Association for Federal Enterprise Risk Management

Image by AzamKamolov from Pixabay

Federal ERM Areas of Practice Guidance – 2023

Community Review Draft – September 2023

AFERM
Association for Federal
Enterprise Risk Management

Contents

Preamble

Association for Federal Enterprise Risk Management (AFERM) Federal ERM Areas of Practice Guidance 2023:

- Risk Culture
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Key Risk Indicators

This document is intended to provide guidance and is not meant to be an enforceable standard against which an agency ERM program is assessed. The key principles and sub-principles provided herein are intended to support and not conflict with requirements established by authoritative government entities such as the Office of Management and Budget, and guidance / recommendations provided through the Federal ERM Playbook. By design, these sources of government ERM program guidance provide agencies with significant flexibility and latitude to structure ERM programs to meet the unique mission, culture and needs of the organization. This document amplifies those government sources with key attributes associated with various Federal ERM areas of practice.

This guidance applies directly to ERM practitioners within U.S. Government Federal Agencies but may have broader application to agencies / organizations at other layers of government. The guidance is designed to provide practical information in the form of key attributes to assist ERM program leaders to develop or strengthen key aspects of their agency's ERM program.

The value of this guidance will vary between Federal agencies and organizations based on several factors. These considerations include but are not limited to the type of organization (i.e., Department, major sub-component, independent agency etc.); governance structure (e.g., single leader or a Board of Governors or Commissioners); organization size; level of ERM program maturity; placement of the ERM function within the organization; internal governance model; and the agency mission and strategy.

Background

The AFERM Vision is to *Be recognized as a credible authority and leader in promoting the effective application of enterprise risk management in the public sector*. Two of the Association's supporting Strategic Goals for 2020 – 2025 are to 1) Advance the Federal Government ERM Profession, and 2) Influence Federal Government ERM Practices. In support of these goals, the AFERM Board of Directors established a working group in October 2020 to evaluate and recommend whether the Association should develop an ERM Standard. Based on the working group recommendation, the Board approved moving forward on this initiative during the January 2021 monthly Board meeting.

To shape the development efforts of the working group, the Board approved 7 general design objectives. This document should:

1. Provide guidance on how to design and sustain an ERM program,
2. Be based on leading practices and publicly available documents,
3. Be applicable to a wide range of agencies varying in size, complexity, mission, and risk culture,
4. Define what is technically required and provide one or more methods where appropriate,
5. Be subject to Peer Review process,
6. Address the need to regularly update the portfolio of risks to respond to change in context, and
7. Be a living document updated as the state of ERM knowledge improves.

The underpinning for this effort is a common understanding that ERM programs are designed and operate according to the following principles:

- create and protect value,
- are based on the best information,
- are an integral part of organizational processes,
- are tailored,

- are part of decision-making,
- take human, cultural, and political factors into account,
- explicitly address uncertainty,
- are transparent and inclusive,
- are systematic, structured, and timely,
- are dynamic, iterative, and responsive to change, the velocity of change, and flow of information,
- facilitate continual improvement of the organization.

Development Approach

The Board recognized that developing guidance across the Federal ERM areas of practice identified by the working group is a multi-year effort and set an initial goal to publish guidance on five additional (nine total) areas of practice by the end of 2023. To achieve this goal, the working group selected areas of practice that are somewhat different between public sector and private sector organizations and for which there is limited publicly available information to guide ERM practitioners in the Federal sector. The areas of practice addressed in this 2023 release are: Risk Culture, Risk Identification, Risk Analysis, Risk Evaluation, Key Risk Indicators.

Each area of practice section went through four phases of development prior to publishing the draft document for general community review and comment, and a fifth phase prior to approval by the AFERM Board.

> *Phase 1 – Initial Draft:* Key principles and subprinciples developed by a single working group member.
>
> *Phase 2 – Collaborative Draft:* All working group members collaborate to create full initial draft.
>
> *Phase 3 – Peer Review:* Each draft submitted to peer review for review and feedback.
>
> *Phase 4 – Adjudicated Draft:* Working group collaboratively adjudicates peer review comments.
>
> *Phase 5 – Final Adjudicated Document:* Working group collaboratively adjudicates community feedback.

Each area of practice section uses a common organizing structure beginning with a description of the area of practice and identifying the important attributes associated with the area of practice. For each identified attribute there is a brief description of what that attribute means; an explanation regarding why the attribute is important to an agency; examples of how an agency might achieve the attribute; example of different types of evidence for the attribute; and additional information relative to small agencies, where applicable.

The members of the development working group include:

Doug Webster	Harold Barnshaw	Nicole Puri
Jason Bruno	Bill Skaradek	Mark Stofanak

Peer Review Process

The peer review process involved volunteers from across the Federal ERM community who are knowledgeable in the technical elements of a federal agency ERM program, are familiar with program design and operation, and are independent with no conflicts of interest that may influence the peer review process. The 12 peer reviewers were grouped into 3 teams comprising 2 federal employees and 2 non-federal individuals.

Peer review teams considered each section from the perspective on whether,

- the principles and subprinciples are relevant, sustainable, and scalable,

- the examples for how an agency might achieve the attribute and possible types of evidence are adequate to achieve the intent of the area of practice,
- the explanations and assumptions provided are reasonable, and
- the guidance is clearly stated to promote understanding.

Members of the Peer Review panel for this Areas of Practice grouping included:

Marianne Roth	Peggy Sherry	Chris Calfee
George Fallon	Tim Mobley	Rich Gallagher
Stephanie Irby	Bill Dykstra	Lewis Motion
Tom Brandt	Karen Weber	Nicole Puri

Practice Area 5: Risk Culture

5.1 Description The term 'culture' reflects the dominant attitudes, beliefs and behaviors of a group or organization. Of these three elements of culture, only behaviors are directly observable making it difficult to measure or assess the culture of any group or organization. One way to think about the relationship between attitude, behavior, and culture is depicted in A-B-C Culture Model in figure 5.1.

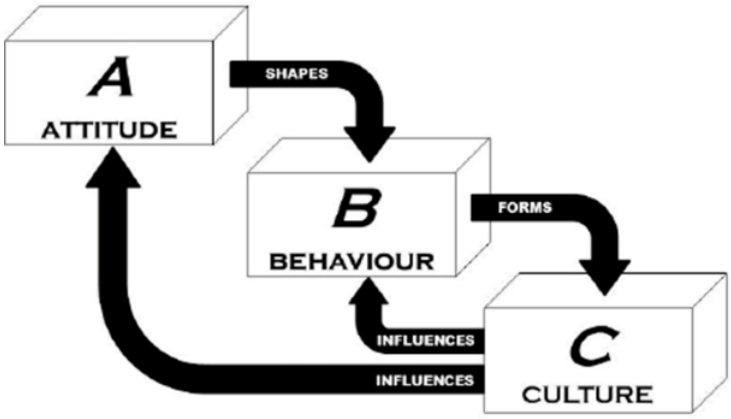

Figure 5.1 A-B-C Culture Model[1]

With respect to risk culture, these attitudes, beliefs, and behaviors shape the way in which employees think about risk and the decisions they make in response to risks. An effective risk culture is one where individuals at all levels across the organization are consistently taking an appropriate amount of risk to achieve agency objectives in a way that reflects the broader risk appetite established by agency leadership. Achieving a consistent and effective risk culture requires leaders to structure policies and processes to motivate employees to exhibit the desired risk-taking behaviors. Over time, these desired behaviors will influence attitudes and strengthen risk culture. Because the risk culture of an agency has a critical impact on the effectiveness of the agency's ERM program and supporting risk management activities, risk culture contributes directly to the organization's success or failure in achieving its goals.[2] Risk culture contributes to an agency's risk management efforts in several ways. Risk culture:

- informs agency strategy and strategic planning as leaders determine the strategic goals and objectives to pursue in an uncertain environment and changing operational context,
- affects agency risk appetite and impacts strategic, operational, and programmatic decisions regarding the type and amount of risk to take in a range of situations and settings,
- influences agency policies, procedures and practices that support the ability of employees to make effective risk-informed decisions regarding how to "take the right risks safely",
- shapes employee attitudes towards risk, affecting the way individuals and groups consider and react to risk,
- helps establish the boundaries of inappropriate behaviors beyond what laws, regulations, and policies provide. These boundaries can blur when leaders send inconsistent messages on the level of acceptable risk and risk management expectations.

Changing an organization's risk culture requires deliberate efforts focused on addressing the gaps between the current and desired risk culture states. In large organizations, different risk cultures often

[1] Hillson, D. (2013). The A-B-C of risk culture: how to be risk-mature. Paper presented at PMI® Global Congress 2013—North America, New Orleans, LA. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/understanding-risk-culture-management-5922

[2] Goals include strategic, operational, performance, compliance and reporting.

exist at different levels, different areas, and within different disciplines. Rick culture change management efforts need to account for these different risk cultures with specific actions initiated to bring these risk cultures into alignment.

The key principles and attributes which contribute to the design, implementation, and operating effectiveness of the Risk Culture area of practice include:

- clear guidance on risk-taking and risk management
- alignment of policies, procedures, and processes to support desired risk culture
- risk-taking, decision making, and communications consistent with desired risk culture
- risk-management skills and competency development
- periodic assessment of risk culture

5.2 Clear guidance on risk-taking and risk management

5.2.1 Description: Agency leadership sets clear expectations for how employees should approach risk-taking; make risk-informed decisions; and communicate risk-related information.

5.2.2 Explanation of Importance: Fostering the desired attitudes, beliefs, and behaviors associated with an effective risk culture requires employees to understand leadership's expectations with respect to risk management. Clearly stated and consistent risk taking, and risk management guidance are essential to creating enterprise-wide alignment of risk-taking and risk-management necessary to managing risk to an agency's mission, goals, and performance objectives within acceptable limits. An agency's risk appetite statement is an excellent vehicle to provide this type of specific and actionable risk-taking guidance. When leadership fails to provide clear expectations and guidance on how they want employees to think about risk, take appropriate risks, and to communicate risk information, the organization faces an environment which can foster disparate risk-cultures at different levels and within functional areas and lines of business. This environment can result in inconsistent risk-taking and risk management decisions that expose the agency unnecessarily to risk events, sub-optimize agency resources, and diminish enterprise-wide performance.

5.2.3 Examples of how it might be achieved:

- through the agency risk appetite statement
- within the agency risk policy statement
- development of risk management related core competencies
- documented and transparent risk management related decision rights and authorities
- including risk management related goals in employee performance appraisals
- through agency policies
- consistent and visible tone from the top on risk-taking expectations
- via agency developed training courses
- through resource allocation proposal guidance

5.2.4 Possible types of evidence and examples:

- risk appetite statement
- risk policy statement
- agency strategic plan
- risk management core competencies
- governing body charters
- annual performance appraisal guidance
- risk management elements in training curricula and related materials
- tracking of instances where risk-taking and risk management went outside of the entity's risk appetite

5.3 Alignment of policies, procedures, and processes to support desired risk culture

5.3.1 Description: Agency ensures that its policies, procedures, and business processes support and reinforce its desired risk culture.

5.3.2 Explanation of Importance: The policies, procedures, and processes of an agency are key aspects of governance in that they support consistency and establish the desired behaviors for employees. An agency's policies and procedures serve as entity-level controls that influence an organization's risk culture.[3] As the policies, procedures, and processes establish the "official rules" of the agency, a misalignment between them and the agency's desired risk culture can reinforce or incentivize behaviors and attitudes inconsistent with leadership's desires.

5.3.3 Examples of how it might be achieved:

- awards and recognition policy explicitly call out risk management
- after-action learning / lessons learned captured from impactful risk events and near misses
- through table-top exercises
- by properly resourcing the agency risk management function
- agency performance appraisal policy explicit incorporates risk management expectations
- risk management embedded in agency developed training courses
- risk management responsibilities and authorities for agency governance bodies clearly defined
- through resource allocation guidance
- incorporating risk management in new hire orientation

5.3.4 Possible types of evidence and examples:

- awards and recognition policy
- performance appraisal policy
- awards board guidance and individual award documentation
- table of organization and funding allocations for risk management function
- governance body charters
- table-top exercise objectives and after-action reports and documentation
- training course objectives
- agency resource allocation proposals and decisions

5.4 Risk-taking, decision making, and communications consistent with desired risk culture

5.4.1 Description: Employees at all levels of the organization exhibit behaviors consistent with the agency's desired risk culture and leadership expectations.

5.4.2 Explanation of Importance: The amount and type of risks employees take (or don't take), their active use of risk information to inform the decisions they make, and how they share risk information vertically and horizontally across the organization are the outward manifestations of an agency's risk culture. Unless desired risk behaviors are reinforced and undesirable behaviors confronted and held in check, the organization will likely find it challenging to achieve the risk culture needed to manage risk effectively in alignment with leadership guidance.

5.4.3 Examples of how it might be achieved:

- evaluate risk-informed decision making and communications during performance appraisals
- encourage desired risk-culture related behaviors through public recognition and awards
- incentivize desired risk behaviors
- challenge behaviors inconsistent with desired culture
- encourage risk reporting and whistleblowing

[3] GAO defines Entity-Level Controls as: "Entity-level controls are controls that have a pervasive effect on an entity's internal control system and may pertain to multiple components" GAO Green Book (2014). Standards for Internal Control in the Federal Government. P. 50.

- assess risk-informed decision making and communications during program reviews and audits

5.4.4 Possible types of evidence and examples:

- risk management core competency
- individual risk management related performance goals
- risk culture survey / assessment results
- awards documentation
- program audit and program review documentation

5.5 Risk-management skills and competency development

5.5.1 Description: The agency works proactively to develop its risk management capacity and capabilities by enhancing risk-management skills and risk management competency consistent with desired risk culture.

5.5.2 Explanation of Importance: A cornerstone of an effective risk culture is the knowledge, skills, and abilities of employees to manage risks consistent with leadership guidance and expectations, and the competence to effectively apply that knowledge, skill, and ability in their daily activities.

5.5.3 Examples of how it might be achieved:

- risk management courses available via learning management system
- in-person risk management related training courses
- promoting risk management related continuing professional education
- including risk management training as part of employee individual development plans
- provide access to commercially available risk-management training
- conduct a risk management training needs assessment and develop related training plan
- after-action learning from impactful risk events and near misses
- through tabletop exercises and scenario planning
- risk management embedded in agency developed training courses

5.5.4 Possible types of evidence and examples:

- training needs assessment
- training attendance / participation records
- employee performance plan templates
- employee performance appraisal policy

5.6 Periodic assessment of risk culture

5.6.1 Description: The agency initiates efforts to periodically assess risk culture to determine whether the current risk culture is likely to lead to acceptable performance outcomes.

5.6.2 Explanation of Importance: Some type of risk culture exists in every organization and may have developed organically. If an organization's environment lacks clear leadership guidance, has misaligned policies and processes, or fails to develop employee skills and competency and reinforced positive risk management behaviors, the current risk culture may not lead to acceptable risk-taking, risk management, and performance. Assessing the current state of risk culture, and periodically reassessing risk culture to monitor progress is, like any change management effort, foundational to success. Absent an assessment of the current risk culture, any efforts to change the risk culture of the organization are unlikely to succeed

in achieving the desired outcome. Figure 5.2 depicts a simple 5-step risk culture change model[4] that begins with a baseline assessment of the current state.

5.6.3 Examples of how it might be achieved:

- administering internal risk culture surveys
- facilitating focus group discussions on risk culture
- completing risk culture assessments
- including risk culture related questions in climate surveys
- conducting risk culture gap analysis and action plans
- define risk culture attributes for each level of ERM maturity

5.6.4 Possible types of evidence and examples:

- risk culture gap analysis and action plans
- risk culture assessment results
- risk culture survey results
- summaries of focus groups
- ERM program maturity assessment results

Step 1: Determine the current risk culture via assessment
(Where are we now?)

Step 2: Define the risk culture desired by the organization for acceptable performance outcomes
(What risk culture do we want?)

Step 3: Identify the gaps between the current and desired risk cultures
(What aspects of our current risk culture need to change?)

Step 4: identify actions needed to close the risk culture gaps and initiate a risk culture change program
(What actions are needed to make the necessary changes to our risk culture?)

Step 5: Reassess risk culture (repeat Step 2)
(Were our actions successful in achieve desired risk culture results?)

Figure 5.2 Five Step Risk Culture Change Process

[4] Hillson, D. (2013). The A-B-C of risk culture: how to be risk-mature. Paper presented at PMI® Global Congress 2013—North America, New Orleans, LA. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/understanding-risk-culture-management-5922

Practice Area 6: Risk Identification

6.1 Description Risk Identification is a structured and systematic process for recognizing potential threats and opportunities significant to achieving the organization's objectives[5]. Risk Identification is the first step of the risk assessment process and produces a comprehensive list of risks that serve as an input to the risk analysis process.

At the enterprise level, the purpose of Risk Identification is to identify the significant areas of uncertainty that would affect the ability of the agency to execute its mission or achieve its strategic goals and objectives. Risk Identification occurs at different points in the life cycle of an agency's ERM program. This life cycle typically begins with the organization's initial efforts to develop their enterprise risk register and continues with a periodic refresh of the agency's risk profile[6]. Enterprise risk identification should also occur during the strategic planning process, and in agencies with more mature ERM programs, as part of a continuous and iterative process. At other layers of the organization, risk identification also occurs on both a periodic and continuous basis. These risk identification efforts occur as part of an organization's internal controls program, during fraud risk assessments, and often at the beginning of programs and projects. Irrespective of where or why the risk identification process is initiated, the key principles and attributes are the same.

The ability of an organization to achieve its objectives reflects the organization's performance, and risk identification should focus on significant areas of uncertainty associated with achieving desired performance outcomes. Therefore, identified risk events should relate directly to the specific objective the organization seeks to achieve. The objective can be broad at the enterprise level (e.g., over-arching objectives in the organization's strategic plan) or within specific functional areas. An objective can also be quite narrow, such as the desired outcome of specific business processes or individual programs[7].

Generally, the complexity of the risks associated with a specific objective will differ depending on the breadth of the objective being considered. For example, risks associated with internal business processes tend to be distinct and limited, reflecting the narrow scope of the process objectives. Conversely, risks associated with strategic objectives are usually broad and more complex. The level of depth and detail required during the risk assessment process depends on the breadth of the objective and complexity of the identified risk. Absent a clear understanding of a specific objective for which risks are being identified, the outcome of the risk identification effort may vary in relevance and could diminish the overall effectiveness of the risk assessment.

The following principles and attributes contribute to the design, implementation, and operating effectiveness of this area of practice:

- Is structured, systematic, and iterative approach that is documented and repeatable
- Uses the agency risk taxonomy[8] to cast a wide net
- Is adaptable to the needs of an organization
- Uses the agency's specified format for risk statements
- Comprehensive, considers a full spectrum of internal and external risks
- Continuous and ongoing

[5] Playbook: Enterprise Risk Management for the U.S. Federal Government, July 29, 2016. Pg. 18.

[6] OMB Circular A-123 requires federal agencies to update their agency risk profile at least once per year, though some organizations update more frequently.

[7] Examples of different types of objectives associated with Risk Identification include, but are not limited to, strategic objectives, performance targets, business process outcomes, program and project outcomes, financial targets, efficiency goals, and effectiveness targets. Any goal or outcome an organization seeks to achieve can be considered an objective against which the Risk Identification process is applicable.

[8] A risk taxonomy is a thorough, stable, and standardized set of risk categories

6.2 Structured, systematic, and iterative approach that is documented and repeatable

6.2.1 Description: To ensure consistency and effectiveness across multiple iterations, Risk Identification should be a rigorous and repeatable process that matures over time.

6.2.2 Explanation of Importance: A structured and systematic approach ensures that efforts to identify risk across each part of the organization are consistent. A documented and repeatable approach also ensures that periodic refreshes and future iterations are done in a consistent manner. Organizations may have "blind spots" stemming from biases and assumptions that can inhibit the Risk Identification process. Documenting the Risk Identification process reduces the likelihood that such blind spots will prevent the identification of significant risk. It is important for the risk identification process to encourage stakeholders to share information about potential risks, and not discourage frank discourse. Because Risk Identification is an iterative process that occurs regularly, an ERM program benefits from repeatable processes and from thorough documentation that allows meeting notes and other artifacts to inform improvements.

6.2.3 Examples of how it might be achieved:

- Ensure that the Risk Identification process is inclusive of all parts of the organization.
- Use a structured, documented, and repeatable approach or script for stakeholder meetings, so that each stakeholder is asked the same basic questions. Figure 6.1 offers a simple example of a structured, repeatable, and documented approach.
- Encourage and elicit frankness and transparency about concerns and possible risks from agency leaders and key external stakeholders (e.g., "what keeps you up at night?" or "what are the biggest risks you manage?") and tailor questions to the organization's mission.
- Ensure participants understand the purpose of the process is to identify risks and not to judge or penalize individuals or groups.
- Thoroughly document all Risk Identification activities, with meeting notes and other artifacts kept in a location accessible to ERM program staff

Objective	Event(s)	Uncertainty	Impact
What is the objective you are trying to achieve?	What event(s) could affect achieving that objective?	How or where can the objective be affected by the event(s)?	How would the event(s) impact the objectives of the organization if it were to occur?

Figure 6.1 Risk Identification Table

6.2.4 Possible types of evidence and examples:

- Effectiveness of Risk Identification is not impacted by personnel change
- All parts of the organization are included in the Risk Identification process
- Identified risks reflect the breadth of the organization and are not disproportionately influenced by one or a few areas
- The Risk Identification effort identifies many potential risks
- Stakeholders actively disclose concerns and information on potential risks
- ERM maturity model or implementation plan (or similar document) includes activities or changes to mature the Risk Identification process
- Improvements to the process can be traced to lessons learned
- Impact and magnitude of realized risks are incorporated in subsequent identification cycles
- Traceable history through risk registers

6.3 Uses agency risk taxonomy to cast a wide net

6.3.1 Description: Using the agency's risk taxonomy encourages individuals involved in the risk identification process to consider all types of risks that could affect the ability of the organization to achieve its objectives.

6.3.2 Explanation of Importance: It is important for the Risk Identification process to "cast a wide net" to capture all types of potential risks significant to achieving the organization's objectives. The agency's risk taxonomy provides a common language and organizational structure that can bridge gaps between different parts of the agency that may describe the same risks using different terminology or jargon. It is important to use a common language to ensure that every stakeholder involved in the Risk Identification process has a common understanding of what is being asked of them and of what the risk identification effort is trying to accomplish. Standardization helps translate risk management to the enterprise level: top-down and down-up.

6.3.3 Examples of how it might be achieved:

- Implement a risk lexicon defining common terms.
- Implement a risk taxonomy of common risk categories and subcategories.
- Define the key terms you will use during the Risk Identification process and be able to define these terms for stakeholders during your risk discovery meetings.
- When a stakeholder uses jargon or terminology that is unfamiliar or ambiguous to you, pause and ask them to define how that term is used in their organization.

6.3.4 Possible types of evidence and examples:

- Meanings for terms used in risk discovery meetings are clearly understood by participants.
- Risk lexicon is used across the organization to develop common understanding of terms.
- Large number of potential major risks before aggregation indicates a wide range of risks from many parts of the organization.

6.4 Adaptable to the needs of the organization

6.4.1 Description: Risk Identification efforts may differ between agencies depending on the objectives of the process. Agencies should adapt the Risk Identification process to the specific needs of their organization.

6.4.2 Explanation of Importance: Risk Identification can be done as a top-down exercise based on conversations with the organization's leadership, as a bottom-up exercise based on conversations with risk owners within each of the organization's functional or programmatic elements, or as a hybrid approach that combines aspects of each. The correct approach for Risk Identification is the one that is most effective at identifying enterprise risks for its organization and is adapted to its governance structure and context. A key advantage of the bottom-up approach is that risk information is obtained from the managers and subject matter experts who are closest to the day-to-day management of risk. However, a comprehensive view of enterprise risk will not simply emerge from a bottom-up aggregation of risks identified within silos because enterprise risk threatens the achievement of the organization's objectives, and such strategies, goals, and objectives come from the top down.

In general, a bottom-up approach provides a wide range of risks but without strategic context. The top-down risk identification approach generates fewer risks events but results in a deeper understanding of the connection to the organization's mission and goals. In a mature ERM program, a combination of both approaches will be used to consider the full scope of enterprise risks from both the business and leadership perspectives.

6.4.3 Examples of how it might be achieved:

- A top-down approach may feature meetings and interviews with the organization's top leadership (such as the Office of the Secretary or equivalent) or the most senior heads of the organization's functional or programmatic elements.
- A bottom-up approach may feature meetings and interviews with managers and subject matter experts located further down the organization chart of each of the organization's functional or programmatic elements, especially those who are close to the day-to-day management of risk.
- A hybrid approach may, for example, consist of first interviewing the organization's top leadership to understand goals, objectives, and how senior leadership views risk, before following up with managers and subject matter experts to learn more detail, or may begin with the bottom-up approach before meeting with senior leadership to validate that the risks identified thus far are actually the major risks facing the organization.
- Use of surveys to reach a larger number of people. In a bottom-up approach, analyze the results, identify the most common risks, and review them with leadership. In a hybrid approach, analyze the survey results and use that data to inform interviews with senior leaders.

6.4.4 Possible types of evidence and examples:

- Identified risks are directly linked to specific organizational objectives.
- The number of risks identified is manageable and supportive of the purpose of the risk identification effort.
- Level of detail collected supports the purpose of the risk assessment
- Associated risk statements meet specified agency format

6.5 Uses the agency's specified format for risk statements

6.5.1 Description: A risk statement is a structured formulation of a risk. Your organization should have a standard format for risk statements. A rigorous risk identification process may uncover risks from different parts of the organization that are similar or closely related: these risks may be aggregated into risk statements that reflect an enterprise view of these risks and are tied to the possible impact of the risk to your organization's goals and objectives.

6.5.2 Explanation of Importance: Translating identified risks into formal risk statements builds a common, enterprise-wide understanding of both what the risk is and why it should matter to the organization. Just as using a risk lexicon helps to ensure that every stakeholder involved in the risk identification process has a common understanding of risk identification, using a common format for risk statements ensures that every stakeholder involved in subsequent stages of the risk assessment process has a shared understanding of each risk and how it may impact the organization. Ensuring that your risk statement format links each risk to a possible impact to the ability of the agency to execute its mission or achieve the strategic goals and objectives of the organization helps to ensure that you are tracking true enterprise risks. Using a specified format for risk statements also ensures that each risk is assessed in a similar manner in subsequent stages of the risk assessment process.

An important part of formulating risk statements is risk aggregation, or combining similar and related risks. It is likely that initial risk discovery efforts will identify the same risk, or similar related risks, in different parts of the organization: these risks may be worded differently in different parts of the organization due to differences in focus, terminology, or past experience. To aggregate risks, you may look to root causes: the same root cause can cause multiple impacts. You may also look at response: a key question for risk aggregation may be whether two risks are being responded to similarly or differently by the organization. Further, the consequences of one risk may be considered the root causes of another. Because these related risks can be conflated if the risk statements are not sufficiently distinct, it is important that risk statements are clear

6.5.3 Examples of how it might be achieved:

- One example of a commonly-used risk statement format is the "IF-THEN" risk statement which includes the event of primary concern and at least one primary impact of the event. An example of an "IF-THEN" risk statement is provided in Figure 6.2
- Another example of a commonly used risk statement format is the "root cause-event-consequence" format, which includes a root cause of the risk, an event that is the risk itself, and a consequence that occurs as a result of the risk. An example of a root cause-event-consequence risk statement is provided in Figure 6.3
- Whichever format is used, a risk statement should at the very least include both the risk itself and how the risk could affect the organization's strategic goals. For example, the "then" statement of the "IF-THEN" format and the "consequence" statement of the root cause-event-consequence risk statement should both refer to potential impacts relevant to the agency's ability to execute its mission.
- Use shared root cause or common risk treatment as two factors for when to aggregate risk

If the agency fails to ensure that its regulatory activities are informed by accurate data, **then** the agency will be unable to issue clear, effective, and timely regulations that protect consumers from unfair or deceptive practices.

Figure 6.2 Example of the IF-THEN format

Root Cause	**Event**	**Consequence**
Skills of agency employees are not aligned to our Data and Cyber Security needs	A Cybersecurity breach exposing confidential data	The agency suffers reputational harm from being unable to secure confidential data; key external partners and stakeholders less likely to work with the agency on shared goals.

Figure 6.3 Example of the root cause-event-consequence format

6.5.4 Possible types of evidence and examples:

- Risks are written in such a way that stakeholders from all parts of the organization can understand the risk, its causes, and its impact.
- Risk impact is clearly linked to the organization's strategic goals and objectives: any stakeholder can understand why a particular risk is relevant to the enterprise's mission.
- Risks sharing a common root cause are aggregated.
- Risks sharing a common treatment are aggregated.
- Risks represent a portfolio view of the entire organization.

6.6 Comprehensive and considers a full spectrum of internal and external risks

6.6.1 Description: Risk Identification should be a comprehensive process that, in addition to casting a wide net, probes areas that may be overlooked or emerging and encompasses both internal and external risks.

6.6.2 Explanation of Importance: As noted earlier, it is important for the risk identification process to "cast a wide net" and capture all potentially significant risks to the achievement of the enterprise's objectives. The process should consider a wide range of enterprise risks and the prioritization and curation of these risks is accomplished later in the risk assessment process. During risk identification, the ERM program should not prematurely engage in subsequent steps of risk assessment: this is not the time to "write off" a risk because it seems likely to be a low priority or appears under control. ERM practitioners should seek to understand the connection between their organization's risk and risks originating from external partners such as key service providers and suppliers. The emergence of a key external partner's risk can easily become one of your organization's risks. The ERM program should ensure that specific risk areas that may be potential "blind spots" for the organization are probed during the risk identification efforts.

6.6.3 Examples of how it might be achieved:

- Consider all the types of risk that could impede your performance, strategic goals, and objectives.
- Don't confuse risk identification with risk management and don't prematurely conduct subsequent phases of the risk assessment process.
- During risk identification, ask stakeholders about how the organization could be impacted by issues with external partners, such as service providers and suppliers.
- Before conducting risk identification, determine if there are risk areas that have historically been overlooked by the organization in previous iterations. This may include interdependencies between risks, strategic risk, emergent and evolving risk, or third-party risk. Make sure to affirmatively focus risk identification efforts on these overlooked areas.

6.6.4 Possible types of evidence and examples:

- Risks identified span all risk categories in the agency's risk taxonomy (i.e., financial, operational, strategic, compliance, reputational, etc.)
- Documented interactions with stakeholders during risk identification
- Identified risks include third party risks (e.g., risks associated with key service providers and suppliers)
- Known "blind spots" or historically overlooked areas have been affirmatively probed

6.7 Continuous, ongoing, and iterative

6.7.1 Description: A mature ERM program improves risk identification iteratively and identifies risk continuously

6.7.2 Explanation of Importance: The iterative nature of risk identification provides a natural opportunity for the ERM program to improve and mature the Risk Identification process over time, such as by using a defined maturity model. At the same time, a mature ERM program identifies risk continuously, not just during a planned refresh process. Strategies for continuous risk identification include: (1) leveraging the external environment and learning from adverse events or near-misses to your organization or similar organizations; (2) leveraging your organization's existing activities for risk identification, such as by establishing an ERM presence at key meetings or working groups where potential new, emergent, or evolving risks may be mentioned.

6.7.3 Examples of how it might be achieved:

- Create a path forward by defining attributes of increased risk identification process maturity in the agency's ERM program maturity model
- Define processes for leveraging the external environment[9] and your organization's own adverse events and near-misses for risk identification
- Demonstrate and explain the value of ERM to leadership to ensure participation at business meetings, which can be leveraged for continuous risk identification (among other purposes)
- Define processes for using your organization's existing meetings, communication channels, and processes as an opportunity for continuous risk identification
- Agency is aware of and monitors emerging or evolving risk

6.7.4 Possible types of evidence and examples:

- Maturity model or similar document includes plans for maturing next iteration of the risk identification process
- ERM program is aware of adverse events or near-misses
- Emergent risks are tracked and documented
- Agency considers the potential impact of risk events occurring in similar organizations
- ERM program is aware of changes in context that could result in emergent or evolving risk becoming increasingly relevant to the organization

[9] Leveraging the external environment means learning from events and developments outside of your organization: for example, adverse events suffered by similar agencies

Practice Area 7: Risk Analysis

7.1 Description: Risk Analysis is the second component of Risk Assessment, which is comprised of Risk Identification, Risk Analysis, and Risk Evaluation. Risk Analysis involves researching and probing available risk data to ascertain causal connections, impacts, root causes of risks, and current controls and response actions. Analyzing risk also involves understanding how the risk ties back to the agency's strategic plan and mission goals. If through the analysis the risk does not clearly impact the plan or goals, it may not be a risk, or may be a risk that can be managed at a level below the full enterprise. Likewise, analyzing risks can help clarify when several identified risks may be related by a common root cause or impact. Risk Analysis is the step where information is gathered and reviewed so that decisions may be made on individual risks in the next step. Risk Analysis and Risk Evaluation are closely related, however, and can be intertwined and iterative, as can Risk Analysis and Risk Identification. For example, when completing Risk Evaluation and scoring or prioritizing a list of risks, you may encounter a new root cause, not was not identified previously, which will impact response strategies. Thus, the entire risk list may need to go back through risk analysis to clarify interconnectedness before determining final priority and risk responses. This step is where information is gathered about the risk in order It is important to remember that a risk may change with time. The organization should establish safeguards (e.g., oversight by the senior risk council) to decrease the chance of failing to reanalyze and treat a risk before it becomes an issue.

Risk Analysis encompasses the following:

- **Root cause/causal chain analysis:** This step involves identifying the problem and using a tool or technique to determine the underlying causes of the risk through a causal chain. A causal chain is an ordered sequence of events in which any one event in the chain causes the next event. In conducting root cause/causal chain analysis, multiple techniques are available to aid in the process, such as the five whys analysis, failure mode and effects analysis (FMEA), fault tree analysis, fishbone diagrams, Pareto charts, scatter plot diagrams, and others. NOTE: It can take several iterations of root cause analysis to uncover the true root cause. Using a root cause tool can help prevent you from identifying an intermediate cause rather than a true root cause. In turn, this can help you implement more effective response strategies by targeting root causes rather than intermediate causes.
- **Consequence/impact chain analysis:** This analysis step involves identifying the consequences or impacts of a change. It is often used for scenario planning exercises, often in working groups. The benefit of this analysis is to help identify direct and indirect impacts of a decision or event, the treatment of which can allow an organization to either avoid or reduce the associated risk. Scenario planning also may be a useful approach to minimizing identified impacts or likelihoods.
- **Consider the impacts of current controls/response actions:** In analyzing the relative importance of enterprise risks, the organization should consider which actions are currently planned or in place already. These actions could be mitigating controls or other response actions, such as modifying or adjusting the strategic plan to address a strategic risk. Once a risk is formally identified understanding which response actions have already been taken or planned helps an organization make better response decisions during the risk evaluation step.

The key principles and attributes which contribute to the design, implementation, and operating effectiveness of the Risk Analysis area of practice include:

- Select and use a repeatable, reproducible methodology for all steps of risk analysis

- Conduct root cause or causal chain analysis on potential enterprise risks[10]
- Use of impact chain analysis to identify intended and unintended consequences (to which responses are developed in the risk evaluation step)
- Consider impacts and root causes that cross the organization
- Consider the impacts of current controls and response activities

7.2 Select and use a repeatable, reproducible methodology for all steps of risk analysis

7.2.1 Description: Agency agrees upon an approach and set of criteria for how to analyze enterprise level risks.

7.2.2 Explanation of Importance: To provide an analysis that can help prioritize risk in the evaluation step, risks must be analyzed using repeatable and reproducible methods. Using a repeatable and reproducible methodology provides datasets that can be compared and prioritized without the concern of bias due to the use of different approaches. Similarly, a common set of criteria across the agency helps to ascertain that impacts and likelihoods which will ultimately be used to rate the risks. This consistency allows for comparison between risks in the evaluation step. Since Risk Analysis involves analyzing risk in relation to the organization's objectives, both the methodology and criteria for risk analysis should consider which performance outcomes the organization is seeking and how the risk ties, either positively or negatively, to the outcome. This approach may change over time based on the maturity of the agency, changes in desired outcomes, or other factors; but it should be applied consistently within the list of risks being analyzed.

7.2.3 Examples of how it might be achieved:

- Approval of methodology by senior leadership/senior risk council
- Use of generally accepted root cause tools and techniques
- Use of generally accepted causal impact tools and techniques, such as scenario planning
- Training for employees on the risk analysis methodology

7.2.4 Possible types of evidence and examples:

- Written methodology or framework for risk analysis
- Analysis documented for each risk that allows comparison across risks, programs, risk categories, etc.

7.3 Root cause or causal chain analysis conducted on potential enterprise risks

7.3.1 Description: Agency conducts an analysis on each Potential enterprise risk to identify true root causes/causal chain.

7.3.2 Explanation of Importance: Assessment of risk is more art than science. Often risk identification will surface the impacts and most obvious symptoms contributing to or associated with the risk. It often takes significant analysis to uncover a root cause, which could have multiple levels of intermediate causes (i.e., causal chains). Root cause analysis is important in the evaluation step of risk assessment because it is the starting point for how to respond to risk. If an agency only treats an intermediate risk cause or risk symptom, it is unlikely the risk will be managed successfully because the root cause has not been treated and continues to cause the risk. To aid in the full identification of root causes, a thorough analysis should be completed. Many tools exist (see section 7.3.3) to help in this analysis and agencies can select the ones that suit them best.

[10] *Potential* enterprise risks are risks which are significant enough to be considered for an organization's Enterprise Risk Profile, as defined in the OMB Circular A-123: Management's Responsibility for Enterprise Risk Management and Internal Control. A full root cause analysis does not need to be conducted on every risk considered for inclusion on the Enterprise Risk Profile or similar documents. It can be a useful tool for the more limited list, particularly risks which will be actively responded to or have proven difficult to manage.

7.3.3 Examples of how it might be achieved:

- Pareto analysis
- Bow tie diagrams
- Fishbone/Ishikawa diagrams
- Five whys analysis
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis

7.3.4 Possible types of evidence and examples:

- Agreement of senior leadership and/or senior risk council that root causes are accurate
- Commitment to address root causes that span across multiple programs/business areas
- Diagrams documenting root causes/causal chains

7.4 Use of impact chain analysis to identify intended and unintended consequences

7.4.1 Description: Agency conducts an analysis on each proposed enterprise risk to identify impact chains.

7.4.2 Explanation of Importance: Taking time to conduct a thorough impact chain analysis will help quantify the impacts of decisions in the near term and can provide insights to assist with preventing or managing those impacts in the future. Given the nature of risks as uncertain events, impact chain analysis can help to prevent or better manage risks. Additionally, impact chain analysis can highlight common or connected impacts across the agency. In conjunction with results from other analysis tools, this data may be used to prioritize or treat risks later in the risk management process. Impact chain analysis combats one negative effect of an agency focusing too much on short-term planning and operational firefighting - it leaves little to no time to understand how decisions made today might impact the agency in the future. Even when lessons learned are collected or there is institutional knowledge of likely impacts, it can be difficult to plan improvements or implement changes to the process.

7.4.3 Examples of how it might be achieved:

- Scenario planning
- Strategic foresight planning
- Impact analysis workshops

7.4.4 Possible types of evidence and examples:

- Documented impact chains
- Completed logic model
- Completed theory of change model

7.5 Consideration of cross organizational impacts and root causes

7.5.1 Description: After identifying potential enterprise risks and identifying their root causes, the agency considers how the root causes and impacts of the risks may overlap across the organization to provide information for the risk prioritization and responses in the evaluation step.

7.5.2 Explanation of Importance: One of the main purposes of Enterprise Risk Management is to elevate and prioritize risks that are the most significant to the agency. Understanding how risks are interconnected through root causes and impacts allows agencies to prioritize risks for enterprise status if they impact a large part of the organization, they are isolated to a smaller area but have an outsized impact on the organization, or if the only way to effectively respond to the risk is to elevate it to the top of the agency. The cross-organization impact and root cause analysis provides the in-depth knowledge needed to understand if the risk falls into one of these three categories and should be escalated to enterprise status.

7.5.3 Examples of how it might be achieved:

- Conduct root cause or impact chain analysis across multiple business areas that have identified similar risks
- Consider potential risk response and evaluate if more than one risk can be successfully treated with the same response[11]

7.5.4 Possible types of evidence and examples:

- Broad leadership agreement on root causes or response strategies
- Documented root cause and impact chain analyses that show overlap between business areas

7.6 Consider the impacts of current controls and response activities

7.6.1 Description: The agency considers the impacts of current controls and response activities for proposed enterprise risks before determining the priority of any risks.

7.6.2 Explanation of Importance: When identifying risks for the enterprise risk profile it is important not to consider risk responses already in place, so that the risk does not get prematurely pushed down or off the list. However, agencies should consider what effective activities or controls are in place to address the risk in the analysis step so that they do not get rated more highly than necessary. This analysis should reflect time, resources, budget, and similar items already dedicated to the risk's response, as well as the maturity of the controls. For instance, if a control is newly in place and not fully tested, the agency may want to prioritize the risk more highly than if the control was already well tested and effective. It may be possible to begin mitigating some portion of the risk by modifying existing controls or responses.

7.6.3 Examples of how it might be achieved:

- Survey groups whose work touches on the risk to understand current actions in place
- Consult personnel responsible for internal controls and audit remediation to understand any connections to the risk
- Discuss potential risk scoring with multiple sources to get the full picture of current activity

7.6.4 Possible types of evidence and examples:

- Risk and control assessment/matrix
- List of current risk response activities for other agency risks
- Prior year risk registers or agency risk profiles
- Other agency reports documenting actions around risks, issues, audit findings, etc.

[11] Although it is appropriate to consider what types of risk responses may be applicable, response activities should not be determined or started at this stage. Risks still must be prioritized before an organization can make informed decisions about how, when, and where to respond to risks. Additionally, considering risks in isolation in this step is appropriate. In the evaluation step that follows, risks will be considered in context before a response is determined.

Practice Area 8: Risk Evaluation

8.1 Description Risk evaluation is the third and final component of Risk Assessment. Before considering potential actions to treat a risk, it should first be determined if the current level of risk is acceptable in relation to the organization's risk appetite. The risk evaluation process is concerned with understanding what the risk actually means to people concerned about or affected by the issue and how the risk relates to other risks on the organization's risk register. Risk evaluation enables a more nuanced understanding of the risk relative to different stakeholders, and in relation to the context in which the risk evaluation is occurring. Where possible, risk evaluation compares the results of risk analysis to the risk criteria established for the organization. This comparison determines where additional action may be required to effectively manage the risk within the boundaries of risk appetite and associated risk tolerances. By completing a thorough risk evaluation, the costs associated with potential risk treatment options (both in terms of risk treatment costs and impacts on desired outputs and performance) developed in the follow-on risk management step are supported and can be objectively justified by the needs of various risk stakeholders.

The results of risk evaluation lead to taking one or more of the following courses of action:

- do nothing
- undertake additional analysis to better understand the risk.
- consider risk treatment options.
- reconsider objectives to avoid the risk (for example, due to cost considerations).

The following principles and attributes contribute to design, implementation, and operating effectiveness of this area of practice:

- considers established risk criteria.
- identifies key stakeholders of organizational objectives and associated risks.
- considers differences in various stakeholder interests and risk appetites.
- prioritizes risk in the risk portfolio.

8.2 Considers established risk criteria

8.2.1 Description: Risk criteria, including a risk appetite and relevant risk tolerances, enable objective decision-making on potential next steps to respond to the risk.

8.2.2 Explanation of Importance: Establishing meaningful criteria provides the organization with a set of objective and repeatable parameters against which risks can be evaluated. Having an established set of risk evaluation criteria is essential to determining if the level of current risk assessed during the risk analysis is at an acceptable level with no further action required, or is at an unacceptable level and requires treatment.

When the risk requires treatment, the risk criteria establishes the parameters to determine if a potential treatment will result in an acceptable level of risk, as well as the attributes any potential treatment should encompass. As ERM programs mature, and when the context in which risks are being evaluated changes, the organization should review and refine its established risk criteria.

8.2.3 Examples of how it might be achieved:

- In order to develop risk criteria, review the organization's risk appetite statement in comparison to the results of the risk analysis. If the risk appetite has various levels of acceptable risk given programmatic or functional area of the organization, select the most relevant category, or use the risk category adopted for the risk analysis.
- Assessment by key stakeholders of the acceptability of the analyzed risk if no formal written risk appetite statement exists.

- Review the risk criteria established by the organization for each program or organization objective, and compare the current level of a particular risk to established risk criteria. Any risk in excess of established risk criteria becomes a basis for treatment of the risk.

8.2.4 Possible types of evidence and examples:

- Documented evaluations of the acceptability/unacceptability of individual risk evaluations
- Written policy establishing unacceptable levels of risk (i.e., risk appetite) for various functional or programmatic areas of the organization, and which necessitate inclusion on a risk register or profile for treatment

8.3 Identifies key internal and external stakeholders of organizational objectives and associated risks

8.3.1 Description: Risks may impact different stakeholders in different ways, and identifying key internal and external stakeholders is necessary to ensure the organization understands how potential risk response decisions will affect key stakeholders.

8.3.2 Explanation of Importance: Effective evaluation of an enterprise-level risk requires an understanding of the stakeholders involved and their importance to the organization's mission, and sensitivity regarding specific organization objectives related to the risk event. A specific risk may affect different stakeholders or stakeholder groups differently. Understanding these differences is necessary to evaluate the acceptability of the risk event to the most important stakeholders. Gaining this understanding supports developing better justified and more cost-effective risk treatments which address key stakeholder needs.

8.3.3 Examples of how it might be achieved:

- Ranking of the most critical stakeholders for a specific objective
- Risk analyses tailored for specific stakeholders or stakeholder groups

8.3.4 Possible types of evidence and examples:

- Identification of key internal and external stakeholders for specific organizational objectives
- Documenting the impacts when different for key stakeholders or stakeholder groups

8.4 Considers differences in various stakeholder risk appetites to guide tradeoffs in risk treatment selection

8.4.1 Description: Once key stakeholders associated with an organizational objective are identified, risk evaluation should be considered from the stakeholder perspectives. This perspective includes acceptability of the current level of risk, the need for treatment, viable treatment decisions, and how aggressive a treatment is necessary.

8.4.2 Explanation of Importance: While the overall organizational risk appetite will guide the evaluation of risk acceptability, a review of specific stakeholder/stakeholder group acceptability will serve to further refine decisions on potential risk treatments. An understanding of how a potential risk impact will affect specific stakeholders and stakeholder groups enables understanding of the acceptability of a risk evaluation from the perspective of the overall organization. This, in turn, enables a portfolio view of risk critical for ERM. Without considering specific stakeholder impacts from a particular risk, risk evaluation will not necessarily guide developing the most effective and justifiable risk treatment that meets the most critical stakeholder interests.

8.4.3 Examples of how it might be achieved:

- Availability and use of risk analyses allowing evaluation of risks to an objective's identified key stakeholders
- Identification of specific stakeholder interests in objectives where risk appetite and existing risk tolerances do not reflect the interests of key stakeholders

8.4.4 Possible types of evidence and examples:

- Review of stakeholder organization documentation on importance of delivering on related outputs and outcomes
- Discussions/interviews with key stakeholders or organizations representing key stakeholders

8.5 Prioritizes risks in the risk portfolio

8.5.1 Description: A key difference between traditional risk management and ERM is that ERM promotes the understanding of risks as a portfolio, identifying how a particular risk relates to and effects other risks the organization is currently facing, or may face in the future.

8.5.2 Explanation of Importance: Developing an understanding of the inter-relatedness, dependencies and positive or negative correlations of a particular risk and its effect on the organization's risk exposure and overall risk portfolio may: 1) change the importance of allocating resources to treating a particular risk due to its impact on other risks across the enterprise; 2) guide the selection of an optimal risk treatment that may address more than one risk; and 3) enable more effective monitoring of risks after treatment. Without such consideration, the organization's risk management program may not be aware how risks and their treatments affect or are affected by other risks or risk treatments of the organization.

8.5.3 Examples of how it might be achieved:

- Consideration of how other existing risks can impact a risk under consideration in terms of impact, likelihood, or speed of onset.
- Consideration of how a risk under consideration will impact other current risks
- Comparison of a risk against the risk appetite and other relevant risk criteria while incorporating consideration of cross impacts with other risks in the portfolio.

8.5.4 Possible types of evidence and examples:

- Results of scenario analysis identifying likely interdependencies among risks impacting their likelihood, impact and velocity
- Meetings/discussion among risk owners and support personnel on the interconnection among specific risks
- Decisions to treat a risk, adjust risk treatments, or reconsideration of acceptable residual risk (after treatment) based upon considerations of risk interdependencies or varying stakeholder interests in risk acceptability.

Practice Area 9: Key Risk Indicators

9.1 Description: Key risk indicators (KRIs) are forward-looking metrics that alert management that a risk's likelihood, impact, or velocity (or any combination of the three) are changing and indicate if the risk is growing or receding. The change(s) reflected by the KRI are considered in relation to the organizations established risk tolerance to determine if the organization needs to initiate response actions. KRIs support risk-based decision making by alerting management to intensifying risks while there is still an opportunity to, for example, allocate financial and human resources to avoid problems or crises. Organizations develop KRIs after considering the inventory of risks, the risk evaluation and prioritization criteria, the risk culture, the status of the internal control environment, and the level of leadership buy-in. KRIs support the performance of an organization by signaling potential changes in an entity's ability to meet objectives.

More specifically, KRIs are a tool to help organizations identify and get ahead of potential risk situations that would impact performance, whereas key performance indicators (KPIs) track actual accomplishments over time. KRIs guard performance by helping to predict whether an organization can achieve a KPI. If a KRI signals a threat to the ability to meet an objective, management can, and should, take action to change course.

Table 9.1 provides an illustrative example of a KRI for the negative impact of Escherichia coli (abbreviated as **E. coli**) in the drinking water on human health, and its relationship to the associated KPI target.

KRI	Mitigating Strategy	Drivers	Risk	Consequences	KPI
Number of days per month the E. coli level in the drinking water is above 11 – 100 MPN/100 ml12	Water filtration efforts	Water pollution fluctuations	Changing levels of water pollution increase human infections	Health/Safety, Reliability, Reputational, Regulatory	No (zero) new E. Coli hospital admissions per year

Table 9.1 KRI Example

An important step in developing effective KRIs is to consider the various forces that have created the current risk environment. Past patterns and influences provide a valuable frame of reference for making decisions on which risks to track more closely with KRIs. For example, the forces that shape the United States economy have changed markedly over the last few decades. These forces include globalization, climate change, evolving technology, an increased focus on environmental, social, and governance issues, and most recently the global pandemic. Federal agencies are now being forced to rapidly evolve to an increasingly dynamic environment to operate effectively.

12 World Health Organization (WHO) drinking water risk assessment guidelines.

The key principles and attributes which contribute to the design, implementation, and operating effectiveness of the Key Risk Indicators area of practice include:

- Monitored against established thresholds
- Developed with senior leadership support and an understanding of the risk and control environment
- Developed with available supporting data
- Established KRI analysis and response processes

9.2 Monitored against established thresholds

9.2.1 Description: Organizations design KRIs to monitor known risks using metrics developed by management and informed by stakeholders.

9.2.2 Explanation of Importance: KRIs monitor known risks. They are not designed or meant to alert management to emerging risks. Management sets thresholds for each KRI based on available data, strategic assumptions, and established organizational risk tolerances. Thresholds should alert management to deviations from their assumptions. The thresholds are trip wires or triggers. Management must understand what should set off alarms (i.e., alerting management of potential risk). The calibration of the threshold is important to avoid false positives (i.e., there might be a good reason for breaking the threshold).

9.2.3 Examples of how it might be achieved:

- Approval of KRIs by senior leadership/senior risk council
- Regular review of the reasonability of the thresholds supporting the KRIs
- Seek input from stakeholders on the assumptions supporting the KRI thresholds
- Confirm that KRI thresholds are consistent with established organizational risk tolerances

9.2.4 Possible types of evidence and examples:

- Documented input from stakeholders supporting the KRI thresholds set by management
- Training that clearly links KRIs with known risks
- KRIs tie to top risks in the risk inventory

9.3 Developed with senior leadership support and an understanding of the risk and control environment

9.3.1 Description: Successfully developing and incorporating KRIs into an organization's risk management activities requires senior leadership support and an understanding of the design and operating effectiveness of controls.

9.3.2 Explanation of Importance: Management's capacity to develop KRIs and take action to address risks is significantly enhanced in organizations with strong senior leadership support and an end-to-end understanding of the risk and control environment. This is because senior leadership allocates new resources and the organization has already invested time and money to identify, understand, and manage known risks. Once management understands the key relationships between risks and internal controls, it gets easier to manage complexity and expected risk situations identified by KRIs.

It is also critical to understand that an organization cannot address all risks with internal controls. Internal controls work best as an integral part of operations that can help mitigate risks and add value. However, internal controls are not always effective at addressing risks arising from outside of the organization. For example, internal controls will not prevent political changes that result in Congress adjusting budgets that adversely impact an agency's ability to achieve its objectives.

Management can choose to avoid (e.g., stop taking an action), reduce (e.g., designing and implementing a new control), transfer or share (e.g., buy insurance, outsource the service that is the source of the risk), or accept (e.g., accept the risk as it is) a risk. Ideally, KRIs help align resources with priorities that are important to senior leadership. That is because approval for resources is much more likely to happen when managers can explain the need for resources in terms of preventing or mitigating risks to objectives relevant to senior leadership. Without that support, management might not get the resources needed to take proactive action to address the risk highlighted by the KRI. That, in turn, puts actual organization performance at risk.

9.3.3 Examples of how it might be achieved:

- Use information from internal and external environments
- Leverage risk inventories, risk evaluation and prioritization criteria, and current capabilities (e.g., processes, internal control design and operating effectiveness)
- Seek regular input from stakeholders on top risks

9.3.4 Possible types of evidence and examples:

- Agreement of senior leadership and/or risk council that the KRIs are tracking risks important to the organization
- Commitment of resources to manage risks identified by breached KRI thresholds
- Documented end-to-end understanding of transactions and supporting processes and controls

9.4 Developed with available supporting data

9.4.1 Description: Management develops KRIs for top risks facing the organization where supporting data is readily available, reliable, and understandable.

9.4.2 Explanation of Importance: It is important that data is readily available, reliable, and understandable to support developing KRIs for the organization's top risks. Effectively developing and monitoring KRIs requires an ongoing commitment of resources, and that commitment will increase if data is not readily available and in a format that is understandable and useful for that purpose Without available, reliable, and understandable data there is likely little value in tracking a KRI and can lead to frustration in collecting, compiling, and formatting the data. Organizations want to select and develop KRIs for the right number of risks to avoid data management and reporting issues. Absent a compelling reason (e.g., reputational considerations), organizations should generally avoid developing KRIs where the cost of getting data is greater than the cost of the impact to the entity should the risk materialize. For key risks where data are insufficient, organizations should use other methods to monitor changes to the risk.

9.4.3 Examples of how it might be achieved:

- Select risks that will get the support needed to effectively manage them
- Manage the number of KRIs to avoid data management complexities and reporting challenges
- Review and validate the assumptions underlying the KRI thresholds

9.4.4 Possible types of evidence and examples:

- Documented assumptions supporting the KRI thresholds (e.g., if this, then that)
- Meeting minutes capturing management discussions about the ongoing applicability of individual KRIs (e.g., are the KRIs still appropriate given the changing environment)
- On a monthly basis, staff updates KRI metrics with results in a timely manner using readily available data

9.5 Established KRI analysis and response processes

9.5.1 Description: The organization has defined structured and repeatable processes to analyze KRI data and to respond when the KRI exceeds its established threshold.

9.5.2 Explanation of Importance: Effective KRIs alert management to risks that are building while there is still time to respond. It is essential for organizations to have a system for timely and effective handling of information from KRIs to identify potential trouble ahead. Management uses KRIs to quickly analyze information for top risks. Speed is important when an organization is trying to stay ahead of problems. Without KRIs, organizations often struggle to analyze information in time to respond to risks before they become serious problems for management.

A robust risk culture will support the speed at which risk information travels to senior leadership for potential action. Executive-level understanding and commitment to risk management methods and tactical tools, such as KRIs, are critical for proactive decision making that drives performance and value.

9.5.3 Examples of how it might be achieved:

- Prioritize addressing risks before problems manifest
- Identify, assess, and prioritize any deviations (i.e., breached KRI thresholds)

9.5.4 Possible types of evidence and examples:

- Documented management approval of monthly metrics
- Release of funds to address a materializing risk