Presentation on

IT Risk Management – Practical approach

by

CA A. Rafeq, FCA, CISA, CIA, CCSA, CGEIT
Past President, ISACA, Bangalore Chapter
Member, CobiT 5.0 Task Force and CGEIT Certification Committee, ISACA, USA

10th October 2009
at
VITS Hotel & National Insurance Academy, Baner, Pune India
Agenda

• Understand ISACA’s IT-related risk management framework, Risk IT and key IT risk issues

• Discuss current standards and frameworks and which elements they are still lacking

• Comprehend how ISACA’s new framework addresses these issues and gaps

• Understand COBIT’s relationship to risk management and how to implement Risk Management
1. Understand ISACA’s IT-related risk management framework, Risk IT and key IT risk issues
Need for IT risk Management

- Key elements of enterprise governance:
  - Need for assurance about the value of IT
  - Management of IT-related risks and
  - Increased requirements for control over information

- Value, risk and control constitute the core of IT governance.

- Timely information to make difficult decisions on value, risk and control quickly and successfully: What should be measured, and how?

- Enterprises need an objective measure of where they are and where improvement is required, and they need to implement a management tool kit to monitor this improvement.

- To implement IT governance and related practices always links back to the risks that will be remediated or the value that will be added.

- Recent survey shows that 80 percent of the respondents believe that IT risk management is important.
Managing Information Technology

**Expectations**

- Harness and exploit IT to deliver business value
- Provide fast development, with appropriate quality and with security
- Ascertain that IT investments have a quantitative return and IT does more with less
- Move from efficiency and productivity gains towards value creation and business effectiveness, especially in industries requiring that the focus move from the back office to the front office

**Reality - The Risks**

- Business losses, reputational damage or a weakened competitive position
- Enterprise effectiveness and core processes directly impacted by the quality of IT deliverables
- The failure of IT initiatives intended to bring innovation to the enterprise to achieve their promise
- Technology that is inadequate for the enterprise or obsolete too soon
- Poor support for the business
- Deadlines that are not met
- Costs that are higher than expected and quality and efficiency lower than anticipated
Risk Management requirements

- Risk awareness by senior corporate officers

- Clear understanding of the enterprise’s appetite for risk

- Understanding of:
  - Compliance requirements
  - Transparency about the significant risks to the enterprise
  - Embedding of risk management responsibilities into the organisation

- Implementing risk management requires that a risk management framework is created and maintained.
Risk Management framework

- Documents a common and agreed-upon level of:
  - IT risks
  - Mitigation strategies and
  - Residual risks.

- Any potential impact on the goals of the organisation caused by an unplanned event is:
  - Identified
  - Analysed
  - Assessed.

- Risk mitigation strategies are adopted to minimise residual risk to an accepted level.

- Result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.
Basic process steps of risk management

Establish the context

Identify the risks

Analyse the risks

Evaluate the risks

Treat the risks
Risk IT Framework Overview

Enterprises Risk: Identify, Govern and Manage IT Risk

The Risk IT Framework
# Table of Contents

Foreword .................................................................................................................................................. 7  
1. Risk IT Framework—Purpose and Target Audience ............................................................................. 11  
   Definition of IT Risk ............................................................................................................................... 11  
   Purpose of the Risk IT Framework ........................................................................................................... 11  
   Intended Audiences and Stakeholders ...................................................................................................... 12  
   Benefits and Outcomes .............................................................................................................................. 13  
2. Risk IT Principles ...................................................................................................................................... 14  
3. Responsibilities and Accountability for IT Risk ..................................................................................... 16  
4. Awareness and Communication ............................................................................................................... 18  
   Awareness and Communication Benefits ................................................................................................. 18  
   Risk Awareness—Risk Culture .................................................................................................................. 18  
   Risk Communication—What to Communicate? ......................................................................................... 18  
   Risk Communication—Stakeholders ........................................................................................................... 20  
5. Responding to IT Risk .............................................................................................................................. 21  
   Risk Response Selection and Prioritisation ............................................................................................... 21  
6. Risk and Opportunity Management Using COBIT, Val IT and Risk IT .................................................... 23  
7. The Risk IT Framework Components ....................................................................................................... 26  
8. The Risk IT Foundation ........................................................................................................................... 27  
   Risk Scenarios .......................................................................................................................................... 27  
   Describing Business Impact ...................................................................................................................... 28  
   Key Risk Indicators .................................................................................................................................... 28  

**IT risk always exists, whether or not it is detected or recognised by an organisation.**
**Table of Contents**

9. The Risk IT Process Model ................................................................. 30
10. Managing Risk in Practice—The Techniques Guide Overview .................................................. 31
11. Description of the Risk IT Framework ............................................................................... 32
    Introduction .................................................................................... 32
    Detailed Process Descriptions ...................................................... 32
    Management Guidelines .................................................................. 33
    Maturity Models ........................................................................... 36
12. The Risk IT Framework ........................................................................ 38
    Risk Governance ........................................................................... 39
        RG1 Establish and Maintain a Common Risk View ................... 40
        RG2 Integrate With ERM .......................................................... 46
        RG3 Make Risk-aware Business Decisions ............................... 51
        Domain Maturity Model (RG) .................................................... 55
    Risk Evaluation ............................................................................... 59
        RE1 Collect Data ........................................................................ 60
        RE2 Analyse Risk ...................................................................... 63
        RE3 Maintain Risk Profile ......................................................... 67
        Domain Maturity Model (RE) ..................................................... 71
    Risk Response ................................................................................ 75
        RR1 Articulate Risk .................................................................... 76
        RR2 Manage Risk ...................................................................... 80
        RR3 React to Events .................................................................. 84
        Domain Maturity Model (RR) ..................................................... 88
 Appendix—Overview of Reference Materials ................................................................................. 92
 Table of Figures .................................................................................. 94
### Types of Risks

<table>
<thead>
<tr>
<th>IT Benefit (Value) Enablement</th>
<th>IT Solution (Project) Delivery</th>
<th>IT Service Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology enabler for new business initiatives</td>
<td>Projects quality</td>
<td>IT Service interruptions</td>
</tr>
<tr>
<td>Technology enabler for efficient operations</td>
<td>Projects relevance</td>
<td>Security problems</td>
</tr>
<tr>
<td></td>
<td>Projects overrun</td>
<td>Compliance issues</td>
</tr>
</tbody>
</table>

#### Business Value
- **Business Value**: Fail to Gain, Gain, Lose, Preserve
Risk Management Principles

The Risk IT framework principles are:

- Effective enterprise governance of IT risk:
  - Always connects to business objectives
  - Aligns the management of IT-related business risk with overall enterprise risk management
  - Balances the costs and benefits of managing risk

- Effective management of IT risk:
  - Promotes fair and open communication of IT risk
  - Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
  - Is a continuous process and part of daily activities
Building Blocks of good IT Risk Management

Based on these principles, the key building blocks of good IT risk management are defined as follows:

- Set responsibility for IT risk management.
- Set objectives and define risk appetite and tolerance.
- Identify, analyse and describe risk.
- Monitor risk exposure.
- Treat IT risk.
- Link with existing guidance to manage risk.
Risk Management – Governance perspective

- Risk Governance
  - Establish and Maintain a Common Risk View
  - Integrate with Enterprise Risk Management
  - Make Risk-aware Business Decisions
- Risk Evaluation
  - Collect Data
  - Analyse Risk
  - Maintain Risk Profile
- Risk Response
  - Articulate Risk
  - Manage Risk
  - React to Events
Benefit of Risk IT framework

The Risk IT framework explains IT risk and will enable users to:

- Integrate the management of IT risk into the overall enterprise risk management of the organisation
- Make well-informed decisions about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
- Understand how to respond to the risk
2. Discuss current standards and frameworks and which elements they are still lacking
ERM Defined:

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The ERM Framework

- Entity objectives can be viewed in the context of four categories:
  - Strategic
  - Operations
  - Reporting
  - Compliance
Risk Analysis

Risk Assessment
- Identification
- Measurement
- Prioritization

Risk Management
- Control It
- Share or Transfer It
- Diversify or Avoid It

Risk Monitoring
- Process Level
- Activity Level
- Entity Level
3. Comprehend how ISACA’s new framework addresses these issues and gaps
<table>
<thead>
<tr>
<th>Role</th>
<th>Benefits of Reasons for Using the Risk IT Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boards and executive management</td>
<td>Better understanding of their responsibilities and roles with regard to IT risk management</td>
</tr>
<tr>
<td>Corporate risk managers (for enterprise risk management)</td>
<td>Assistance with managing IT risk, in line with generally accepted enterprise risk management principles</td>
</tr>
<tr>
<td>Operational risk managers</td>
<td>Linkage of their framework to Risk IT; identification of operational losses or development of key risk indicators</td>
</tr>
<tr>
<td>IT management</td>
<td>Better understanding of how to identify and manage IT risk and how to communicate IT risk to business decision makers</td>
</tr>
<tr>
<td>IT service managers</td>
<td>Enhancement of their already good view of more operational IT-related risks, which should fit into an overall IT risk management framework</td>
</tr>
<tr>
<td>Business continuity managers</td>
<td>Alignment with enterprise risk management (since assessment of risk is a key aspect of their responsibility)</td>
</tr>
<tr>
<td>IT security managers</td>
<td>Positioning of security risk amongst other categories of IT risk</td>
</tr>
<tr>
<td>Chief financial officers (CFOs)</td>
<td>Gaining a better view of IT-related risk and its financial implications</td>
</tr>
<tr>
<td>Enterprise governance officers</td>
<td>Assistance with their review and monitoring of governance responsibilities and other IT governance roles</td>
</tr>
<tr>
<td>Business managers</td>
<td>Understanding and management of IT risk—one of many business risks, all of which should be aligned</td>
</tr>
<tr>
<td>IT auditors</td>
<td>Better analysis of risk in support of audit plans and reports</td>
</tr>
<tr>
<td>Regulators</td>
<td>Support of their assessment of regulated enterprises’ IT risk management approach</td>
</tr>
<tr>
<td>External auditors</td>
<td>Additional guidance on IT-related risk levels when establishing an opinion over the quality of internal control</td>
</tr>
<tr>
<td>Insurers</td>
<td>Support in establishing adequate IT insurance coverage and seeking agreement on risk levels</td>
</tr>
<tr>
<td>Rating agencies</td>
<td>In collaboration with insurers; a reference to objectively assess and rate how an enterprise is dealing with IT risk</td>
</tr>
</tbody>
</table>
Risk Scenarios

- **Actor**
  - Internal (Staff, Contractor)
  - External (Competitor, Outsider, Business partner, Regulator, Market)

- **Action**
  - Disclosure
  - Interruption
  - Modification
  - Theft
  - Destruction
  - Ineffective design
  - Ineffective execution
  - Regulation
  - Inappropriate use

- **Asset/Resource**
  - People & Organisation
  - Process
  - Infrastructure (Facilities, IT Infrastructure)
  - Enterprise Architecture Components (Information, Technology, Applications)

- **Threat Type**
  - Malicious
  - Accidental
  - Failure
  - Natural

- **Time**
  - Duration
  - Timing of occurrence (Critical, Non-Critical)
  - Timing to detect
<table>
<thead>
<tr>
<th>Technique/Guidance</th>
<th>Domain/Process</th>
<th>Risk Governance</th>
<th>Risk Evaluation</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RG1 Establish and Maintain a Common Risk View</td>
<td>RG2 Integrate with Enterprise Risk Management</td>
<td>RG3 Make Risk-aware Business Decisions</td>
<td>RE1 Collect Data</td>
</tr>
<tr>
<td>1. Defining a risk universe and scoping</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Constructing risk scenarios</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Sample generic IT risk scenarios</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Describing risk—expressing impact in business terms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Describing risk—COBIT business goals mapping with other impact criteria</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Describing risk—qualitative and quantitative methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Describing risk—expressing impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Describing risk—expressing frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Risk factors in the risk assessment process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Describing risk—risk maps, risk register?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Defining risk appetite and risk tolerance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. A risk analysis workflow</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Risk aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Key risk indicators and risk reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Risk response and prioritisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Using COBIT and Val IT to map controls to risk scenarios</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Risk profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. Risk communication flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix I—How COBIT and Val IT practices can help manage risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix II—Risk management principles and practices in Risk IT vs. other frameworks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Process RG1:
Establish and maintain a common risk view

Process Goal:
Ensure that risk management activities align with the organization's objective capacity for IT-related loss and leadership's subjective tolerance.

Key Activities:
RGL.1 Develop an enterprise-specific IT risk management framework
RGL.2 Develop IT risk management methods
RGL.3 Perform an enterprise-wide IT risk assessment
RGL.4 Propose IT risk tolerance thresholds
RGL.5 Approve IT risk tolerance
RGL.6 Align policy and standards statements with IT risk tolerance
RGL.7 Promote an IT risk-aware culture
RGL.8 Promote effective communication of IT risk

© 2008 ITGI
4. Understand COBIT’s relationship to risk management and how to implement Risk Management
Figure 2—IT Governance Focus Areas

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.

- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.

- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.
IT Risk Management

The board should manage enterprise risk by:

- Ascertaining that there is **transparency** about the significant risks to the organisation
- Being aware that the final **responsibility** for risk management rests with the board
- Being conscious that risk mitigation can generate **cost-efficiencies**
- Considering that a proactive risk management approach creates **competitive advantage**
- Insisting that risk management is **embedded in the operation** of the enterprise

“It is the IT alligators you do not see that will get you!”
IT Risk Management

Risk Management Expands….

• Risk Allocation - contracts, SLAs, etc.
• Risk Mitigation - security & control practices
• Risk Transfer - insurance & liability
• Risk Assurance - audit & certification
• Risk Acceptance - formal, transparent

"Wisdom consists in being able to distinguish among dangers and make a choice of the least harmful."

—Niccolo Machiavelli
Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analyzing and communicating IT risks and their potential impact on business processes and goals

by focusing on

development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

is achieved by

• Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
• Performing risk assessments
• Recommending and communicating risk remediation action plans

and is measured by

• Percent of critical IT objectives covered by risk assessment
• Percent of identified critical IT risks with action plans developed
• Percent of risk management action plans approved for implementation
CONTROL OBJECTIVES

P09 Assess and Manage IT Risks

P09.1 IT Risk Management Framework
Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.

P09.2 Establishment of Risk Context
Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.

P09.3 Event Identification
Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.

P09.4 Risk Assessment
Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

P09.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

P09.6 Maintenance and Monitoring of a Risk Action Plan
Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.
# Management Guidelines

**P09 Assess and Manage IT Risks**

<table>
<thead>
<tr>
<th>From</th>
<th>Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Strategic and tactical IT plans, IT service portfolio</td>
</tr>
<tr>
<td>P010</td>
<td>Project risk management plan</td>
</tr>
<tr>
<td>D52</td>
<td>Supplier risks</td>
</tr>
<tr>
<td>D54</td>
<td>Contingency test results</td>
</tr>
<tr>
<td>D55</td>
<td>Security threats and vulnerabilities</td>
</tr>
<tr>
<td>ME1</td>
<td>Historical risk trends and events</td>
</tr>
<tr>
<td>ME4</td>
<td>Enterprise appetite for IT risks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>P01, D54, D55, D512, ME4</td>
</tr>
<tr>
<td>Risk reporting</td>
<td>ME4</td>
</tr>
<tr>
<td>IT-related risk management guidelines</td>
<td>PO6</td>
</tr>
<tr>
<td>IT-related risk remedial action plans</td>
<td>PO4, A16</td>
</tr>
<tr>
<td>Activities</td>
<td>CPO</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Determine risk management alignment (e.g., assess risk).</td>
<td>A</td>
</tr>
<tr>
<td>Understand relevant strategic business objectives.</td>
<td></td>
</tr>
<tr>
<td>Understand relevant business process objectives.</td>
<td></td>
</tr>
<tr>
<td>Identify internal IT objectives, and establish risk context.</td>
<td></td>
</tr>
<tr>
<td>Identify events associated with objectives (some events are business-oriented; some are IT-oriented [IT is A, business is C]).</td>
<td>I</td>
</tr>
<tr>
<td>Assess risk associated with events.</td>
<td></td>
</tr>
<tr>
<td>Evaluate and select risk responses.</td>
<td>I</td>
</tr>
<tr>
<td>Prioritise and plan control activities.</td>
<td>C</td>
</tr>
<tr>
<td>Approve and ensure funding for risk action plans.</td>
<td>A</td>
</tr>
<tr>
<td>Maintain and monitor risk action plan.</td>
<td>A</td>
</tr>
</tbody>
</table>

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.
**Goals and Metrics**

**IT**
- Protect the achievement of IT objectives.
- Establish clarity on the business impact of risks to IT objectives and resources.
- Account for and protect all IT assets.

**Process**
- Establish and reduce the likelihood and impact of IT risks.
- Establish cost-effective action plans for critical IT risks.

**Activities**
- Ensuring that risk management is fully embedded in management processes.
- Performing regular risk assessments with senior managers and key staff members.
- Recommending and communicating risk remediation action plans.

**Metrics**
- Percent of critical IT objectives covered by risk assessment.
- Percent of IT risk assessments integrated in the IT risk assessment approach.

- Percent of identified critical IT events that have been assessed.
- Number of newly identified IT risks (compared to previous exercise).
- Number of significant incidents caused by risks that were not identified by the risk assessment process.
- Percent of identified critical IT risks with an action plan developed.

- Percent of IT budget spent on risk management (assessment and mitigation) activities.
- Frequency of review of the IT risk management process.
- Percent of approved risk assessments.
- Number of actioned risk monitoring reports within the agreed-upon frequency.
- Percent of identified IT events used in risk assessments.
- Percent of risk management action plans approved for implementation.
Plan and Organise
Assess and Manage IT Risks

Maturity Model

P09 Assess and Manage IT Risks

Management of the process of Assess and manage IT risks that satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals is:

0 Non-existent when
Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial/Ad Hoc when
IT risks are considered in an ad hoc manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2 Repeatable but Intuitive when
A developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.
3 Defined when
An organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual’s discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

4 Managed and Measurable when
The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.

5 Optimised when
Risk management develops to the stage where a structured, organisationwide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.
### IT Risks

<table>
<thead>
<tr>
<th>Value Drivers</th>
<th>Risk Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consistent approach for IT risk management</td>
<td></td>
</tr>
<tr>
<td>• Effective management of IT risks</td>
<td></td>
</tr>
<tr>
<td>• Continuous evaluation of current IT risks and threats to the organisation</td>
<td></td>
</tr>
<tr>
<td>• Broadened IT risk management approach</td>
<td></td>
</tr>
<tr>
<td>• IT risks and business risks managed independently</td>
<td></td>
</tr>
<tr>
<td>• The impact of an IT risk on the business undetected</td>
<td></td>
</tr>
<tr>
<td>• Lack of cost control for risk management</td>
<td></td>
</tr>
<tr>
<td>• Each risk seen as a single threat rather than in an overall context</td>
<td></td>
</tr>
<tr>
<td>• Ineffective support for risk assessment by senior management</td>
<td></td>
</tr>
</tbody>
</table>

Framework fits with the risk management objectives of the enterprise. Use similar risk classification principles and, wherever possible in a business-driven hierarchy, for example:
Case study

Maturity level assessment of Risk Assessment Process using CobiT maturity model
<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Sl. No.</th>
<th>Ideal Score</th>
<th>Maturity Statement</th>
<th>Not at all</th>
<th>Some what</th>
<th>Largely</th>
<th>Completely</th>
<th>Item Gap</th>
<th>Average Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Risk assessment for processes and business decisions does not occur.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 0</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>IT risks are considered in an ad hoc manner.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>Informal assessments of project risk take place as determined by each project.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0</td>
<td>Specific IT-related risks such as security, availability and integrity are occasionally considered on a project-by-project basis.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0</td>
<td>IT-related risks affecting day-to-day operations are seldom discussed at management meetings.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0</td>
<td>Where risks have been considered, mitigation is inconsistent.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>0</td>
<td>There is an emerging understanding that IT risks are important and need to be considered.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>An immature and developing risk assessment approach exists and is implemented at the discretion of the project managers.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>The risk management is usually at a high level and is typically applied only to major projects or in response to problems.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>Risk mitigation processes are starting to be implemented where risks are identified.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Level 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An organisation wide risk management policy defines when and how to conduct risk assessments.</td>
<td></td>
<td></td>
<td>0.333</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>-----------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Risk management follows a defined process that is documented.</td>
<td></td>
<td></td>
<td>0.000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Risk management training is available to all staff.</td>
<td>✓</td>
<td>✓</td>
<td>0.667</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>Decisions to follow the risk management process and to receive training are left to the individual's discretion.</td>
<td>✓</td>
<td></td>
<td>0.333</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified.</td>
<td></td>
<td>✓</td>
<td>0.333</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>A process to mitigate key risks is usually instituted once the risks are identified.</td>
<td>✓</td>
<td></td>
<td>0.000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>Job descriptions consider risk management responsibilities.</td>
<td></td>
<td>✓</td>
<td>0.000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Level 3** 0.238

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>The assessment and management of risk are standard procedures.</th>
<th></th>
<th></th>
<th>1.000</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>Exceptions to the risk management process are reported to IT management</td>
<td></td>
<td>✓</td>
<td>0.333</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>IT risk management is a senior management-level responsibility.</td>
<td></td>
<td>✓</td>
<td>0.000</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation.</td>
<td>✓</td>
<td></td>
<td>0.667</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios.</td>
<td>✓</td>
<td></td>
<td>0.667</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept.</td>
<td>✓</td>
<td></td>
<td>0.667</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>All identified risks have a nominated owner, and senior management and IT management have determined the levels of risk that the organisation will tolerate.</td>
<td>✓</td>
<td></td>
<td>0.667</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>IT management has developed standard measures for assessing risk and defining risk/return ratios.</td>
<td>✓</td>
<td></td>
<td>1.000</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>Management budgets for an operational risk management project to reassess risks on a regular basis.</td>
<td></td>
<td>✓</td>
<td>1.000</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>A risk management database is established and part of the risk management processes is beginning to be automated.</td>
<td>✓</td>
<td></td>
<td>0.667</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>IT management considers risk mitigation strategies.</td>
<td></td>
<td>✓</td>
<td>0.000</td>
</tr>
</tbody>
</table>

**Level 4** 0.606
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Description</th>
<th>Score</th>
<th>Maturity Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>Risk management has developed to the stage where a structured, organisationwide process is enforced and well managed.</td>
<td>✓</td>
<td>1.000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Good practices are applied across the entire organisation.</td>
<td>✓</td>
<td>0.867</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>The capturing, analysis and reporting of risk management data are highly automated.</td>
<td>✓</td>
<td>1.000</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Guidance is drawn from leaders in the field and the IT organisation takes part in peer groups to exchange experiences.</td>
<td>✓</td>
<td>0.333</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Risk management is truly integrated into all business and IT operations, is well accepted, and extensively involves the users of IT services</td>
<td>✓</td>
<td>1.000</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Management will detect and act when major IT operational and investment decisions are made without consideration of the risk management plan.</td>
<td>✓</td>
<td>0.333</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>Management continually assesses risk mitigation strategies.</td>
<td>✓</td>
<td>0.867</td>
</tr>
</tbody>
</table>

**Level 5**

**Maturity Score**

**Target Score by March 2008** 4+
Walk-through of templates

• Risk Assessment Template
• Risk assessment examples
• Risk treatment examples

• Using CobiT for Risk Analysis for BCP
• Asset classification
• Vulnerability analysis
Summary: IT Risk Management – Governance perspective

- Be driven by stakeholder value
- Adopt an governance framework – Risk-IT
- Ask the right questions
- Focus on IT’s
  - Alignment with the business
  - Value delivery
  - Risk management
- Measure results
- Use appropriate frameworks and best practices
- Adapt as required
Questions?
Thank you!
rafeq@vsnl.com
Primary Reference:
www.isaca.org

IT risk always exists, whether or not it is detected or recognised by an organisation.