

Toolkit: Interactive Sourcing Risk Register

FOUNDATIONAL Refreshed: 16 January 2015 | Published: 25 March 2010

Analyst(s): Frances Karamouzis, Frank Ridder

At its most basic level, risk is exposure to economic loss from uncertainty. The interactive sourcing risk register is a critical tool that essentially acts as a repository for the capture, communication (including reporting), and ongoing centralized monitoring of all the related sourcing risk.

Gartner foundational research is reviewed periodically for accuracy. This document was last reviewed on 16 January 2015.

About This Toolkit

This Toolkit is related to: Sourcing & Vendor Relationships

When to Use:

Overview

Gartner considers sourcing risk management to be an iterative business process that is a subset of the overall enterprisewide risk management plan. At its core, risk management is the responsibility of the enterprise. This overall risk management must be applied to sourcing, which includes the discipline of managing both internal and external resources. More specifically, Gartner's 10 multisourcing competencies include risk management as one of the 10 elements (see "Ten Competencies and Key Activities for Mastering Multisourcing"). In this Toolkit, we will present an interactive sourcing risk register.

At its most basic level, risk is exposure to economic loss from uncertainty. Moreover, enterprises continue to spend large amounts of resources to focus on risk management. In a 2009 Gartner study, over 250 enterprises reported spending more than 5,000 staff-hours and as much as 30,000 staff-hours per annum on assessing controls for the following:

- Assessing business partners (48% of enterprises)
- Assessing service providers (32% of enterprises)
- Assessing vendors (29% of enterprises)

Here, we present a pragmatic interactive tool to help this effort to be more efficient and effective. The sourcing risk register is a critical tool that acts as a repository for the capture, communication (including reporting), and ongoing centralized monitoring of all the relevant sourcing risks. It incorporates a number of areas, including the probability, criticality, quantitative impact and budget tracking for the management of the risk. The most valuable aspect of the sourcing risk register is that it establishes a common approach for thinking about and discussing risks in a methodical, standardized, comprehensive and formalized manner for the purposes of taking appropriate action.

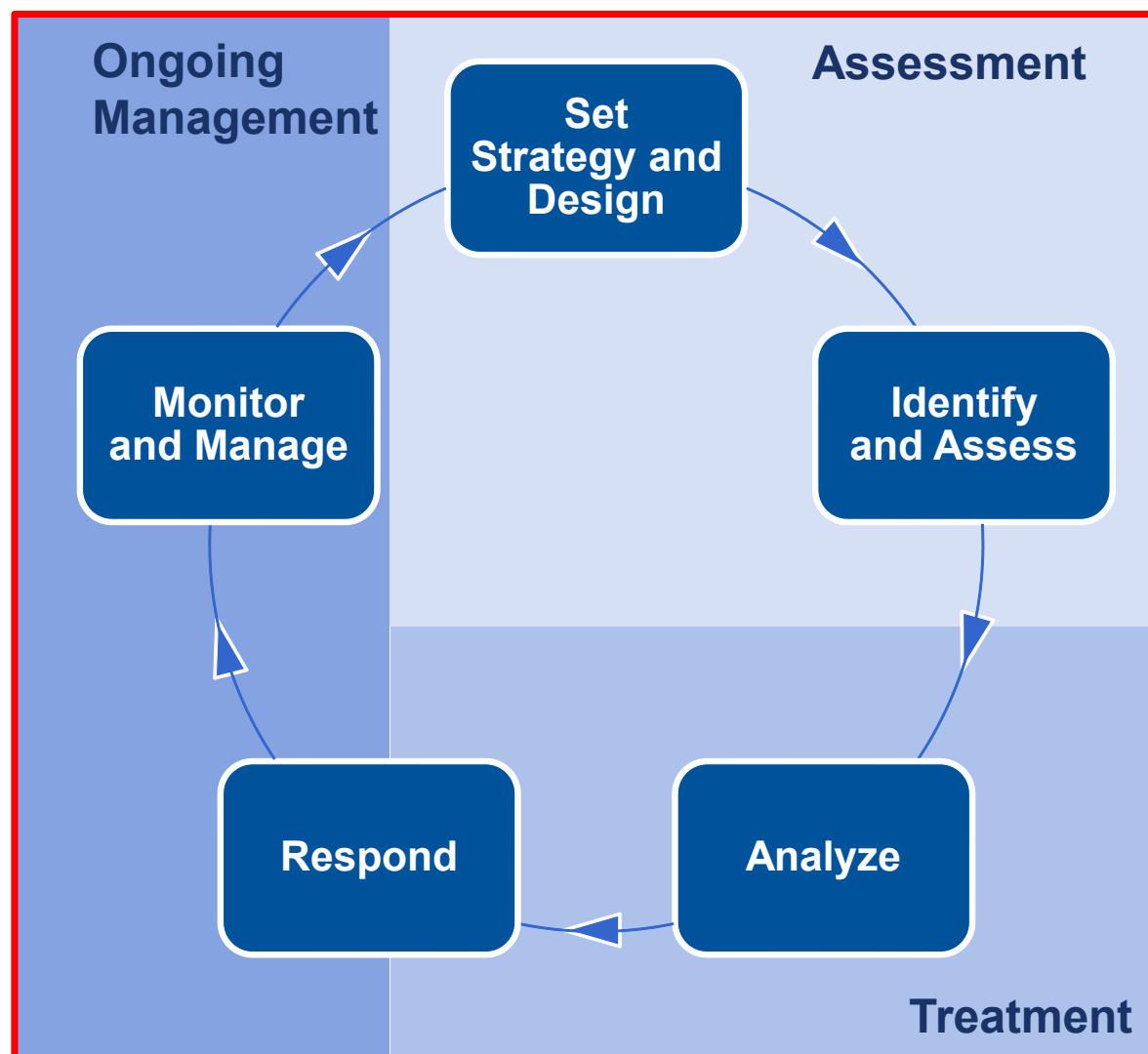
Approach

The overall approach for the use of this sourcing risk register is as follows:

- Convene the team. Gartner has extensive research on the roles, responsibilities and all the various personnel that should be involved in the overall enterprise and, more specifically, the sourcing risk management area. Based on those best practices, the overall team charged with the responsibility for the sourcing register should come together. As a team, members convene and begin the work on the sourcing risk register. At times, the team may also reach out to internal subject matter experts, external experts, and external stakeholders (such as suppliers, customers, business partners and regulators).
- Determine the overall tools and process. Using the agreed-on enterprise and specific sourcing risk approach, as well as the overall governance structure, the team should evaluate Gartner's tools as well as other resources. The team needs to go through all the variables described in this tool, agree on the risk categories, the relative scales used to classify the risk, the definition of levels (low to high), and most of all, the reporting measures and timing. The team should finalize the structure of its sourcing risk register, its role as a communication tool, and the overall risk management process and governance structure.
- Define the timeline to review, update and process reports from the risk register on a regular basis. Specific internal or external events may trigger an ad hoc risk review.
- Manage the budget and financial exposure to ensure that risk and security investments are aligned with business and sourcing strategies.

The sourcing risk management process consists of five phases (see Figure 1).

Figure 1. Sourcing Risk Management Framework



Source: Gartner (March 2010)

The use of this sourcing risk register plays a role in all five phases of the sourcing risk management process:

1. **Set strategy and design** — During this phase, the team designs the risk register and executes all the items listed in the Approach section. The deliverable at the end of this phase is the finalized sourcing risk register structure, the reporting and the timing of the process steps.
2. **Identify and assess** — During this phase, the sourcing risk register is used to capture the identified risks within the scope and granularity defined in the strategy deliverables that were set forth. The sourcing risk register is also used to process all the variables for each risk. This includes an assessment of the likelihood, impact and relevance of the risk.

3. **Analyze** — During this phase, the team must go through the most work-intensive portion of the process in which it must conduct an extensive analysis of the identified risks. The results of this analysis are reflected in the categorization, prioritization and impact analysis of the risks.
4. **Respond** — During this phase, the critical outcome that is captured in the sourcing risk register is the tracking of the action items for mitigating the risk (overall risk treatment, which involves the approach and remedies), the budget, the defined owner for the execution, and the status and due date of the risk treatment.
5. **Monitor and manage** — During this phase, the sourcing risk register is used to capture the updates related to threshold levels, budgets, status and timelines of the updated risk treatment action items. The risk register is the working document in which the overall responses and treatment plans are summarized and documented for the purposes of an audit trail, validation, ongoing reporting and central repository.

Format

A risk register can take a number of different forms — there is no set defined format. The format is determined by creating a tool that works for the organization to ensure the most effective communication, and it results in ongoing actions related to the management and mitigation of the identified risk.

Gartner has previously published an overall enterprisewide view of IT-related risk through a sample IT risk register (see "Toolkit: Sample IT Risk Register"). Here in this Toolkit, we take the risk register to the next level with a detailed approach to sourcing throughout the four phases of the sourcing life cycle, and with particular attention to the risk management associated with the 10 multisourcing competencies. This sourcing risk register is interactive and allows for the key reporting and management of the risk. It is designed to be part of an iterative process that we have documented in "The Importance and Construct of Sourcing Risk Management." Based on a defined milestone review cycle, the sourcing team should ensure that the sourcing risk register is updated with new, modified or archived risks.

The content of the sourcing risk register can vary. Here, we have summarized the variables that Gartner has included in its sourcing risk register. Based on extensive work with numerous clients with regard to the total cost of sourcing, and applying a risk-adjusted cost of sourcing, Gartner believes that the following variables constitute a solid foundation for the sourcing risk register:

- **Tracking number** — A number is automatically generated by the tool to allow for a unique reference ID to track the risk item.
- **Description** — This is a high-level description of the sourcing risk. This should be clear and concise and must serve to appropriately communicate the risk while not raising alarm. More importantly, the risk should be expressed in business terms rather than including extensive technical language. This reinforces the primary purpose of the risk register, which is to communicate risks so that the responsible and accountable roles can take appropriate actions.
- **Business unit** — The identification of specific business units allows for tracking, reporting, and most importantly, determining if there is a type of extensive exposure in one specific business

unit or groupings of business units. Due to the huge variety of business unit definitions and nomenclatures within the extensive Gartner client base, this field is free-form.

- **Category** — These Gartner risk categories are grouped based on the structure of the risk-adjusted total cost of sourcing models. Here, we summarize the high-level categories:
 - Information security and compliance (including intellectual property, privacy and security risks)
 - Country risks (including government-specific risk, economic risks, sociological and cultural areas and geopolitical risk)
 - Maturity risks (including service categories, the maturity of the software, integration layer, the platform, the infrastructure or management processes)
 - Competency risk (including competencies applicable to the specific area being sourced and the sourcing life cycle risks)
 - Operational risks (including risks like brand value risk, business process areas, policy and procedural risks)
- **Subcategory** — Beyond the main risk categories above, we have provided for two levels of subcategories. This allows the team to use the tool to create a more detailed structure of the risks for tracking, management, reporting and treatment approaches.
- **Raised** — This captures the date when the risk entry was identified.
- **Raised by** — This is personnel who identified and captured the risk line item.
- **Impact description** — This is a high-level description of the impact of the sourcing risk. Here again, this should be clear and concise and must serve to appropriately communicate the impact to the overall organization risk, while not raising alarm. More importantly, the risk should be expressed in business terms rather than including extensive technical language. This reinforces that the primary purpose of the risk register is to communicate risks so that the responsible and accountable roles can take appropriate actions.
- **Impact category** — The impacts can also be categorized. Some sample categories include:
 - Operational impacts are related to a key business or IT process that, if compromised, will have some type of harmful impact on the performance or execution of the process.
 - Brand value impacts relate to some harmful or damaging consequences that are associated with the perceptions, attitudes, mind share, and reputation of the enterprise or its positioning in the market.
 - Constituency impacts are related to other parties within the enterprise's direct or indirect sphere of influence. This may include suppliers, business partners, customers and the local physical community where the enterprise resides. In some ways, this may be an extension of brand value impacts or captured as a separate category.

- Regulatory impacts are usually directly related to compliance requirements regarding specific legislation. Thus, they are often distinctly discernable and typically separately tracked.
- Corporate cultural impact is usually associated with risks that relate to attitudes, motivations, morale and overall climate of the internal organization. The collective impact of these areas has often proved to directly impact employee productivity, and willingness to exercise diligence.
- **Financial impact (in U.S. dollars)** — This is a high-level estimation of the financial impact should the event identified as a risk occur. In some cases, the financial impact is extremely difficult to determine. As such, the impact category can be used to parse out and report on risks that might fall into categories that are much more difficult to estimate, such as corporate culture.
- **Impact level** — This field is designed to assign a structure to the intensity of the impact to the organization or, more specifically, to the asset, system or process. The scale is Level 1 (low) to Level 10 (high). Here again, this field can be used to parse out and report on risks that might fall into specific categories.
- **Probability** — This field is designed to capture the probability of a risk's occurrence. The scale is Level 1 (low) to Level 10 (high). This considers the likelihood or probability of its occurrence. The level may be determined by using external research, databases and other indexes to inform about the probability of a risk.
- **Priority** — This field is designed to capture the priority of a risk. The scale is Level 1 (low) to Level 4 (high). This prioritization can be associated with business priorities, timeliness variables and levels of effort reflected in the budgeting fields.
- **Risk criticality** — This field is automatically calculated (and the color codes shift accordingly in the actual cell in the spreadsheet tool) as a factor of the impact and probability fields. Based on these two fields, the risks are grouped into the four risk levels shown in Figure 2.

Figure 2. Four Levels of Risk Criticality

Risk Criticality Level	Value
Red	76 - 100
Orange	51 - 75
Yellow	26 - 50
Green	1 - 25

Source: Gartner (March 2010)

- **Mitigating actions** — This field is designed to capture a short, terse description of the action plan to mitigate the risk. The risk register is not designed to be the storage vehicle for detailed action plans. Most enterprises will likely have much more extensive supplementary documents that have a detailed treatment plan for the risks. This may also include policies and procedures, especially for regulatory and/or compliance risks.

- **Budget** — The extensive supplementary documents described above in the mitigating actions field normally also include budgetary allocations for people, process, assets and technology to execute the detailed treatment plan designed for either the ongoing management or mitigation of the risk. The totals of this budget should be captured in the risk register.
- **Owner** — This field is designed to capture accountability for the ongoing execution of the risk mitigation action plan.
- **Status** — This field is designed to capture the overall status of this risk entry. There are four stages, including work in progress (WIP), open, close or on hold. Here again, the spreadsheet tool color codes are automated to reflect the status selected. Please note that, if the status is marked as "close," then the whole row will be marked in gray to readily identify that it's closed.
- **Due** — This date is focused on the timing for the mitigation activity or next milestone for monitoring the treatment of the risk.

Toolkit Details

The ZIP file download contains the following documents:

  **174175_sourcing_risk_register.xlsm**

This attachment in Microsoft Excel 2007 contains an interactive sourcing risk register. Organizations can use it as a repository for the capture, communication (including reporting), and ongoing centralized monitoring of all the related sourcing risk.

  **174175_sourcing_risk_register.xls**

This attachment is similar to the one above and is intended for organizations using Microsoft Excel 2003.

  **toolkit_interactive_sourcing_174175.pdf**

This is the PDF version of this file.

Directions for Use

Download the Toolkit ZIP file by selecting the link under the "Download Toolkit Resource" header at the top-right of this page. A PDF copy of this content is included as part of the ZIP.

Recommended Reading

"What Is a Risk Register, and Why Do You Need One?"

"Toolkit: Sample IT Risk Register"

"The Importance and Construct of Sourcing Risk Management"

"Q&A on the Value of Quantifying Risk vs. Qualifying Risk When Communicating With the Business"

"Gartner for IT Leaders Overview: The IT Risk Manager and Chief Risk Officer"

"An Overview of IT and Enterprise Risk Management"

"A Risk Hierarchy for Enterprise and IT Risk Managers"

"Assess and Manage Vendor Risks to Protect Your Business"

Disclaimer

Unless otherwise marked for external use, the items in this Gartner Toolkit are for internal noncommercial use by the licensed Gartner client. The materials contained in this Toolkit may not be repackaged or resold. Gartner makes no representations or warranties as to the suitability of this Toolkit for any particular purpose, and disclaims all liabilities for any damages, whether direct, consequential, incidental or special, arising out of the use of or inability to use this material or the information provided herein.

GARTNER HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters

AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit <http://www.gartner.com/technology/about.jsp>

© 2010 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."