Risk Governance
Week #1 – CRISC Exam Prep

Bill Pankey
Tunitas Group

Agenda

About ...
– Course
– CRISC Exam
– Me
– You

Common Risk View
Enterprise Foundations
Integrated Management
Risk Management Frameworks
– Standards
– Process
– Practice

Risk Governance
Top Challenges*

Accenture 2011 Risk Management Survey

Reducing costs 47%
Aligning with the overall business strategy 43%
Implementing regulatory demands 41%
Improving risk management and modeling 41%
Data management (availability, consistency, organization) 40%
Developing a risk culture 36%
Integrating Risk and Finance information and processes within the organization 34%
Retaining and sourcing resources and talent 31%
Developing risk metrics 30%
Availability of comprehensive technological solutions 30%
Raising risk management as a priority for executive leadership 30%
Improving reporting 27%
Collaborating with business units 26%
Identifying risk management value proposition 24%
Expanding the Chief Risk Officer’s role and view of risk 21%

*http://goo.gl/FVdo9

ISACA Starting Position

*IT risk is business risk*

– Affect on business strategy
  • Value creation / opportunity

– Preservation of asset value
  • Tangible & Intangible

⇒ Various information security risks, project risks, operational risks are not necessarily IT risks.
  • IT risk management requires relevance and alignment

⇒ IT risk more than just information security risk
  e.g., not achieving business value, service delivery problems, inflexible architecture
ISACA Starting Position

- Benefit Enablement Risk:
  - Lost opportunity to use IT to improve the effectiveness or efficiency of new or existing business process.
- Program / Project Delivery Risk:
  - Failure to deliver business value in projects or program
- Service Delivery Risk
  - Performance errors in the delivery of IT services. Information security errors.

ISACA Starting Position

IT Risk must be managed as an enterprise risk
- Reflect the enterprise risk appetite and culture
- Consolidate with other risk across organization
- Acquire business sign-off on control environment

=> IT risk management must adapt to the ERM context

What if ERM is immature or non-existent?
**ISACA Starting Position**

Effective IT Risk Management:
- Provides tone at the top
- Assigns personal accountability
- Provides accurate information in timely fashion
- Minimize impact of controls consistent with cost and benefit
- Promotes continuous improvement

*Are there workarounds?*

---

**CRISC Exam Prep**

**Class Lectures**
- Tonight
  - 1 session for each CRISC domain
    - Risk Identification & Assessment
    - Risk Response
    - Risk Monitoring
    - Control Design & Implementation
    - Control Monitoring
  - 1 session for exam strategy

2+ hours
Which of the following is the best measure of IT Risk Management success?
- Extra-ordinary IT-related expense
- # of threats mitigated
- Completeness of control catalog
- Low residual risk score
CRISC Exam

120 questions
- forced choice question
  • Select single best | “least bad” answer
- no deduction for incorrect answers
- 4 hours

Firewall between CRISC Test Enhancement Committee and ISACA study material \ education activity
- 8/9 CISA; 6/9 CISM; 4/9 CGEIT
- Jack Jones (FAIR inventor) committee chair

About You

Experienced professionals w/ diverse risk management responsibilities

x Industry Sector

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>

x Management Area

<table>
<thead>
<tr>
<th>Management Area</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td></td>
</tr>
<tr>
<td>Forensics</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
</tr>
<tr>
<td>IT rule compliance</td>
<td></td>
</tr>
<tr>
<td>Privacy compliance</td>
<td></td>
</tr>
<tr>
<td>ICS rule compliance</td>
<td></td>
</tr>
<tr>
<td>Market compliance</td>
<td></td>
</tr>
</tbody>
</table>
Agenda

About ...
  - Course
  - CRISC Exam
  - Me
  - You

Common Risk View
  - Enterprise Foundations
  - Integrated Management

Risk Governance Frameworks
  - Standards
  - Process
  - Practice

A Note on Language

Muddled risk lexicon
  - Many competing and sometimes conflicting definitions

Precision in language is desirable ... but it can be exclusionary

"Risk" refers to the likelihood (or frequency) and magnitude of loss that exists from a combination of asset(s), threat(s) and control conditions. As a derived value, it cannot take a plural form (i.e., “risks”). From ISACA CRISC pages

Goal is of IT risk management is the achievement of business objectives
  - Adapt to the language used by the business organization

But for CRISC test takers, caution is warranted.
Risk Governance

Risk accompanies the business strategy

– Board responsibility is to ensure that risk is commensurate with reward
– How does it accomplish this?

10 Best practices for risk governance*

1. Understand the company’s key drivers of success.
2. Assess the risk in the company’s strategy.
3. Define the risk-oversight role of the full board and its standing committees.
4. Consider whether the company’s risk management system—including people and processes—is appropriate and has sufficient resources.
5. Work with management to understand and agree on the types (and format) of information the board requires.
6. Encourage a dynamic and constructive risk dialogue between management & board.
7. Closely monitor the potential risks in the company’s culture and its incentive structure.
8. Monitor critical alignments—of strategy, risk, controls, compliance, incentives, and people.
9. Consider emerging and interrelated risks: What’s around the next corner?
10. Periodically assess the board’s risk oversight processes: Do they enable the board to achieve its risk oversight objectives?

*National Association of Corporate Directors “Risk Governance: Balancing Risk & Reward”

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in the Tunitas Group CRISC Exam Preparation Class. No other use is permitted without express written authorization.
What is Risk?

Different answers will affect risk management objectives & practices

- Volatility of outcome
  - Variance about an expected outcome (e.g., as in finance)
- Expected outcome
  - Anticipated average loss (e.g., as in information security)
- Potential positive or negative outcome
  - PMI BOK and ISACA
  - Undefined in law & regulation

*of course, the conundrum is exacerbated by a plethora of measurement methods*

What is Risk?

Two essential aspects: uncertainty & loss

Oxford Dictionary: The possibility that something unpleasant or unwelcome will happen.

Counter to alternative definitions that will routinely be encountered

- Risk has to include possibility of loss
- Risk has only losses. Gains are opportunities.
- Risk is not synonymous with volatility

Risk is *vector valued*, not the product of probability and outcome

- *Assumption* of risk neutrality conflicts with the intended support for organization risk preferences and appetite.
What is Risk Management

Enterprise risk management is*:

*a process, ... applied ... across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

4 categories of objectives:

– Strategic. High level goals, mission
– Operations. Resource optimization
– Reporting. Reliability of management information
– Compliance. Satisfaction of laws and regulation


COSO Governance Concepts

• Internal environment
  
  Tone, risk management philosophy, appetite & tolerance

• Objective setting
  
  Risk management process, roles & responsibilities

• Monitoring
  
  Ongoing management reporting & adjustment
Risk Philosophy

Not a term of art well defined in standards

Generally, the organizational attitude toward risk

– Perceive value or risk management: mitigation, avoidance, etc.

– Expressed though a collection of risk related attributes (e.g., appetite and tolerance)

Risk Appetite

Boundaries of risk ‘acceptance’

– “amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity’s risk management philosophy, and in turn influences the entity’s culture and operating style”

– effectively establishes the enterprise mitigation policy

Determined by:

– Objective ability to absorb loss

– Management philosophy & culture

– External influences

  • Laws and regulation

  • Customer expectation

Changes over time
Risk Map

EXAMPLE
Risk Appetite

Appetite => risk policy

Really UnAcceptable: far beyond normal risk appetite; respond immediately.
UnAcceptable: above normal risk appetite; additional mitigation within time boundaries.
Acceptable: No special action beyond maintaining current control
Opportunity: Very low risk, cost saving or other opportunity gained from relaxing control or assuming more risk

Healthcare “Sentinel Events”

Events that should never occur in a hospital, e.g.:
- Wrong side surgery. Wrong patient surgery.
- Patient death or disability due to contaminated drugs, devices, biologics
- Patient death or disability due to medication error
- Paten suicide
- Large breaches of confidential patient data

Trigger immediate response process
- Formal root cause analysis
- Mandatory corrective action plan
- Mandatory reporting to oversight agencies (for some)

IT risk management relevance
- Map IT events upon to sentinel events
- Little or No appetite (‘unacceptable’ or ‘really unacceptable’) for information system events that could result in a sentinel event
Risk Tolerance

Less useful, perhaps

- “Risk tolerances relate to the entity’s objectives. Risk tolerance is the acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective.”

For example, measures of shortfall that the organization will ‘satisfice’.

Practice Question

An organization that recently suffered a catastrophic loss should:

A. Change the level of acceptable risk
B. Change the level of unacceptable risk
C. Re-evaluate probabilities
D. Re-evaluate impact
Awareness & Communication

Transparency does not mean the unmanaged communication of:

- Risk strategy / appetite
- Actual level of risk
- Risk management process and issues

Support ‘risk aware’ decisions

Seek to avoid

- Overconfidence
- Perception that the organization is hiding something from stakeholders (internal or external)
- Perception that risk is not ‘well managed’

Risk Management Roles

Objective Setting

Board
  Establish common risk view / risk appetite
CEO
  Manage risk
Risk Officer
  Collect data and report
Business Management
  Risk aware decisions
  Analyze risk
  Maintain risk profile
IT Management
  Support all risk management activity in a secondary role
Business Process Owner
  React to events
Control Functions
  Support all risk management activity
HR
  Communicate common risk view
Audit
  Communicate common risk view
  React to events

“business monarchy”
Risk acceptance is managed as a risk governance activity.

[Diagram of Risk IT Process Model]

Risk IT Artifacts

[Table and chart]

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in the Tunitas Group CRISC Exam Preparation Class. No other use is permitted without express written authorization.
Common Risk View

Develop risk management framework

- Determine how to integrate IT risk into strategic plans
- Classify IT risk factors, events and potential impact
- Define risk rating scales and control categories
- Determine IT risk tolerance and appetite
- Embed existing enterprise-wide risk management principles and views

Business Relevance of IT Event

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in the Tunitas Group CRISC Exam Preparation Class. No other use is permitted without express written authorization.
Business Relevant Categories for Expressing the Impact of Adverse Events

Extended information criteria (COBIT)
- Efficacy
- Efficiency
- Confidentiality
- Integrity
- Availability
- Reliability
- Compliance

Factor Analysis of Information Risk (FAIR)
- Productivity
- Response cost
- Replacement
- Competitive Advantage
- Legal
- Reputation

Extended Balanced Scorecard
- Financial
  - Share Value
  - Profit
  - Revenue
  - Cost of Capital
- Customer
  - Market share
  - Customer satisfaction
  - Customer Service
- Internal
  - Regulatory Compliance
- Growth
  - Competitive advantage
  - Reputation

COSO ERM
- Strategic
- Operations
- Reporting
- Compliance

Healthcare Provider*
- Patient Care
- Logistics
- Reputation
- Regulatory Compliance
- Financial / Billing

Westerman’s 4A's
- Agility
- Accuracy
- Access
- Availability

Integrate with ERM

Risk IT Governance Domain

- Ensure appropriate business involvement in IT risk committees
- Ensure IT involvement in enterprise business risk committee
- Coordinate IT incident response plans with business response plans
- Harmonize risk categories, methods, scales, etc with ERM methods

Figure 26—Process RG2 Integrate with ERM

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in the Tunitas Group CRISC Exam Preparation Class. No other use is permitted without express written authorization.
Risk Aware Decisions

- Sell the business value of IT risk analysis data and results to business decision makers
- Review analysis results with business owners to ensure coordinated response (business and IT)
- Obtain business sign-off of residual risk.

Governance Metrics

A wicked problem
- Need to assume that risk is appropriately analyzed and assessed, in order to determine that it is appropriately managed. However, an indication of poor risk management is misunderstood or poorly assessed risk.

ISACA IT risk governance metric
- Recourse to enterprise [business] risk metrics. Presumably more ‘objective’ ($$$)
- Presumes grand experiment (strategic use of IT or not)
- Correlate enterprise and IT risk measures

Copyright ©2011 Tunitas Group. All rights reserved. This presentation material may be used solely by participants in the Tunitas Group CRISC Exam Preparation Class. No other use is permitted without express written authorization.
Agenda

About ...
- Course
- CRISC Exam
- Me
- You

Common Risk View
Enterprise Foundations
Integrated Management

Risk Governance

Risk Management Frameworks
- Standards
- Process
- Practice

ERM Frameworks

COSO ERM
Special status due to specific mention in Sarbanes-Oxley law.
Often imprecise, i.e. does not define ‘risk’
Difficult to understand?

ISO 31000 Risk Management Framework ($$)
- Based on AS/NZ 4360 (free for download)
- Procedural framework for identification analysis and treatment of generic risk
- Intended to harmonize risk management processes, support existing standards (e.g. ISO 27005)
- Risk defined as “effect of uncertainty of objectives”
NIST RMF

NIST Risk Management Framework that is replacing NIST C&A processes (SP 800 37)

Interesting (or not) features:

- All of the information about business objectives and impacts, encapsulated in the classification of information and systems
- Controls selected on basis of classification and deployment environment
- Control effectiveness is assessed before systems are authorized to maintain or process classified data

Designed for managing information security

- Could be adapted to IT risk generally (???)

Risk IT Practitioner Guide

Closely aligned with Risk IT

A “Guide’ without pretention to be a ‘standard, set of heuristics

Recommended for concrete, actionable advice, e.g.
- risk scenario construction
- risk maps

Free download for ISACA members from ISACA.org.
- $115 otherwise