - Supply chain industry's framework of KGIs & KPIs is likely to be tuned to specific factors related to success of supply chain company.

Agenda

- Practice Test Items
- **Extended Enterprise**
 - **Definitions & Concepts**
 - **Governance Issues**
- Case Studies
 - US healthcare
 - INTC-MSFT-DELL-FDX
- Domain Tasks and Competencies

Governance of the Extended Enterprise



- **ITGI Publication**
 - Basic reverence for CGEIT
- **Contents**
 - Extended Enterprise
 - Challenge
 - Value Creation / realization
 - Governance Framework
 - Governance Implementation
- **Relevance**
 - CGEIT competencies must be timely & relevant. The Extended Enterprise is a model for the modern corporation

Core Competency aka 'the Core'

- A *core competency* is a something that is central to the way that the Company does business and meets 3 criteria:
 1. Produces benefit for customers of the Company
 2. Hard for competitors to imitate, reproduce or displace
 3. Can be leveraged to multiple products and / or markets
- **Examples:**
 - Patented manufacturing process
 - Company's database of consumers & preferences (Amazon)
 - Distribution channel (Mary Kay)
 - Special service expertise (Halliburton)
 - Dominant ownership of an essential component (GE w/ containers)
- Modern Corporate strategy focuses on creating, maintaining, securing and extending 'core capability'

Value Chain

- The *core competency* may be insufficient to produce competitive products. For example, may need:
 - Additional components
 - Productization
 - Training
 - Distribution
- The additional activity required for market success dilutes the impact of the company's core competency
 - Potential barrier to market success
 - Distracts from the focus on core competence
 - Slows learning
- Need to acquire, support, and otherwise collaborate with partners to deliver value to customers ... requires a collection of activities called the 'value chain'

15

Extended Enterprise

Enterprise engineered to meet the requirements of the *new economy*

- **Customer driven production processes**
- **Globalization of markets**
- **Reduced time to market**
- **Improved logistics**
- **E-Business**
- **Global workforce outsourcing / off-shoring**

Requirement to Focus on the 'core'

- **Reduced transaction costs and lower trade barriers increase the opportunity for increased specialization (i.e. higher quality / lower cost widgets)**

What is the Extended Enterprise?

- **Extended enterprise is a collaboration of supplier chains \ networks**
 - No one supplier controls the entirety of the value delivered to the customer
- **Survival strategy in new age is for an enterprise to focus on its competencies that are competitive differentiators**
 - Outsource the remaining necessary functions to those other companies that do them better / cheaper

Example

- **PC Manufacturing**
 - **Many co-dependent participants**
 - Dell – Intel – MSFT – disk & ancillary component manufacturers – low cost call centers – FedEx – bankcard processors
 - **Value realization depends upon performance across participants**
 - **Risk propagates across participants**
 - **Multiple branding of product delivered to customer**

Example

- **US Healthcare sans Primary Care Physician**
 - **Consolidation of historically fragmented supply chains on areas of specialties**
 - Large physician practice groups; hospital consolidation, pharmacy benefit managers; drug & device manufacturers, health plans
 - **Responsibility for delivery of care quality diffuse**
 - Risks created at many points in the care delivery cycle
 - Ability of any one player to change quality depend upon the autonomous decisions of other industry participants
- **Kaiser attempts to ensure care quality as a single care delivery entity thru vertical integration (HMO)**
- **Medicare attempts to ensure care quality though enforcement of the reimbursement policies of a *monopoly* health plan**
- **US Federal government will attempt to ensure care quality through its management of health information.**

Extended Enterprise Challenge

From the perspective of the company participating in the extended enterprise:

The goal is value creation and management, but:

- **Diversity of values \ goals**
 - Each party if focused on their own core competency rather than 'finished goods' or service supplied by the value chain
- **Information sharing requirements (interop)**
 - E.g., specification for next generation widget
- **Performance measurement conflict where:**
 - Performance measured (ultimately) in terms of realized value (customer utility)
 - Value delivery depends (in part) on performance of external parties
- **Lack of channels to get timely feedback from the value chain?**
 - Need to ensure that the market is not changing faster than the Company is learning about it. (slow learning problem)

Knowledge Sharing Challenge

- **Sharing of objectives, goals & expectations critical to value *realization***
 - Decisions based on how actions facilitate / forward mission achievement
- **Thru different levels / types of info sharing**
 - Goal relationships
 - Core business relationships (transactional)
 - Resource relationships (HR, financial & IT))
 - Knowledge relationships (analytics)



Step One: Partner Identification

- How does the company know who are potential partners in an extended enterprise?
 - Requires intimate knowledge of downstream activity subsequent to the Company's value addition
- Motivation to create the extended enterprise
 - Opportunistic
 - Defensive



“Core” Governance Framework

- **Distinct from ‘central command and control’ model**
 - Allow autonomy and flexibility to business partners
- **Objectives**
 - **Vision: define what needs to be implemented**
 - Setting up shared technology & information infrastructure
 - Integrating & Aligning strategy
 - **Leadership: implement shared values**
 - Extended enterprise mapping
 - Education
 - **Change: implement measurable process imp**
 - Effective use of balanced scorecards
 - Applying appropriate key measurements (CSF/PKI/KGI)
 - **Architecture: establish cohesive approach**
 - Establish organizational structures
 - Information linkage and flow of services among partners

Governance Maturity for Extended Enterprise

- 0 **Not ready.** Impossible to achieve effective partnerships. Inability to share info about customers / products and service relationships
1. **Partial integration / Ad hoc.** High risk; partnerships are possible only if entire information systems and business processes are outsourced to most competent partner
2. **Core systems integrated management / Intuitive.** Strong leadership may be able to contract for limited partnerships with significant employee empowerment

Governance Maturity for Extended Enterprise

3. **Fully integrated management / Defined.**

Contracts clarify overall accountability and key performance indicators among partners. Partners are rewarded based on performance against key performance indicators.

4. **Monitoring management / Controlled & Measurable.**

Contracts extend to the core resource sharing level and monitoring systems started to be implemented.

5. **Knowledge management / Ideal & optimized.**

Contracts extend to the knowledge sharing level to meet customer expectations on a continuous basis.

Is the Mature Extended Enterprise Possible?

- Three facets of governance structure
 1. Each corporation's board of directors
 2. Governance of inter-corporate entities
 3. Governance of extra-corporate entities
- How to accomplish 2 & 3 thru some sort of formal mechanism w/o violation of anti-trust / restraint of trade prohibitions (ANX)
- More likely are less formal, ad hoc limited agreements to exploit temporary market advantage

Extended Enterprise: US Healthcare

- Positive patient outcomes depend upon the coordinated activity of specialists and specialty services, e.g.:
 - Referrals from primary care practitioner
 - Diagnosis & treatment plan from specialists (multiple)
 - Labs and imaging centers
 - Surgeon
 - Hospital surgery and recovery
 - Nursing services
 - Pharmacy
 - Rehabilitation / restoration therapy
 - Follow-up with new treatment plan
- 'Failure' of any one party negatively affects patient outcome

27

Extended Enterprise Information Problem

- *Effectiveness*
 - Practitioners need relevant information about the treatments, treatment plans & instructions of other providers:
 - Timeliness
 - Reliability
 - The Practitioners assume liability for the actions that they take on the basis of this information.
 - Practitioners need timely information about the outcomes related to their treatments
- *Efficiency*
 - Information acquisition is a secondary task (at best)
 - Health information has a low signal to noise ratio / Physician liability
- *Confidentiality*
 - Practitioners must share patient confidential information with multiple parties

28

Healthcare's Information Issues

Due to the structure of the US healthcare industry

- Information sharing primarily on a point by point basis
 - Every care provider maintains their own records for their own purpose (treatment, reimbursement, liability)
 - No consolidated record of care
 - Most complete record will be that of the health plan paying for (some) of the care. Significant timeliness and data quality issues with that record.
- Any one provider will have incomplete picture of patient's condition and treatment history
 - Omitted treatment | misdiagnosis | Negative interactions
 - Increased cost
 - ❖ Resulting in diminished patient outcomes

29

Historical Solutions

- Historical solutions
 - Family / primary physician
 - Coordinates care activity and thus information exchange, ie
 - Specialist is a consultant to the PCP
 - PCP is the admitting physician
 - Model broken by current reimbursement scheme
 - Health plan case manager
 - Receives information that support claims for reimbursement
 - Small subset / summary of clinical information
 - Patient
 - Carries a paper record; reports 'what my other docs say'
 - What worked for paper record less effective w electronic records
 - Reliance on the most motivated but least competent party in the care lifecycle

30

Emerging Solution

- Electronic Health Record
 - Repository for relevant medical history, medications, current conditions, orders, etc
 - 'virtual' record consolidating
 - *Standards based*
 - Made by consensus standards bodies (ie ANSI)
 - *Mandates* for use from Federal government through its (Medicare) purchasing power
- 3rd Party Health Information Exchanges
 - Facilitate location and acquisition of patient specific health information
 - Developed by commercial entities thru \$500M grant program
 - *Mandates* for use from Federal government through its (Medicare) purchasing power

31

Some remaining problems

- EHR & HIE support the availability of the required information; governance issues remain. How to ensure:
 - Providers effective use of the available information
 - Prevention of and responsibility for data misuse
 - HIE tends to obscure the context in which information was collected / limitation of standards
 - Data quality
 - Reduce error propagation
 - Care co-ordination
 - Leverage data for improved care quality (evidence based medicine)
- ❖ Important aspect of alignment regards taking advantage of new information and IT in support of corporate mission

32

Value Chain Governance Mechanisms

- Dominant customer asserting ownership of value chain
 - US Federal government through Medicare / Medicaid (40% of healthcare \$\$)
 - Business roundtable on behalf of major commercial purchasers
 - ⇒ health insurers =>
- 3rd party commercial 'health exchanges' creating collaboration of providers subject to use agreements
- Standards developed by value chain participants & vendors
- State and Federal Law

33

Outsourcers – the CGEIT view

- **IT Strategy – why are we outsourcing?**
 - How are the terms of the outsource contract controlled
- **Resource Management**
 - How do we insist the outsourcer manage certain resources
 - People
 - Infrastructure
 - Are there certain resources on which we *do not* wish to impose constraints?
- **Performance Measurement**
 - Do the defined performance measure elements touch all the important CGEIT bases?

34

Outsourcers – the CGEIT view, cont'd

- **Risk Management**
 - What specific elements of the outsourcer's contract deal with risk management...hint: look at the decision process – who makes which decisions – sort of a RACI chart view.
- **Value Delivery**
 - Is the outsourcer responsible for specific elements of value delivery ...*or*
 - Is the sponsoring senior executive responsible for the value ostensibly delivered through the outsourced relationship

35

Contract Employees – the CGEIT view

- **The classic “extended enterprise” case**
 - Moves real people from the line item “full time equivalents” to
 - Professional Services
- **Resource Management**
 - How will contract employees work alongside full-time staff?
 - How will their work be judged?
 - Who may make changes in the contract resource list and for what reasons?
 - What about training? Are contract employees paid their hourly rate for attending training?
 - Etc.

36

Contract Employees – the CGEIT view, cont'd

- **Performance Measurement**
 - Compare the measurement schemes for contractors versus full-time employees.
- **Risk Management**
 - Background checks for contractors?
 - Are contractors appropriately covered by insurance (E&O)
 - Bonded?
 - How are risky decisions made involving contractors?

37

SaaS* – the CGEIT perspective

- What data is moving to/from the SaaS provider?
- What Intellectual property is moving to/from the SaaS provider?
- How granularly are the service elements defined in the contract (e.g. transaction level responsiveness?)
- Does a move to SaaS violate the terms of existing contracts with other partners
- Does a move to SaaS give rise to new regulatory issues?
- ...plus all of the issues we discussed under “outsourcers”

*Software as a Service

38

Cloud Computing – CGEIT perspective

- **SaaS on steroids (from a governance perspective)**
- **Of special concern:**
 - Downstream cloud provider outsourcing – does that violate your contract?
 - Code signing
 - Special security steps: e.g. blanking memory or profoundly erasing media, etc.
- **What about billing?**
 - What will the bill contain for cloud services
 - How can we audit the bill?
 - Will the bill itself contain confidential information?
- **Probably much more – when we finally get a definition of cloud computing**

39

The Extended Governance Book

- **Deserves some serious study**
 - In many cases defines IT as it should be rather than what we're stuck with
- **Good discussion of strategy – not simply the extended enterprise perspective**
- **Touches on the concepts involved in “changing the organizational culture”**
 - A “trick question” issue for the CGEIT Exam
- **Not so good on governance elements, IMHO**

40

The Extended Governance Book, cont'd

- **Important perspectives on “Architecture”**
 - IT Architecture as a *primary communications tool*, and
 - Enterprise Architecture seen as a *vehicle to improve the process of making critical business decisions*
- ***The book is really only 100 pages long + another 100 pages of appendices...***

