|  |  |
| --- | --- |
| Risk Management Process | |
| **Process Owner**: Delivery Center of Excellence | **Approval Date**: 10/20/2017 |
| AUTHORIZED DOCUMENTS ARE PUBLISHED ONLINE ONLY. VERIFY ANY COPY AGAINST THE ONLINE SYSTEM BEFORE USE. | |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | Date | Summary of Changes | Author |
| 0.1 | 05/12/2015 | Created initial draft | Meredith Luecker |
| 0.2 | 05/12/2015 | Performed peer/management/QA review. Ready for EPG review. | Beth Leonard |
| 1.0 | 07/29/2015 | Final approved baseline. | EPG |
| 1.1 | 10/10/2017 | Yearly QA review. | Matt Clark |
| 1.2 | 10/15/2017 | Performed management review; no major changes. | Beth Leonard |
| 2.0 | 10/20/2017 | Final approved baseline. | Beth Leonard |

Record of Acceptance/Approval

|  |  |  |
| --- | --- | --- |
| Delivery Center of Excellence | | |
| Printed Name: Beth Leonard |  | Date: |
| Signature: Virtual approval |  | 10/20/2017 |

|  |  |  |
| --- | --- | --- |
| Process Description | | |
| Risk management allows the project manager (PM) to identify potential problems and take preventive action to avoid a negative impact to project scope, schedule, cost, quality, or resources. A continuous risk management approach is applied throughout the project lifecycle to effectively anticipate and mitigate risks that may critically impact project success. A project’s risk response strategy is documented and executed according to the approach approved in the Project Management Plan (PMP) or Risk Management Plan (RMP), if a project chooses to create a sub plan for risk management. Figure 1‑1 below shows the process steps for risk management.    Figure ‑: Risk Management Process Steps with Inputs and Outputs | | |
| Assets and References | | |
| * *Attain Project Management Policy* * *Attain Engineering Management Policy* * Project Management Plan Template (PMP) * Risk Management Plan Template (RMP) * Attain In-process Review Template (IPR) * Attain Risk Peer Review Checklist Template | | * Attain Risk Issue and Decision Log Template * Attain Corrective Action Report Template * Attain Risk Management Process Training * Attain Delivery Center of Excellence (DCoE) SharePoint intranet site * Project CM repository |
| Suggested Measures | | |
| * Number of risks based on category and/or source; trended over time period * Number of risks controlled, accepted, transferred, and avoided; trended over time period * Risk mitigation peer reviewed vs. original ratings within IPR – comparative to standard deviation for statistical process control (Risk estimation accuracy) (e.g., >90% accuracy target) | | |
| Roles and Responsibilities | | |
| Project Customer | * Participates in risk escalation and approves contingency plans | |
| Senior Management | * Provides oversight and resources as needed * Participates in risk escalation and contingency planning * Participates in program management reviews (PMRs/IPRs) and provides feedback on high-severity risks | |
| PM | * Documents the risk plan in the PMP/RMP * Documents risks and associated contingency plans in a risk register * Reviews the risk register and contingency plans during project team meetings * Reports risk status to senior management and customer on a regular basis * Has ultimate responsibility for the final decision regarding risk actions * Ensures monthly IPRs are provided to Delivery Excellence for peer review | |
| Project Team | * Works with the PM to identify, analyze, monitor, and control all risk items during the project lifecycle * Reports risk status to the PM on a regular basis as defined in the PMP/RMP | |
| Delivery Excellence | * Provides process templates, guidance, and training * Ensures adherence to the process * Receives risk metrics from the PM | |
| Definitions of Acronyms and Terms | | |
| CM | configuration management | |
| DCoE | Delivery Center of Excellence | |
| IPR | In-process review | |
| OTP | Organization Training Plan | |
| PMP/ | Project Management Plan | |
| PMR | program management review | |
| RMP | Risk Management Plan | |
| SMP | Service Management Plan | |
| SOW | Statement of Work | |

# Process Steps for Risk Management

The following subsections detail the process steps for risk management.

## Develop Project’s Defined Process

Review the *Attain Risk Management Process*. The PM, or designee should document project specific risk process information, based on the customer needs, in either a standalone RMP or defined within a section in the PMP/Service Management Plan (SMP). The Attain Risk Management Plan Template aligns with this process and can be used in conjunction with the Attain Risk Issue and Decision Log Template. If the customer requires a different process to be followed, tailor the project’s plan to meet customer needs and justify tailoring using the tailoring form located in the DCoE SharePoint intranet site. Work with the Attain Delivery Excellence team to complete the tailoring steps. The project team, and relevant stakeholders, review and approve the RMP, PMP, or SMP. Ensure IPR process is addressed within plan.

The applicable project team members must be trained on the *Attain Risk Management Process*. Refer to the *Attain Organization Training Plan (OTP)* for process training requirements.

* **NOTE:** The Assets and References section above lists available templates and documents that can be found on the DCoE SharePoint -intranet site. Other comparable templates are available and may be used to support this process.
* **NOTE:** In the RMP, capture how risks are documented, managed, communicated, and reported to relevant stakeholders. Risks can be documented in either of the risk register templates found in the DCoE portal on SharePoint, a risk list within SharePoint, or by another method specified by the RMP/PMP.

## Document Risks

Internal and external stakeholders contribute to the identification of risks. Document the risk description, potential impact(s), risk source, and risk category in the risk register. Refer to the risk register templates for examples of risk sources and categories. While usage of the Attain Risk Issue and Decision Log provided in the DCoE intranet site Template Library for use by the PM is not required, a comparative log may be used.

* **NOTE:** The Attain Risk Management Plan Template and the Attain Risk Issue and Decision Log Template contains detailed instructions beyond what is listed within this process. Utilize the plan and template in conjunction with this process when documenting risks at the project/contract level on a weekly/monthly basis. Utilize the IPR template to raise higher-level risks to the IPR board on a quarterly basis. Submit to Delivery Excellence for peer review on a monthly basis.

## Analyze and Prioritize Risks

Evaluate, categorize, and prioritize by severity each identified risk in the risk register based on the risk parameters; Risk Impact, Probability of Occurrence, and Severity. During risk analysis, analyze potential risk events based on the impact (if the risk occurs) and the probability of occurrence.

Table 1‑1 provides an example of quantitative risk severity (prioritization) analysis determination.

Table ‑: Risk Severity Quantitative Determination

| Probability | Impact | | | | |
| --- | --- | --- | --- | --- | --- |
| 5 | 5 | 10 | 15 | 20 | 25 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 1 | 1 | 2 | 3 | 4 | 5 |
|  | 1 | 2 | 3 | 4 | 5 |

Conducting a quantitative risk analysis is recommended so that the project team has the best insight into the risks impeding the project. Since impact is the primary driver for treating risks, determining the quantitative impact (e.g., 6 week schedule delay, $500,000 budget overrun) results in targeted, highly effective risk treatment plans.

In the RMP/PMP, define the threshold for severity for which the risks will be monitored. All risks below the specified threshold need not have a detailed response/contingency plan.

## Determine Risk Response Strategy

Based on the outcome of risk analysis activities, document risk triggers, indicators that a trigger is imminent, and an appropriate risk response strategy for each risk. Industry accepted strategies include the following:

* **Acceptance** – Acceptance recognizes the risk and its uncontrollability. It is a “passive” technique that focuses on allowing whatever outcome to occur without trying to prevent it. This technique is normally used for “low” or “very low” risks where a scope-efficient means of reducing the risk is not apparent.
* **Avoidance** – Avoidance uses an approach that avoids the possibility of risk occurrence. It can be thought of as nullifying the risk by changing the contract parameters established between the customer and contractor.
* **Control** (or **Mitigation**) – Control involves taking action to reduce the risk’s likelihood or impact. Control-based actions occur at all points throughout the project lifecycle and are typically the most common response. They typically identify a mitigating action or product that becomes part of the project plan to be monitored and reported within the project’s regular analysis and reporting activities.
* **Transference** – Transference is the process of moving the risk from one party to another. For example, transferring the risk to the customer or to a sub-contractor. Typically, transference includes sub-contracting a portion of work to specialist suppliers who are able to reduce the organization’s overall risk exposure. This technique is best utilized during the proposal process. Transfer can also include the use of third-party guaranties.
* **Monitor** – Monitoring may be selected in the event that the risk response has been successful and the risk is believed to be no longer applicable. The project team can use this status to monitor for a period of time before closing out the risk.

Based on severity, draft risk response plans for all risks where the risk strategy is avoidance, control, or transference; and follow those plans through closure. Response plans are made to ensure that the risk does not occur (i.e., action taken to reduce the probability of risk occurring). Risk response strategies and plans should be approved by relevant stakeholders and reviewed at least monthly, as documented in the RMP (or PMP, as appropriate), in order to re-assess and revise risks and response strategies as needed.

* **NOTE**: Risks that are accepted require no response /contingency plan.

## Determine Contingency Plans

Draft contingency plans for high priority risks, as appropriate. Contingency plans are those that are put into action once the risk happens to help reduce the impact of the risk.

## Monitor and Control Risks

Clear lines of communication promote trust and honesty among project stakeholders. It is the PM’s responsibility to provide risk status to stakeholders in a timely manner so that the stakeholders have an opportunity to make effective decisions that make sense to their strategic objectives. Document the risk management communication and reporting frequency, and methods, in the project’s RMP/PMP. High stakes risks warrant more frequent communications than a low to moderate stakes risk. Continuously update and review the risk register so that new risks are captured and existing risks remain at an acceptable level. If triggers are increasingly imminent for high stakes risks, elevate the concern to senior Attain and customer management, as appropriate, for additional intervention.

Should risks become issues, transfer the risk to the issue log tab of the Attain Risk Issue and Decision Log for more detailed corrective action. Thresholds for more formal corrective action reporting should be identified within the project’s PMP/SMP. Consider using the Attain Corrective Action Report Template.

* **NOTE**: Inform senior management of high risk/high stakes risk items immediately so that a risk response strategy may be put in place in order to minimize the likelihood of a trigger occurring. **Ensure these types of risks are addressed within the IPRs. Refer to the Attain IPR Template for details and instructions.**

## Store Documentation in the Configuration Management Repository

The PM provides the risk register and any other appropriate risk-related artifacts to the configuration manager, or designee. The configuration manager stores the documents appropriately under configuration control in the centralized configuration management (CM) repository.