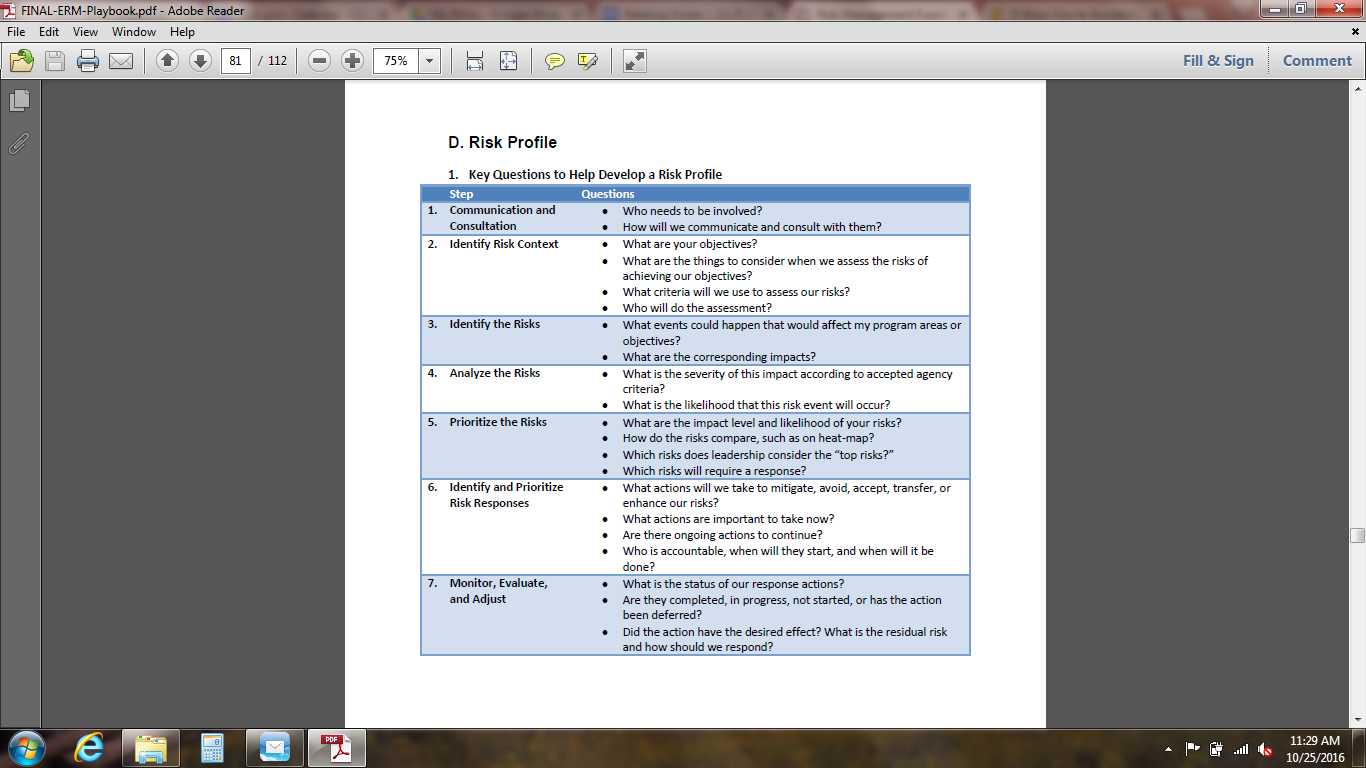
**Guidance for Preparing a Risk Register:**

**Risk Identification, Analysis, and Documentation**

**Introduction:** As part of the Enterprise Risk Management (ERM) implementation process, Components will develop risk registers to equip their leadership with information about risks that affect the vital interests or execution of Component- and agency-wide strategic objectives. A risk register contains details of the risks identified by an organization, in this case Component -wide risks, their level of priority, and the risk management actions underway to address the risks. The agency working group, consisting of representatives from ­­­­­­­­­[Component names] are assigned to help their Components develop the risk registers on a quarterly basis, collect the risk registers, and use them to prepare an agency-wide Risk Profile. The Component risk registers are meant to be used for risk management for the Component. Risk registers should be iteratively updated by Components to ensure external events, shifting priorities, and new information are incorporated. As ERM matures at the agency, so too will the risk identification, documentation, and analysis process within the Components and at the enterprise level. This document provides the “how-to’s” of developing a prioritized list of risks in the risk register, as well as a high level overview of ERM practices.

**Key Questions to Help Develop a Risk Register[[1]](#footnote-1)**



**Key Practices:** It is recommended to follow these practices to optimize Component efforts:

* Develop and promulgate consistent definitions to enable risk identification, documentation, and implementation.
* Leverage existing risk assessment and risk analysis tools in your Components to identify risks and build the risk register, such as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Integrate existing practices in your Component, like safety, operational, and financial risk management. For example, barrier and hazard analysis are often used to identify safety risks for people and property and can be incorporated into your efforts.
* Receive commitment by your leadership and set up an approach that ensures their active participation.
* While those creating the Component risk registers do not have to be risk experts or strategic planners, they must gain an understanding of the environment in which the risks are to be managed, taking into account strategic objectives for their Component and for the agency. Consider assembling a Component team of key program managers, directors, and stakeholders to develop and validate your risk register.
* Develop the risk register to inform your Components view of risks to promote better tradeoff decisions and enhance application of foresight.
* Understand and document key assumptions and uncertainties for risks identified and managed.
* Place an emphasis on creating an environment of "safe" disclosure of risks. Encourage program managers, directors, and stakeholders to share risk information to better collaborate on an action plan together and avoid risk contagion into other parts of your organization.

**Essential Factors of ERM**

* **Understand Mission Space, Values, Goals, and Objectives** to identify, assess, and manage those areas that may impede Component success.
* **Policies, Standards, and Regulations:** Account for policies, standards, or regulations in place and that complement or align with ERM efforts.
* **Scope and Criticality of the Decision:** Understand the decisions that have to be made for each risk, and the range of options available to your leaders. Consider the breadth and depth of the decisions’ impact. For example, if a high value program has schedule overrun by 12 months, should the program be cancelled, are there other options available, and how would this affect the program and the rest of the agency?
* **Decision Makers and Stakeholders:** Engage Component leaders and their staff at the outset of risk identification to tailor the risk register information. Understand the authorities and responsibilities of leaders, as well as their comfort level with risk management concepts and language. Similarly, stakeholders — those individuals or groups affected by the decisions — should be appropriately engaged and represented throughout the process to ensure concerns are being addressed.
* **Decision Timeframe:** Consider the time horizon from risk identification to risk management actions, and how the frequency of risk register updates influences the Component over the short-term or long-term. Use this to manage leadership and stakeholder expectations for risk management actions.
* **Risk Management Capabilities and Resources:** Develop a risk register that is practical and aligned with the Components capabilities, capacity, and processes. Also, ensure resources applied to support risk management in your organization and ERM for agency are commensurate with the complexity and magnitude of risks at hand.
* **Availability and Quality of Information:** When evaluating decision requirements, consider the availability and quality of information that can support the risk management effort, as available information will affect how the risks are managed. Convey anticipated data limitations, including data uncertainties.

**Identify Potential Risk:** Identifying a preliminary list of risks can generally be done from a basic knowledge of the subject matter and the decision needed. Risks can be identified at the Component level or as risks that are agency-wide. Consider these factors:

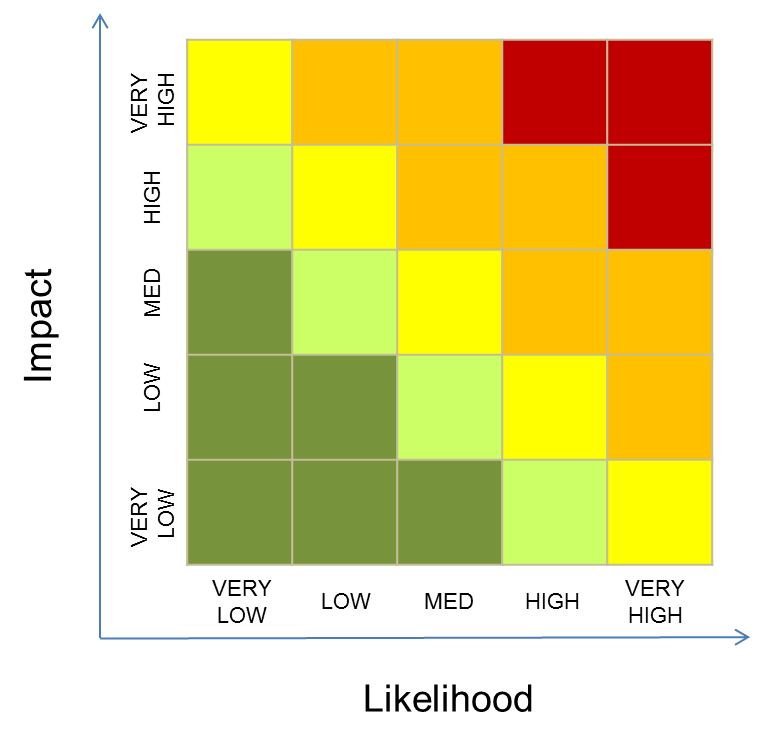
Gathering Risk Information: Collect data and evidence on different types of risks. Commonly used sources include historical records, models, simulations, and elicitations of subject matter experts and leadership. Data does not need to be quantitative. For example, the risk register may include difficult-to-quantify reputational effects. Throughout the process of identifying risks and the risk levels, compare risk information and identify uncertainties. The agency should identify common risk categories or a risk taxonomy that include items like **Financial, Reputational, Contractual, Programmatic, Legal, Compliance, Human Resources, Safety, Civil Rights, Reputational, and Economic.** While this list is not a collectively exhaustive list of risks, it accounts for the breadth of risks that may affect an organization.

Risks To and Risks From: Define elements affected (goals, objectives) to determine the “risk to” and capturing the things (hazards, resources, and institutional failures) that affect them to determine the “risk from.” This includes trigger points that would have to happen for a risk to occur. This approach will yield a fairly broad list of potentially adverse outcomes that will assist in the identification of mitigation efforts and resources.

Internal and External Risk: Risks affecting organizational effectiveness arise from both internal and external sources. Examples of internal sources are issues such as financial stewardship, program management, and systems reliability. These internal risks have the potential to derail effective operations and adversely affect mission accomplishment. Many organizations have additional risks to manage that are caused by external factors. Examples include global, political, economic, and societal trends, as well as hazards from natural disasters, malicious cyber activity, fraud, and accidents. Consider risks that are both within and outside of a Component’s direct control, including third parties, vendors, or contractors, but present a genuine risk to their strategic objectives. For major risks outside of direct Component control, often the only response may be to prepare contingency plans.

Unusual, Unlikely, and Emerging Risks:It is valuable to make a concerted effort to identify risks beyond those usually considered. For example, risks that are newly developing, even if they are poorly understood, are useful to identify to monitor the development of those risks over time. Risks that are highly unlikely but have high consequences, also known as “Black Swans” or megatrends, should also be identified and incorporated into the assessment, if possible. For example, rising sea levels from climate change and the potential effects on real property near coastal regions can be identified. Risks can include identifying unusual, emerging, and rare risks. Brainstorming a wide range of perspectives enables the identification of these risks, as well as the crosscutting nature of these risks. However, no risk identification process will capture every potential unwanted outcome — there will be things that happen that are unanticipated.

**Assess the Risk:** This section walks you through the components of risk assessment so that you can understand, prioritize, and document your Component’s risks in a risk register. Risk should be assessed, at a minimum, according to five levels: Very high risk, high risk medium risk, low risk, and very low risk. A high risk can greatly impede a Component’s ability to achieve their strategic objectives because the risk will have high impact, high likelihood, or both. A low risk is unlikely to occur and/or may have a low impact, but is worth documenting so that its potential effects can be monitored and considered in combination with other risks. On a 5-point scale, each risk for the Component would be assessed as **Very High = 5, High = 4, Medium = 3, Low = 2, or Very Low = 1**.The combination of impact and likelihood are what make up a risk “score.” This is depicted in the figure below, known as a *risk matrix* or a *risk heat map*):



Risk Calculation: Assessment of each risk is based on two factors: **Likelihood** and **Impact**.

* The **impact** (or consequence) of a risk occurring is assessed as **Very High = 5, High = 4, Medium = 3, Low = 2, or Very Low = 1**. Impact is the potentially negative effects of an incident or situation to the ability of an organization to execute its mission and achieve its strategic objectives. Each impact score should include, at a minimum, an assessment of mission disruption, economic impact, and external visibility (reputational impact). The resulting scores will be calculated automatically in a risk assessment workbook provided. The scales used for each impact category is shown in the following table:

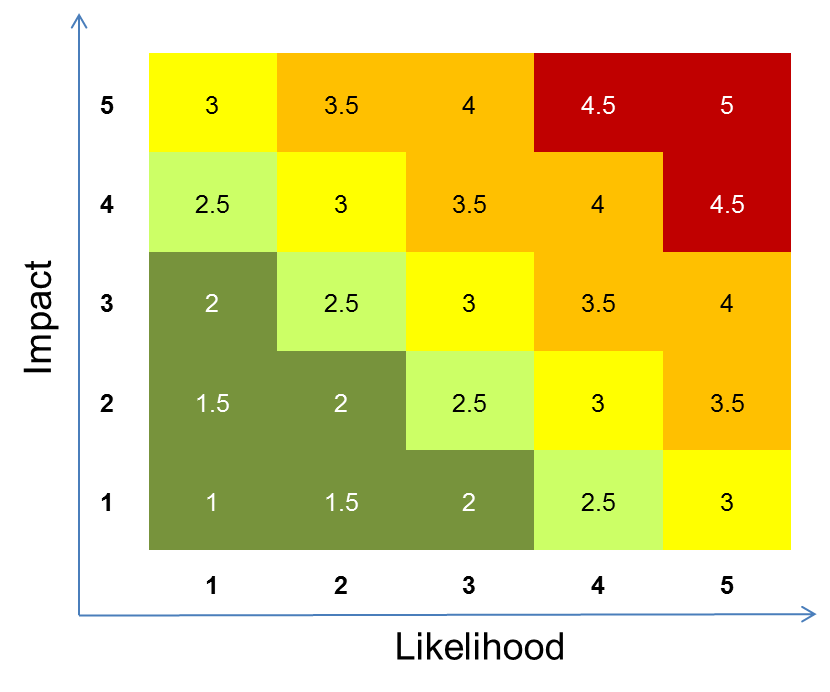
**CONSEQUENCE ASSESSMENT**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | VERY HIGH = 5 | HIGH = 4 | MEDIUM = 3 | LOW = 2 | VERY LOW = 1 | SCORE |
| **Mission Disruption** | More than 8 infrastructures (or systems or networks) affected; major disruption to agency program(s) | More than 4, less than 8 infrastructures (or systems or networks) affected; major disruption to agency program(s) | More than 2, less than 4 infrastructures (or systems or networks) affected; moderate disruption to agency program(s) | At least 1, no more than 2 infrastructures (or systems or networks) affected; minor disruption to agency program(s) | No more than 1 infrastructure (or system or network) affected; or minor disruption to an agency program |  |
| **Economic Impact** | More than $50 million | More than $10 million and less than $50 million | More than $5 million and less than $10 million | More than $1 and less than $5 million | Less than $1 million |  |
| **External Visibility** | Visibility of risk with US Population, including mainstream media coverage and public interactions | Visibility of risk in reports by GAO, IG, CRS, or federal media (i.e., Federal News Radio, etc.) | Visibility of risk with other federal government agency (agencies) or department(s) | Visibility of risk at the Administrator and Deputy Administrator level | Visibility of risk at the Component level |  |
|  |  |  |  |  |  | **Impact Score** |

* The **likelihood** of a risk occurring is assessed as **Very High = 5, High = 4, Medium = 3, Low = 2, or Very Low = 1**. Likelihood is the chance of an incident happening or a situation occurring, defined in the table below as probabilities of occurrence.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **LIKELIHOOD ASSESSMENT** | | | | | | |
|  | VERY HIGH = 5 | HIGH = 4 | MEDIUM = 3 | LOW = 2 | VERY LOW = 1 | Score |
| **Mission Disruption** | Very Likely | Somewhat Likely | Uncertain | Not Likely | Very Unlikely |  |
| **Economic Impact** | Very Likely | Somewhat Likely | Uncertain | Not Likely | Very Unlikely |  |
| **External Visibility** | Very Likely | Somewhat Likely | Uncertain | Not Likely | Very Unlikely |  |
|  |  |  |  |  |  | **Likelihood Score** |

* Impact and likelihood scores are automatically calculated. Risk scores equate to the figure below:

:

Example. A Component is concerned about cyber intrusions to one of its key IT systems. You perform a risk assessment that yields the following scores:

* Mission Disruption: **Very High - 5.** A cyber intrusion could cause mission disruption to several programs in the Component because of the recovery and remediation required to identify leaked information and latent viruses.
* Economic Impact: **Medium - 3.** Invoices valued at more than $2 million will be delayed due to the recovery and remediation of the IT system after a cyber intrusion. The cost of setting up firewalls and to hire information security analysts will be more than $1 million.
* External Visibility: **High - 4.** GAO and OIG may investigate a cyber intrusion of this nature.

**(Overall Impact Score: High - 4.1 calculated in the risk assessment workbook)**

* Likelihood of Mission Disruption: **Somewhat Likely - 4.** In the case of a cyber intrusion to collect information, it is somewhat likely to disrupt the mission.
* Likelihood of Impact: **Not Likely - 2** Economic impact is uncertain at the level noted.
* Likelihood of External Visibility: **Uncertain - 3** A cyber intrusion is uncertain for coverage by external sources.

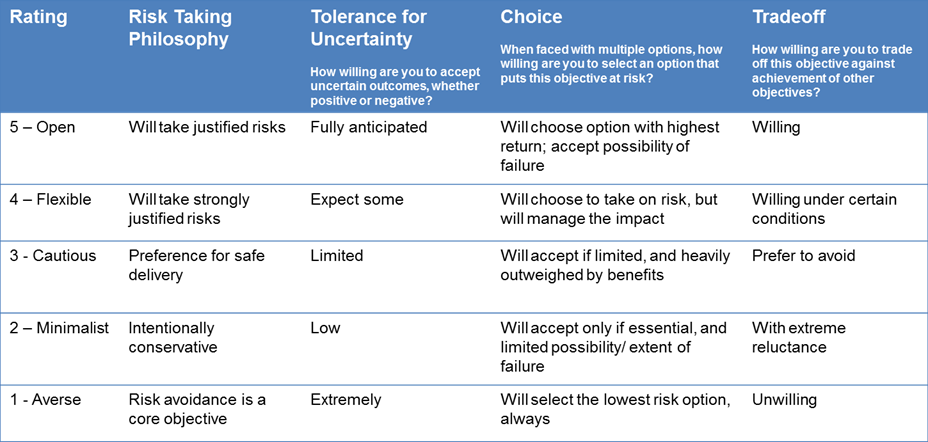
**(Overall Likelihood Score: Medium - 3.1, calculated in the risk assessment workbook)**

* The Impact Score and the Likelihood Score are averaged to achieve an overall risk score.

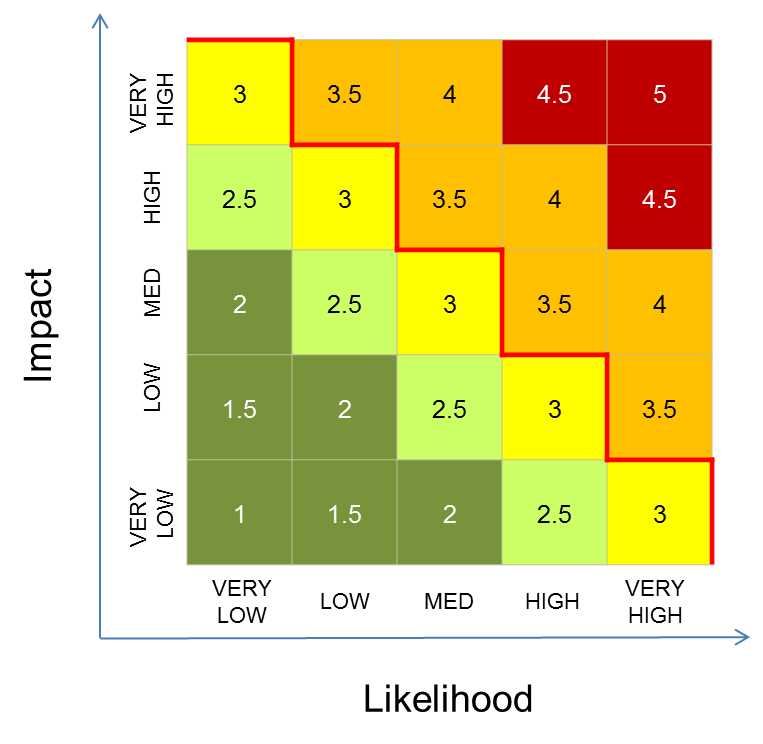
**(Overall Risk Score: High - 3.6, calculated in the risk assessment workbook)**

Evidence and Comments. Evidence that is qualitative or quantitative in nature should be provided for impact scores and likelihood scores. Comments can be provided by the Component to further explain any of the impact or likelihood scores.

Risk Appetite: Risk scores will be compared to the risk appetite of the agency. If a risk is above the risk appetite level, then it should be prioritized higher by the Component and noted as such in the risk register.  **Risk appetite** is the agency-wide agreement of the amount of risk the agency is willing to accept in pursuit of strategic objectives. This means the agency may avoid risks that could have exceedingly negative impacts, as well as pursue calculated risks that could have beneficial outcomes (opportunities). Risk appetite also helps define organization’s risk culture by capturing the norms and traditions that inform daily decisions made by management and employees. The table below provides a way to think about risk appetite levels from Corporate Executive Board in 2015 and GAO in 2016. The agency sets their risk appetite rating at approximately **3 - Cautious**.



Because the agency places its risk appetite at **3 - Cautious**, you can determine if your risk falls below or above the risk appetite level, indicated in the figure as the **red line**:



Example (continued): In the case of the cyber intrusion example, the risk is above the risk appetite level for the agency, making this risk a high priority.

**Findings**: Once you have completed a risk assessment for each risk, information should be documented in the risk register form.

**Composition of Risk Register:** The risk register should contain the following information:

* The **strategic objective(s)** to which the risk aligns from the most recent Component Strategic Plan and the agency Strategic Plan. References to the Administrator’s Priorities are also included in this section. Multiple strategic objectives can be listed if they are relevant.
* A brief **risk description** to make the risk easy to discuss, typically an “If, Then” statement to capture the cause and effect.
* The **risk score** section contains the risk score calculated in the risk assessment workbook.
* The **Component** **owner** of the riskis the person managing the risk, such as a program manager, a division director, or even the Component head if the risk is assessed as High.
* The date that the risk was first **raised** will be placed in this section of the risk register.
* **Last risk score and date recorded** should be noted for risks that are tracked on an ongoing basis. If the risk is newly added to the risk register, identify the risk as the “first risk score” with the date.
* **Risk management actions** include all mitigating actions underway to manage the risk, including monitoring risk if nothing can be done about at risk at this time, controlling risk through internal controls and procedures (for example), sharing risk by pooling resources with other offices, avoiding risk by forgoing certain actions, or a combination thereof.
* **Key assumptions and uncertainties** for the risk or during the risk assessment processshould be communicated for each risk. For example, if you made analytical assumptions, note those in the risk register. Document uncertainties about data sources as well. Documenting assumptions and uncertainties aids the risk owner should the risk occur, as it will ensure this information was communicated upfront and in a transparent manner.

**Risk Register Template**

A fillable risk register form and an example can be found at [insert link]**.**

**Risk** **Register Timeline:** Components develop and update risk registers on a quarterly basis. Components are responsible for managing and updating their Component risk registers. The CRO team collects the risk registers and provides these to the ERM Group to evaluate the risks from an enterprise perspective and to provide final findings in an agency Risk Profile. The agency Risk Profile will be prepared in the same manner as the Component risk registers, with a few noteworthy exceptions. First, the ERM Group will consider interactions of risks across Components and if interactions will amplify or attenuate a risk. Second, the ERM Group will consider risks that are not assigned to any one Component, such as climate change risks, which are cross-cutting in nature. Third, the ERM Group will consider, when possible, systematic, emerging, and unlikely - but catastrophic - risks (also known as Black Swans). Fourth, the ERM Group will consider other sources of enterprise risks like the GAO High Risk List. The ERM Group provides an agency Risk Profile to the Senior Management Team for final validation, who then re-distributes to their offices for action. The quarterly timeline is as follows:

* Fiscal year quarter ends
* 1 day after the quarter ends, a data call goes to the Components for risk registers
* Components have 21 days to develop and update their risk register and submit to the CRO Team
* The ERM Group has 5 days to evaluate enterprise risks and make final recommendations for the agency Risk Profile
* The Senior Management Team validates the agency Risk Profile and re-distributes to relevant stakeholders in the Components and the ERM Group

**Risk Management:** Ultimately, the objective of the risk assessment process is to provide decision makers with an understanding of “inherent” or initial risk -- the risk before mitigating actions are taken -- and the residual risk -- the risk after mitigating actions are taken. Actions include controlling risk through internal controls and procedures (for example), sharing risk by pooling resources with other offices to manage the risk, avoiding risk by forgoing certain actions, monitoring risk if nothing can be done about a risk at this time, or a combination thereof. You can work with your Component to identify and assess risk management options. Portions of this step may be performed by different practitioners as long as they can tie proposed options to the results of a risk assessment. Risk management costs — both monetary and non-monetary — serve as valuable data for aiding decision makers in making effective and efficient choices. It is important to note again that to state that risk will be eliminated through risk management actions is inaccurate, although risk can be controlled to tolerable levels. Also, some risks will be assessed as inherent to agency’s mission and strategy, such as the risk associated with new OMB mandates or budget fluctuations of federal agency customers due to changes in appropriations. While doing nothing is not an appropriate response for these types of risks, the most practical option may be to document the risk and monitor it.

While choosing risk management actions, you should discuss the costs and benefits, expected outcomes, and likelihood of success of each action. Since risks often shift, it is important to revisit the risk management actions regularly to incorporate new information and re-evaluate based on changing circumstances. Proposed risk management actions should be discussed with senior Component leadership. Include strengths and weaknesses, in a way that informs their common understanding of the Component’s risks.

**Evaluation and Monitoring:** Components should assess the effectiveness of risk management implementation and the actual risk mitigating actions themselves. Through effective evaluation and monitoring, you may find it necessary to adjust risk management actions. It is crucial that a process of performance measurement be established to evaluate whether the actions taken ultimately achieve the intended risk mitigation results. It is also important to monitor the larger context within which an identified risk and risk management efforts exist. Good situational awareness may reveal changes in the context that require changes in the risk management effort. Both types of monitoring — effectiveness and situational awareness — allow for effective risk management over time.

**Risk Occurrence:** Should a risk occur that was listed on the Component risk register, bring it to the attention of Component leadership immediately and ensure the ERM Group and senior management team are aware of the risk so that actions and responses can be taken. This will ensure appropriate resources and strategies can be implemented to address the issue. A risk event template, for example, could be created to track risk occurrences and subsequent corrective action plans.

1. Between Steps 6 & 7 on the chart, action/response decisions & implementation will be made by those in authority [↑](#footnote-ref-1)