IT Scenario Analysis in Enterprise Risk Management

Scenarios are a powerful tool in a risk manager’s armory—they help professionals ask the right questions and prepare for the unexpected. Scenario analysis has become a ‘new’ and best practice in enterprise risk management (ERM) (see figure 1). Scenario analysis is also a centrepiece of ISACA’s Risk IT framework.1, 2

Risk scenario analysis is a technique to make IT risk more concrete and tangible and to allow for proper risk analysis and assessment.3 It is a core approach to bring realism, insight, organisational engagement, improved analysis and structure to the complex matter of IT risk.

**SCENARIO ANALYSIS FLOW**

One of the challenges for IT risk management is to identify the relevant risks amongst all that can go wrong. A technique to overcome this challenge is the development and use of risk scenarios. Once these scenarios are developed, they are used during the risk analysis, in which the frequency of the scenarios occurring and the business impacts are estimated.

**Figure 2** shows that IT risk scenarios can be derived two different ways:

- **A top-down approach**, in which one starts from the overall business objectives and performs an analysis of the most relevant and probable IT risk scenarios that are impacting the business objectives
- **A bottom-up approach**, in which a list of generic scenarios is used to define a set of more concrete and customised scenarios

The approaches are complementary and should be used simultaneously. Indeed, risk scenarios must be relevant and linked to real business risks. On the other hand, using a set of example generic risk scenarios helps ensure that no risks are overlooked and provides a more comprehensive and complete view of IT risk.

The following is a practical approach that has been proven helpful in developing a set of relevant and important risk scenarios:

1. Use a list of example generic risk scenarios4 to define an initial set of concrete risk scenarios for the organisation.

2. Perform a validation against the business objectives of the organisation.

3. Refine the selected scenarios based on the validation; categorise them to a level in line with the criticality5 of the organisation.

4. Reduce the number of scenarios to a manageable set.6

5. Keep all risks in a list so they can be re-evaluated in the next iteration and included for detailed analysis if they have become relevant at that time.

6. Include ‘unspecified event’ in the scenarios to address incidents that are not covered by the specified scenarios. Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, frequency and impact of the scenario are assessed. Important components of this assessment are the risk factors, which are described in the next section.

This is not rocket science, so why do organisations fail to use risk scenarios more often and routinely? Keep in mind that scenarios are in fact harder to develop than they seem. A good scenario takes time to build and requires good input from a number of areas of the enterprise; therefore, a whole set takes a large investment of time and energy.

**RISK FACTORS**

Risk factors are factors that influence the frequency and/or business impact of risk scenarios. They can be of different natures and can be classified in two major categories:

- **Environmental factors**, which can be divided into internal and external factors—the difference being the degree of control an enterprise has over them:
  - Internal environmental factors are, to a large extent, under the control of the enterprise.
  - External environmental factors are, to a large extent, outside the control of the enterprise.
- **Capabilities**, i.e., how good the enterprise is in a number of IT-related activities. They can be distinguished in line with ISACA’s three major frameworks:

---

**Urs Fischer, CISA, CRISC, CPA Swiss**, is an independent IT governance, risk and compliance consultant. From 2003 to 2010, he was vice president and head of IT governance and risk management for the Swiss Life Group. Previously, he was head of IT audit for the Swiss Life Audit Department based in Zurich, Switzerland. Since 1989, Fischer has worked in the IT governance, audit and security areas and has gained extensive IT governance, risk management and information systems compliance experience. Involved in the development of COBIT® 4.0 and 4.1, he is also helping with the development of COBIT 5. A member of ISACA’s Guidance and Practice Committee, in June 2010, he received the John Lainhart IV Award from ISACA.

---

**Do you have something to say about this article?**

Visit the Journal pages of the ISACA web site ([www.isaca.org/journal](http://www.isaca.org/journal)), find the article, and choose the Comments tab to share your thoughts.
Figure 1—Risk Analysis and Risk Response Overview

Risk Analysis

Estimate Frequency and Impact

Risk

Risks Exceeding Risk Tolerance Level

Parameters for Risk Response Selection
- Cost of Response to Reduce Risk Within Tolerance Levels
- Importance of Risk
- Capability to Implement Response
- Effectiveness of Response
- Efficiency of the Response

Select Risk Response Options


Prioritise Risk Response Options

Prioritised Risk Responses

Risk Action Plan

Risk Tolerance


Figure 2—IT Risk Scenario Development

Top-down Scenario Identification

- Identify business objectives.
- Identify scenarios with the most impact on the achievement of objectives.

Business Objectives

- Identify all hypothetical scenarios.
- Reduce risks through high-level analysis.

Bottom-up Scenario Identification

Generic Risk Scenarios

Refined and Specific IT Risk Scenarios

Risk Factors

- External Environmental Factors
- Internal Environmental Factors
- Risk Management Capability
- IT Capability
- IT-related Business Capability

External Environmental Factors

Internal Environmental Factors

Risk Management Capability

IT Capability

IT-related Business Capability

- Business Objectives
- Generic Risk Scenarios
- Bottom-up Scenario Identification
- Top-down Scenario Identification

IT Risk

Risk Analysis

Estimate Frequency and Impact

Source: ISACA, The Risk IT Framework, USA, 2009
- IT risk management capabilities—To what extent the enterprise is mature in performing the risk management processes defined in Risk IT
- IT capabilities—How good the IT processes are, as defined in COBIT
- IT-related business capabilities (or value management)—Expressed through the Val IT processes

The importance of risk factors lies in the influence they have on IT risk. They are heavy influencers of the frequency and impact of IT scenarios and should be taken into account during every risk analysis, when frequency and impact are assessed. Figure 3 depicts risk factors.7

COMPONENTS OF RISK SCENARIOS
An IT risk scenario is a description of an IT-related event that can lead to a business impact, when and if it should occur. For risk scenarios to be complete and usable for risk analysis purposes, they should contain certain components, as shown in figure 4.

SCENARIO DEVELOPMENT
The use of scenarios is key to risk management, and the technique is applicable to any enterprise. Each enterprise needs to build a set of scenarios (containing the components described previously) as a starting point to conduct its risk analysis. Building a scenario means that each possible value of every component is combined. Each combination should then be assessed for relevance and realism and, if found to be relevant, entered into the risk register. In practice, this is, of course, not possible because it would result in far too large a number of scenarios. The number of scenarios to be developed and analysed should be kept to a much smaller number to remain manageable, since every possible combination cannot be retained.8

CONCLUSION
Scenarios have three benefits that make them very powerful for understanding risks and opportunities.9 First, scenarios expand one’s thinking. People will think more broadly if they develop a range of possible outcomes. By demonstrating how—and why—things could quickly become better or worse, they increase their readiness for the range of possibilities the future may hold.

---

<table>
<thead>
<tr>
<th>External Environmental Factors</th>
<th>Internal Environmental Factors</th>
<th>Risk Management Capability</th>
<th>IT Capability</th>
<th>IT-related Business Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market/economic factors</td>
<td>Strategic importance of IT</td>
<td>(Risk IT)</td>
<td>(COBIT)</td>
<td>(Vol IT)</td>
</tr>
<tr>
<td>Rate of change</td>
<td>Complexity of IT</td>
<td>Risk Governance</td>
<td>Plan and Organise</td>
<td>Value Governance</td>
</tr>
<tr>
<td>Industry/competition</td>
<td>Complexity of the entity</td>
<td>Risk Evaluation</td>
<td>Acquire and Implement</td>
<td>Portfolio Management</td>
</tr>
<tr>
<td>Geopolitical situation</td>
<td>Degree of change</td>
<td>Risk Response</td>
<td>Deliver and Support</td>
<td>Investment Management</td>
</tr>
<tr>
<td>Regulatory environment</td>
<td>Change management capability</td>
<td></td>
<td>Monitor and Evaluate</td>
<td></td>
</tr>
<tr>
<td>Technology status and evolution</td>
<td>Risk management philosophy and values</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strategic priorities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3**—Risk Factors in Detail


---

Enjoying this article?
- Read the ISACA publication *Global Status Report on the Status of Governance of Enterprise IT (GEIT)—2011*
  [www.isaca.org/research](http://www.isaca.org/research)
- Join this author at the 2011 Asia-Pacific CACS conference in Dubai, UAE, where he will deliver a workshop on IT risk management and using ISACA’s Risk IT framework, and at the 2011 EuroCACS Conference in Manchester, England, UK
  [www.isaca.org/asiacacs](http://www.isaca.org/asiacacs) [www.isaca.org/eurocacs2011](http://www.isaca.org/eurocacs2011)
- Access the Risk Management topic in ISACA’s Knowledge Center
  [www.isaca.org/knowledgecenter](http://www.isaca.org/knowledgecenter)
Second, scenarios uncover inevitable or near-inevitable futures. In developing scenarios, people will search for predetermined outcomes—particularly unexpected outcomes, which are often the most powerful source of new insight uncovered in the scenario-development process.

And, finally, scenarios protect against ‘groupthink’. Often, the hierarchy of an organisation inhibits the free flow of debate. Employees will wait (especially in meetings) for the most senior executive to state an opinion before venturing their own, which then often magically mirrors that of the senior person. Scenarios allow the organisation to break out of this trap by providing a political ‘safe haven’ for contrarian thinking.

Scenarios will not provide all the answers, but they help executives ask better questions and prepare for the unexpected. That makes them a very valuable tool indeed.

ENDNOTES

1 ISACA, *The Risk IT Framework*, USA, 2009
3 Risk analysis is the actual estimation of frequency and magnitude/impact of a risk scenario. Risk assessment is a slightly broader term and includes the preliminary and ancillary activities around risk analysis, i.e., identification of detailed risk scenarios and definition of responses.
4 *The Risk IT Practitioner Guide* provides a list of generic IT risk scenarios. This list can be used as a basis to build the enterprise’s own set of relevant risk scenarios.
5 Critical entities deserve to have risk scenarios defined at a detailed level; non-critical entities can do with quite generic scenarios that are not elaborated in too much detail. Note that the entity can be an organisational unit, but can also be something cross-organisational, e.g., a grouping of similar business processes and activities.
6 ‘Manageable’ does not signify a fixed number, but should be in line with the overall importance (size) and criticality of the unit. There is no general rule, but if scenarios are reasonably and realistically scoped, the enterprise should expect to develop at least a few dozen scenarios.
7 Risk factors are discussed in detail in *The Risk IT Practitioner Guide*.
8 Some guidance and considerations for the development and maintenance of manageable numbers of relevant scenarios can be found in *The Risk IT Practitioner Guide*.
9 Based on Roxburgh, Charles; ‘The Use and Abuse of Scenarios’, *McKinsey Quarterly*, November 2009