CONTEMPORARY PRACTICES IN RISK MANAGEMENT
IMPLEMENTATION IDEAS FROM LEADING COMPANIES
JANUARY 2012
DISCLAIMER

Copyright © 2012 by The Institute of Internal Auditors (IIA) located at 247 Maitland Ave., Altamonte Springs, FL, 32701, U.S.A. All rights reserved. Published in the United States of America. Except for the purposes intended by this publication, readers of this document may not reproduce, redistribute, display, rent, lend, resell, commercially exploit, or adapt the statistical and other data contained herein without the permission of The IIA.

ABOUT THIS DOCUMENT

The information included in this special report is general in nature and is not intended to address any particular individual, internal audit activity, or organization. The objective of this document is to share information and other internal audit practices, trends, and issues. However, no individual, internal audit function, or organization should act on the information provided in this document without appropriate consultation or examination.

ABOUT THE AUTHOR

Kathryn Bingham currently serves as Six Sigma Master Expert™ and Learning Champion for the internal audit function at Raytheon Co. Bingham is responsible for change leadership, encompassing integration of Six Sigma and internal audit processes, employing change models to achieve multimillion dollar savings, and enabling innovation and successful business turnarounds. Her role also involves leader development, coaching, and instructional design and execution across multiple knowledge domains, including finance, risk management, Six Sigma, ethics, and diversity. She is currently pursuing a Ph.D. in leadership science.

Raytheon would like to thank The IIA’s Audit Executive Center™ for assisting in the coordination of the roundtable and each participant’s candid sharing of processes and tools. All figures are provided without attribution and edited to protect information of a proprietary nature.
TABLE OF CONTENTS

DISCLAIMER ............................................................................................................................................................................... 1
ABOUT THIS DOCUMENT .......................................................................................................................................................... 1
ABOUT THE AUTHOR................................................................................................................................................................. 1

CONTEMPORARY PRACTICES IN RISK MANAGEMENT ........................................................................................................ 3

RISK MANAGEMENT APPROACHES ........................................................................................................................................ 3
THE RISK UNIVERSE ................................................................................................................................................................. 5
COMMUNICATION APPROACHES ............................................................................................................................................ 7
APPROACHES TO RISK RANKING ........................................................................................................................................... 9
AUDIT COMMITTEE COMMUNICATION APPROACHES ........................................................................................................ 16
RISK ENVIRONMENT CHALLENGE ........................................................................................................................................ 16

TOOLS & TEMPLATES ............................................................................................................................................................. 17

TOOLS & TEMPLATES 1: RISK GOVERNANCE TABLE ......................................................................................................... 17
TOOLS & TEMPLATES 2: RASCI CHART ................................................................................................................................ 18
TOOLS & TEMPLATES 3: QUALITATIVE SURVEY EXAMPLE .................................................................................................. 19
TOOLS & TEMPLATES 4: RISK PROFILE ............................................................................................................................... 20
TOOLS & TEMPLATES 5: RISK DECISION AND ACTION FRAMEWORK .................................................................................. 21
TOOLS & TEMPLATES 6: SAMPLE CHART TO CAPTURE AUDIT PLAN PROGRESS .............................................................. 22
CONTEMPORARY PRACTICES IN RISK MANAGEMENT

In sports, you’re only as good as your last game. For innovators, you’re only as good as your next big thing. As internal auditors, you’re only as good as the risks you have foreseen and enabled the organization to address or avoid. A critical component of a successful partnership between internal audit and the rest of the organization involves possessing the right skills and tools to identify, analyze, and communicate risks; enabling management to appropriately address risks; and providing assurance to stakeholders in the areas of governance, risk management, and compliance. Whether the operating environment is robust or faltering, internal auditors bring visibility and transparency to key issues with the potential to impact business objectives.

Internal audit’s continuous risk monitoring (CRM) process at Raytheon forms the foundation for understanding business risks and developing the audit plan. As part of the organization’s commitment to continuous improvement, CRM leaders and participants evaluated the end-to-end risk assessment, audit plan development, and communication processes with the board to identify opportunities to increase effectiveness and efficiency. In the past, the department engaged in multiple one-on-one benchmarking sessions with external peers. Desiring to quickly gain insight from multiple companies and industries, Larry Harrington, Raytheon’s chief audit executive (CAE), and Kathryn Bingham, Raytheon Six Sigma Master Expert™, approached The Institute of Internal Auditors’ (IIA’s) Audit Executive Center to request a roundtable session with the idea that outcomes, tools, and leading practices could be shared with internal audit leaders and their staff.

The full-day, face-to-face session encompassed a group representing 10 large companies from a mix of industries: aerospace and defense, consumer retail, global manufacturers of large products, financial services, chemical engineering, and transportation. Although participants represented large organizations, the ideas presented can be applied to all internal audit departments regardless of size. In addition to preparing for the three areas of interest — risk assessment, audit plan development, and communication with the board — about half of the participants brought information related to their organization’s overarching enterprise risk management (ERM) processes.

RISK MANAGEMENT APPROACHES

Organizations represented in the roundtable displayed a diversity of structural approaches to internal auditing and risk management. The robustness of risk-related processes was independent of each organization’s structural alignment to geographic region, business unit, operational function, or risk framework (e.g., the Committee of Sponsoring Organizations (COSO) of the Treadway Commission’s Enterprise Risk Management — Integrated Framework).
In addition, less than half of the companies described having a designated chief risk officer (CRO). A common leading practice, however, involved assigning risk ownership and accountability to specific senior managers. Furthermore, formal and informal leader councils support discussions on enterprise risk across silos.

Each event participant described a process flow for risk identification through audit plan development. (Figure 1 offers a universal view distilled to the simplest elements.) Basic components of the process flow encompass risk identification and risk universe development; risk assessment; risk prioritization and plan development; management and board review; and the final audit plan. Variations included sources of inputs (refer to Figure 2) and risk framework models, top-down and bottom-up assessment processes, iterative engagement with management, and flexible versus static final audit plans.

**IMPLEMENTATION IDEA 2**

Compare current risk resource/reference inputs to the list in Figure 2. Identify two or more new inputs (i.e., partnering with an external auditor) to implement during the next quarter.

**TOOLS AND TEMPLATES**

Craft a responsible, accountable, supported, consulted, informed (RASCI) chart to document the individuals in the audit or risk organization responsible for meeting periodically with organizational leaders to discuss risk (refer to Tools & Templates 2).

---

**Figure 1: Basic Risk Identification through Audit Plan Process Flow**

**Figure 2: Examples of Risk Inputs and Collaborative Efforts**

<table>
<thead>
<tr>
<th>INTERNAL ACTIONS AND INPUTS</th>
<th>COLLABORATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Assessments of business roadmaps, monthly business reports, and links to risks.</td>
<td>✓ Co-sourcing arrangement with Ernst &amp; Young.</td>
</tr>
<tr>
<td>✓ Attendance at operations meetings, trial balance reviews, and other internal reviews.</td>
<td>✓ Leveraging external information, reading, and peer networks, including:</td>
</tr>
<tr>
<td>✓ Ongoing face-to-face meetings with business and functional leaders, at least quarterly.</td>
<td>▪ Corporate Executive Board ‘hot spots.’</td>
</tr>
<tr>
<td>✓ Input from field team members with knowledge of the company.</td>
<td>▪ KPMG, PricewaterhouseCoopers, The IIA, and other professional resources.</td>
</tr>
<tr>
<td>✓ Quarterly committee and council meetings (e.g., Program Leadership Council).</td>
<td>▪ Industry publications.</td>
</tr>
<tr>
<td>✓ Input from product and contract subject-matter resources.</td>
<td>▪ General business and financial publications.</td>
</tr>
<tr>
<td>✓ Risk speculation discussions among company leaders, audit alumni, and external benchmarking groups.</td>
<td>▪ Economic trends (e.g., domestic and global).</td>
</tr>
<tr>
<td>✓ Facilitation of enterprisewide risk surveys of business and functional directors.</td>
<td>▪ External benchmarking groups.</td>
</tr>
</tbody>
</table>
THE RISK UNIVERSE

All roundtable participants talked about the importance of developing a comprehensive risk universe. Three participants use frameworks sourced from Big Four firms and tailor each framework to the unique needs of the industry and organization. For example, one company uses a “placemat” format of the risk framework — aligned to the COSO ERM framework — and augmented by identifying accountable executives and risk owners by category (refer to Figure 3). Other leading practices roundtable participants described include:

- Linking identified risks to the organization’s strategy.
- Examining the skill sets needed to execute the organization’s strategy and internal audit’s competency for reviewing emerging risks.
- Incorporating assessments of reputational risk factors.
- Determining potential unknown risks.

A key factor involves risk ownership for identifying, assessing, and addressing risk. One company differentiates ownership of known versus unknown risks (refer to Figure 4).

IMPLEMENTATION IDEA 3

One participating company evaluates the following reputational risk factors: leadership, performance, products and services, innovation, citizenship and corporate social responsibility, governance, and the workplace. CAEs should schedule sessions to facilitate communication around each of these factors, which risks the internal audit function already considers, what controls exist related to these categories, and the best ways to assess risks and controls related to these categories.

TOOLS AND TEMPLATES

Use Figure 3 as a guide when creating visual aids for communicating risk and ownership.
**Figure 3: Risk and Control Framework Example**

The image shows a Risk and Control Framework chart from the Special Report: Contemporary Practices in Risk Management. The chart outlines various risk categories, sub-categories, and owners, along with corresponding risk areas such as strategy, operations, and infrastructure. The framework is designed to help organizations systematically identify, assess, and manage risks across different areas of the business.

Adapted from Deloitte’s – Risk Intelligence Map.
Additional inputs to robust risk awareness include case studies, surveys, and quarterly meetings. Performing a risk case study works best in an environment where the business product delivery process (i.e., the product, general mix of customers, and operational model) is relatively stable. The case study process involves selecting a risk category area and taking a deep dive to assess risks, processes, and control activities. As a consulting approach, the case study allows internal auditors to assess entire systems and document detailed conclusions for management action. Case studies also serve as references for ERM decisions and as a framework for prioritizing audit efforts. Figure 5 highlights output components of a case study report.

COMMUNICATION APPROACHES

Event participants universally agreed that performing a survey offered a means to capture consistent, more comparable inputs from company leaders or process owners. Surveys can be disseminated electronically or deployed in meetings using electronic response devices to aggregate the group’s anonymous input. Surveys also can be used as a guide during face-to-face interviews. Quantitative responses — especially those offering Likert scales (e.g., ratings from one to five paired with descriptors such as strongly disagree, disagree, neutral, agree, and strongly agree) — enable rapid comparative analysis. However, qualitative methods, such face-to-face interviews and focus group discussions, provide greater depth of information when designed and used effectively.

Three companies highlighted the use of quarterly risk discussion meetings to provide a continuous pulse of the business environment and monitor changes. Each company took a different approach to
planning and executing the sessions. For example, one unique option consisted of strategically focusing quarterly discussions on specific topics, including ERM, corporate strategy, risk management, and business continuity on an annual rotation basis (refer to Figure 5). A second company developed a robust two-day agenda for quarterly meetings (refer to Figure 6); the framework supports decisions related to maintaining the organization’s rolling audit plan.

Figure 5: Focused Risk Dialogues

![Focused Risk Dialogues](image)

Figure 6: Two-day Quarterly Risk Dialogue Agenda

<table>
<thead>
<tr>
<th>Day 1: Breakout Sessions</th>
<th>Day 2: Team Discussions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUDITABLE ENTITIES</strong></td>
<td><strong>TEAM DISCUSSIONS</strong></td>
</tr>
<tr>
<td>Review auditable entities that did not make the original plan (e.g., have risk changes to these areas taken place?).</td>
<td><strong>INVESTIGATIONS</strong></td>
</tr>
<tr>
<td></td>
<td>Are we seeing trends? Does the investigation lead us to related concerns?</td>
</tr>
<tr>
<td><strong>REVIEW 10K RISK FACTORS</strong></td>
<td><strong>“FAT-TAILS”</strong></td>
</tr>
<tr>
<td>Review risks outlined in the current 10K and assess risk. Also verify information from annual operating plan documents.</td>
<td>Are there any catastrophic events that we have not already considered? If so, what can be done and, what would be the effect?</td>
</tr>
<tr>
<td><strong>ERM INPUT</strong></td>
<td><strong>TEAM OUT-BRIEFS</strong></td>
</tr>
<tr>
<td>Review data from year-end ERM report and incorporate information into the risk assessment.</td>
<td></td>
</tr>
<tr>
<td><strong>EMERGING ISSUES</strong></td>
<td><strong>GROUP DISCUSSIONS</strong></td>
</tr>
<tr>
<td>Document emerging issues applicable to each risk area. For any areas identified, document the corresponding business risks and what we might audit.</td>
<td><strong>ADDELETE AUDITS</strong></td>
</tr>
<tr>
<td></td>
<td>Should we add or delete audits from the plan? If so, when and where?</td>
</tr>
<tr>
<td><strong>IN-PROCESS OR COMPLETED AUDITS</strong></td>
<td><strong>SCHEDULE IMPACTS</strong></td>
</tr>
<tr>
<td>Discuss issues emerging from in-process or recently completed audits. This information should be shared with the larger group as it may cut across another risk area.</td>
<td>What is the impact to the schedule, and what resourcing issues does the change create?</td>
</tr>
<tr>
<td><strong>SYSTEM IMPLEMENTATIONS</strong></td>
<td><strong>COMMUNICATIONS WITH STAKEHOLDERS</strong></td>
</tr>
<tr>
<td>Review system implementation lists that may impact your risk area and discuss impacts to the plan.</td>
<td>How should we communicate with stakeholders? What audit results should be conveyed to them?</td>
</tr>
<tr>
<td></td>
<td><strong>SUMMARIZE RESULTS AND UPDATE AUDIT PLAN</strong></td>
</tr>
</tbody>
</table>
APPROACHES TO RISK RANKING

Companies use a variety of tools and processes to support the assessment and prioritization of identified risks. A common theme involved the use of heat maps. The case study example in Figure 7 presents a version with likelihood ranked from rare > unlikely > possible > likely > almost certain, and impact ranked across the continuum of insignificant > minor > moderate > major > critical (refer to the bottom right corner in Figure 5).

The majority of heat map examples used a high, medium, and low rating system for both factors. Participants at the roundtable acknowledged the subjectivity involved in assigning the risk ratings; stronger processes incorporated a risk rating matrix to limit the level of subjectivity and drive consistency into the effort (refer to Figure 8). Leading practice augments the ratings with additional factors, such as risk velocity and preparedness. Figure 9 captures a rating matrix for preparedness, while Figure 10 demonstrates a “spider chart” reflecting gaps related to the preparedness factor across multiple risk categories.

IMPLEMENTATION IDEA 5

One company contrasts a more traditional bottoms-up risk assessment and audit plan development with a top-down, shareholder value-based approach. CAEs should compare the elements of the two models in Figure 11 with the organization’s existing process and consider how to integrate potential enhancements.

TOOLS AND TEMPLATES

Completing a risk profile (refer to Tools & Templates 4) for each risk provides a comprehensive overview of risk, contributors, and mitigation strategies, as well as associated status, risk rating scores, and comparative mitigation impact.
Figure 7: Results of ERM Case Study on IT Security

The following IT security process areas are considered most effective in reducing risk:

- IT security policies and standards are documented and available to all employees to ensure consistency of approach and to educate users on their role in keeping systems secure.

- IT security training is required for all employees. Training compliance is tracked and required before network and internet system access is granted.

- Automated secure password policies and controls are employed to deter both internal and external sources from gaining unauthorized access.

- IT security threats are proactively researched and communicated. Dedicated company resources investigate these threats.

- Confidential and restricted data are protected at rest and in transit by strong encryption or masking to prevent accidental or intentional misuse.

- Network components such as firewalls, intrusion detection and protection systems, and virus software are used to prevent and detect unauthorized access to and attacks on the network.

- Physical access to data centers is maintained on an ongoing basis, 24 hours a day, seven days a week. Compliance audits occur regularly.

Improvement areas include:

- Perform additional network penetration and attack simulations, focusing on servers that are not included in currently performed quarterly scans.

- Periodically monitor third-party contracts to ensure IT security questionnaires and site visits are completed on a timely basis and scores are communicated.

- Retest any data facilities not scoring above 95 percent on their latest security scorecard.
Figure 8: Risk Rating Matrix

<table>
<thead>
<tr>
<th>Likelihood of Risk Occurrence</th>
<th>Mission Impact</th>
<th>Or Financial Impact</th>
<th>Or Operations and Resilience Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (8–10)</td>
<td>Significantly impacts our ability to achieve the company’s mission</td>
<td>Results in a single-year financial impact &gt; $500MM with ongoing impact</td>
<td>Significantly disrupts enterprise-wide customer service or operational reliability or impacts the brand in the long-term</td>
</tr>
<tr>
<td>Medium (4–7)</td>
<td>Moderately impacts our ability to achieve the company’s mission</td>
<td>Results in a single-year financial impact greater than $100MM and less than $500MM, with some ongoing impact</td>
<td>Moderate impact on enterprise-wide customer service or operational reliability or impacts the brand for a limited period of time</td>
</tr>
<tr>
<td>Low (1–3)</td>
<td>Limited impact on our ability to achieve the company’s mission</td>
<td>Results in a single-year financial impact &lt; $100MM, and little ongoing impact</td>
<td>Limited disruption of customer service or operations reliability with no impact on the brand</td>
</tr>
</tbody>
</table>

Figure 9: Preparedness Rating

<table>
<thead>
<tr>
<th>Preparedness Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/9/8/7/6/5/4/3/2/1</td>
</tr>
<tr>
<td>High/Medium/Low</td>
</tr>
</tbody>
</table>

8–10
- High: Company currently has a high degree of preparedness to prevent or respond to this risk.

4–7
- Medium: Company currently has a moderate degree of preparedness to prevent or respond to this risk.

1–3
- Low: Company currently has a limited degree of preparedness to prevent or respond to this risk.

The company uses a preparedness scale to describe the level at which it can reasonably anticipate and potentially mitigate the impact of a risk. Certain risks are more difficult to prepare for because of their inherent uncertainty about the time, place, and scope of a potential event. On this scale, a lower level of preparedness reflects a greater degree of uncertainty, while a higher level of preparedness reflects more certainty in this regard. However, the scale does not reflect existing or planned mitigation efforts nor does it suggest the company is more or less prepared than other organizations with similar risk profiles.
Figure 10: Overlay of Preparedness Rating and Impact Rating to Identify Gaps
Clear roles and responsibilities, along with common definitions for risk language, enable a consistent and comprehensive approach to addressing organizational risk. One roundtable participant described her company’s distribution of ERM roles and responsibilities among the board of directors, audit committee, the organization’s senior leadership and management team, and the internal audit department (refer to Figure 12).

In many organizations, lines may blur as groups share performance of risk activities. Consequently, clarity regarding who will be specifically accountable for identified tasks assures critical oversight. Likewise, as dialogue regarding risk moves across levels and between groups, using predefined terms for risk appetite and tolerance assures alignment and consistency when deciding whether risks should be accepted, transferred, mitigated, or controlled.
Figure 12: ERM Roles and Responsibilities

**Roles and Responsibilities for ERM**

**BOARD OF DIRECTORS**
- Define oversight responsibility across board committees.
- Receive periodic ERM updates from the audit committee.
- Consider risks when reviewing the company’s annual plan and strategy.

**LEADERSHIP AND MANAGEMENT**
- Set risk tolerance levels.
- Define organizational responsibilities for risk management.
- Determine significant risks to the business.
- Develop risk mitigation and management strategies based on the company’s risk tolerance levels.
- Monitor the business to ensure risk mitigation activities are in place and operating effectively.

**AUDIT COMMITTEE**
- Review ERM framework at the enterprise level.
- Understand management’s process for identifying, managing, and assessing risk.
- Consider the ERM process’ output quality.
- Receive updates on critical risk changes.

**CORPORATE AUDIT**
- Support management’s ERM process.
- Document risk assessments using a consistent approach.
- Coordinate ERM activities.
- Identify and validate controls are in place to mitigate risk.
- Report objectively on results of risk evaluations.

**IMPLEMENTATION IDEA 6**

Figure 13, adapted by one company from the Institute of Actuaries of Australia’s Risk Appetite, provides a foundation for framing risk discussions. CAEs could combine this model with risk matrices and other tools to create a shared risk language and assessment methodology.

**TOOLS AND TEMPLATES**

Use the Risk Decision and Action Framework (refer to Tools and Templates 5) to overlay risks on a heat map and support discussions on choosing appropriate responses to risks. Decisions to accept, transfer, mitigate, or control risks can be shaped by asking questions about:

- The organization’s knowledge and experience with specific risks.
- The ability to prevent risk occurrence or minimize risk impact.
- The robustness of disaster recovery plans and preparedness efforts.
- The level of reputational impact.
- Where the risk fits within the organization’s appetite and tolerance.
- Whether the company is maximizing opportunity in addition to considering risk.
Figure 13: Defining Risk Appetite and Tolerance

**Risk Capacity:** The broad-based amount of risk a company is able to accept in pursuit of its mission, vision, business objectives, and strategic goals. The risk capacity is directly related to an entity’s capital, liquidity, and external stakeholder influence.

**Risk Appetite:** The broad-based aggregate amount of risk a company is willing to accept in pursuit of its mission, vision, business objectives, and strategic goals. Risk appetite is directly related to an entity’s risk capacity as well as its culture, desired risk level, risk management capacity, and business strategy.

**Risk Tolerance:** The magnitude of risks that the organization is willing to take to achieve its business strategies and objectives. Risk tolerance is such that the aggregation of risk tolerances ensures that the organization operates within its established risk appetite.

**Risk Target:** The optimal level of risk that the organization desires to take to achieve specific business objectives and operate within its risk appetite and tolerance levels. The risk target is based on management’s desired returns, the role of risk to achieve returns, and the organization’s capacity to manage its risk/reward profile.

**Risk Limits:** Thresholds to ensure that variation from expected outcomes will be consistent with the risk target, but will not exceed the risk appetite and tolerance level. Defined process level controls and management authorities should reflect risk limits.
AUDIT COMMITTEE COMMUNICATION APPROACHES

Event participants shared a variety of examples pertaining to board communication. A current trend is to discontinue the use of lengthy, detailed reports and board packages. Companies keep briefing documents to no more than six PowerPoint slides or Word pages.

A selection of participants also reported that their organization moved to, or is transitioning to, a rolling audit plan. For example, one organization provides the board with an audit plan, but uses quarterly risk meetings to determine items to delete from or add to the plan due to risk environment changes. Each quarterly update looks ahead a full 12 months — not merely the remainder of a calendar year.

Another roundtable participant indicated his CAE provides the board with a plan in which the initial six months are firm, but the second half of the year is subject to change.

Figure 14: Board and Audit Committee Communication Topics

RISK ENVIRONMENT CHALLENGE

Internal audit and risk management functions operate in an environment of greater scrutiny. How organizations identify, assess, and prioritize risks — as well as how they apply frameworks and models and select audits — are all subject to the lens of hindsight when a crisis occurs or unanticipated risks are realized. Leaders will be judged by the critical eye of the “coulda, woulda, shoulda.” Adapting to this reality is not an option. As a result, risk management professionals and internal auditors must provide clear insight on business risks and the management decisions around how to appropriately address them.
## TOOLS & TEMPLATES

### TOOLS & TEMPLATES 1: RISK GOVERNANCE TABLE

<table>
<thead>
<tr>
<th>Sub-category</th>
<th>Risk Owner</th>
<th>Subject-matter Expert</th>
<th>Governance</th>
<th>Professional Organizations</th>
<th>Government Oversight</th>
<th>Organizational Benchmarking</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Area A</td>
<td>Name of accountable senior leader</td>
<td>Individual with comprehensive explicit and tacit knowledge</td>
<td>Individual, council, review panel, or other internal oversight</td>
<td>Boards, institutes, associations, or other</td>
<td>Specific government agency(ies) as applicable</td>
<td>Knowledge resources and other benchmarking engagements as applicable</td>
<td></td>
</tr>
<tr>
<td>Risk Area B</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
**TOOLS & TEMPLATES 2: RASCI CHART**

A RASCI chart typically documents processes and the array of individuals who have a specific role in each step or phase. The acronym defines the person or role aligned:

- **RESPONSIBLE**: The person (or role) who does the work.
- **ACCOUNTABLE**: The person (or role) who owns the process — usually a manager.
- **SUPPORTS**: Anyone who either backs up the responsible party or enables the process in some way.
- **CONSULT**: A person or group who must be consulted before decisions or actions take place.
- **INFORM**: A person or group who must be informed of outcomes or results.

The following example reflects responsibility for periodic risk dialogues with business and functional leaders, as shared by members of an audit department’s leadership team:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Risk Monitoring</td>
<td>Q</td>
<td></td>
<td></td>
<td>Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1   IT, Businesses</td>
<td>Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2   Corporate</td>
<td>Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3   Businesses</td>
<td>Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4   Business Unit 1</td>
<td>Q</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5   Business Unit 2</td>
<td>Q</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6   Business Unit 3</td>
<td>Q</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7   Business Unit 4</td>
<td>Q</td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8   Business Unit 5</td>
<td>Q</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9   Business Unit 6</td>
<td>Q</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional functions and actions covered:**
- Human resources, Supply chain, Engineering, etc.
- Financial statements, 10K & 10Q reviews, external sources of information and analyses
- Approximately 47 line items and intentional growth in annual coverage annually
**TOOLS & TEMPLATES 3: QUALITATIVE SURVEY EXAMPLE**

NOTE: The survey can be used as a guide during face-to-face interviews with multiple leaders or process owners or can be used in an electronic survey format.

<table>
<thead>
<tr>
<th>Question</th>
<th>Interviewee:</th>
<th>Title:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Did you have major changes in management, operations, programs, systems, and/or controls?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. What are the top three challenges/risks facing your division/area/department?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. What are the steps you are taking or planning to take to mitigate these risks?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Please describe any business process improvement initiatives currently in progress or planned in your division.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Are there particular areas of fraud that are causing the division concern beyond what is normal? What actions are you taking to mitigate this risk?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Were nonroutine, third-party audits conducted in your division?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Please identify three potential projects/areas you would like considered for the 2012 audit plan.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Would you like to discuss other important questions or issues?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## TOOLS & TEMPLATES 4: RISK PROFILE

The risk profile template provides a comprehensive overview of risk, contributors, mitigation strategies and associated statuses, risk rating scores, and comparative mitigation impacts.

<table>
<thead>
<tr>
<th>Risk Contributor</th>
<th>Mitigation Strategies</th>
<th>Planned (Failed)</th>
<th>Implemented</th>
<th>Audited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contributor:</td>
<td>Mitigation Activity:</td>
<td></td>
<td>X</td>
<td>0</td>
</tr>
<tr>
<td>Contributor:</td>
<td>Mitigation Activity:</td>
<td></td>
<td>X</td>
<td>.5</td>
</tr>
<tr>
<td></td>
<td>Mitigation Activity:</td>
<td></td>
<td>X</td>
<td>.5</td>
</tr>
<tr>
<td></td>
<td>Mitigation Activity:</td>
<td></td>
<td>X</td>
<td>.7</td>
</tr>
<tr>
<td>Contributor:</td>
<td>Mitigation Activity:</td>
<td></td>
<td>X</td>
<td>.5</td>
</tr>
</tbody>
</table>

**Risk Score**
- Likelihood: 9
- Impact: 8
- Preparedness: 6
- Total Risk Score: 23

**Mitigation Impact**
- Risk Score: 23
- Likelihood: 9
- Impact: 8
- Preparedness: 6
- Total Mitigation Impact: 23

**Residual Risk**
- Result: 7.5
- Tolerance Target: 7
- Mitigation Deficiency: 5
- Total Residual Risk: 7.5

**Tolerance Target**
- Result: 8
- Tolerance Target: 8
- Mitigation Deficiency: 5
- Total Tolerance Target: 8

**Mitigation Deficiency**
- Result: 5
- Tolerance Target: 5
- Total Mitigation Deficiency: 5
TOOLS & TEMPLATES 5: RISK DECISION AND ACTION FRAMEWORK

- Impact
  - Transfer
  - Accept

- Probability
  - Mitigate
  - Control
TOOLS & TEMPLATES 6: SAMPLE CHART TO CAPTURE AUDIT PLAN PROGRESS

NOTE: This illustration depicts a first quarter chart and, as such, many audits are not yet initiated. Values should shift to the right as more audits are completed throughout the year.