**VistA Adaptive Maintenance VAEC Security**

**(VAM)**

Contractor Project Management Plan



Department of Veterans Affairs

Office of Information & Technology

Contract No: VA118-16-D-1009

**Date: May 3, 2019**

Version 1.2

PAGE INTENTIONALLY LEFT BLANK

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 05/03/2019 | 1.2 | Updated Contractor Project Management Plan | AbleVets |
| 04/03/2019 | 1.1 | Updated Contractor Project Management Plan | AbleVets |
| 03/04/32019 | 1.0 | Initial draft of the document | AbleVets |

Artifact Rationale

The Project Management Plan (PMP), according to the Guide to the Project Management Body of Knowledge (PMBOK®), is a formal, approved document used to guide both project execution and project control. The primary uses of the PMP are to document planning assumptions and decisions; facilitate communication among stakeholders; and document approved scope, cost, and schedule baselines. By showing the major products, milestones, activities, and resources required on the project, it is also a statement of how and when a project's objectives are to be achieved.

The project manager creates the PMP following input from the project team and key stakeholders. The plan should be agreed on and approved by at least the project team and its key stakeholders.

The PMP is mandatory for all projects. While it is a project-level document, it should be updated as necessary, including for each increment.

Table of Contents

[1. Introduction 1](#_Toc7698952)

[1.1. Project Overview 1](#_Toc7698953)

[1.2. Project Scope 2](#_Toc7698954)

[1.3. Technical Approach 3](#_Toc7698955)

[1.4. Goals and Objectives 4](#_Toc7698956)

[1.5. Stakeholders and Key Personnel 4](#_Toc7698957)

[2. Project Organization 5](#_Toc7698958)

[3. Testing 6](#_Toc7698959)

[4. Monitoring and Control Mechanisms 6](#_Toc7698960)

[4.1. Budget Monitoring 6](#_Toc7698961)

[4.2. Schedule Monitoring 7](#_Toc7698962)

[4.3. Risk Monitoring 7](#_Toc7698963)

[5. High-Level Build Schedule 7](#_Toc7698964)

[6. Project Success Criteria 8](#_Toc7698965)

[7. Communication Management Plan 8](#_Toc7698966)

[8. Risk Management Plan 9](#_Toc7698967)

[8.1. Identify Risks 9](#_Toc7698968)

[8.2. Risk Analysis 10](#_Toc7698969)

[8.2.1. Risk Probability 10](#_Toc7698970)

[8.2.2. Risk Impact 10](#_Toc7698971)

[8.2.3. Risk Severity 11](#_Toc7698972)

Table of Figures

[Figure 1: Project VAM Organizational Chart 5](#_Toc7700544)

[Figure 2: EAC Tool Example 7](#_Toc7700545)

Table of Tables

[Table 1: PWS Task Areas 1](#_Toc7700563)

[Table 2: Stakeholders 4](#_Toc7700564)

[Table 3: Risk Probability Matrix 10](#_Toc7700565)

[Table 4: Risk Impact Matrix 10](#_Toc7700566)

[Table 5: Risk Severity Matrix 11](#_Toc7700567)

# Introduction

This Contractor Project Management Plan (CPMP) lays out the approach, timeline, and tools to be used in delivering the VistA Adaptive Maintenance VAEC Security (VAM) project. This CPMP defines how the VAM project will be executed, monitored and controlled, and closed in accordance to the VA Integration Process (VIP). It will be progressively elaborated by updates throughout the course of the VAM project.

This CPMP includes the strategy for coordination and execution of planned, routine, and ad hoc data collection reporting requests as identified within the PWS. This CPMP is meant to be a communication vehicle for ensuring the key stakeholders of VAM share a common understanding of the VAM project.

While this CPMP is the plan that defines how the VAM project is being executed, monitored, controlled, and closed, the VAM project’s schedule is a separate document that lists planned dates for performing tasks and activities to meet milestones identified in this CPMP.

## Project Overview

VAM is meant to Manage, plan, develop, design, integrate, test, and implement centralized services to provide comprehensive, real-time 24/7 monitoring and security for all Veteran data in all VistA systems migrated to the VA Enterprise Cloud.

The VistA Adaptive Maintenance system is a Cloud-Smart / Cloud-Native application developed and deployed in the dedicated U.S. FedRAMP-HIGH, HIPAA-compliant VA Enterprise Cloud (VAEC) leveraging Amazon Web Services (AWS) commercial cloud infrastructure and services. VAM provides comprehensive, commercial cloud-based monitoring and security for all clients, applications, and users that access VistA data using VistA’s Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for production enterprise’s use in the VAEC leveraging AWS Kinesis, and provides comprehensive commercial cloud-based VistA RPC Interface monitoring and security for all VistA systems migrated to the VAEC. VAM is 100% Legacy-free, Cloud-Native, and Non-invasive - allowing it to be scaled and deployed enterprise-wide without any change to any VistA system required.

In other words, VAM is meant to be Data-Driven, minimally-invasive intelligent auditing and alerting classifier system of RPC inquires in to the VistA.

Table 1: PWS Task Areas

| **PWS/TASK** | **Summary of Task Requirements** |
| --- | --- |
| 5.1 Project Management | 1. CPMP 2. Monthly Progress Report 3. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate 4. Signed Contractor Rules of Behavior 5. VA HIPAA Certificate of Completion 6. Onboarding Status Report |
| 5.2 Adaptive Maintenance Services | 1. Comprehensive RPC Interface Audit Report 2. MUMPS RPC to JSON Model Data Definition 3. Version Description Document (VDD) 4. Automated CloudWatch Configuration 5. Security Vulnerability Report |
| 5.3 Testing | 1. Master Test Plan 2. RPC Interface Test Suite |
| 5.4 Assessment and Authorization (A&A) Support | Update the following VAEC A&A artifacts quarterly, as applicable.   1. System Security Plan 2. Security Configuration Plan 3. Information System Contingency Plan 4. Incident Response Plan 5. Privacy Impact Assessment 6. Risk Assessment 7. Security Configuration Checklist (SCC) 8. System Interconnection Agreements (MOU and Interconnection) 9. Interconnection Security Agreement 10. Signatory Authority |
| 5.5 Initial Operating Capability (IOC) Support | 1. Production Operations Manual 2. Deployment, Installation, Backout, and Rollback Guide 3. User Guide |
| 5.6 Release and Deployment Support | 1. Capacity, Performance, and Scalability Assessment for National Deployment |

## Project Scope

The VAM Project will provide the complete audit, analysis, and translation of the entire VistA RPC interface into a modern machine-processable form, to be operationalized and scaled for production enterprise use on the VAEC CloudWatch monitoring tool in order to provide a comprehensive cloud-based VistA RPC Interface monitoring and security for all VistA systems migrated to the VAEC.

The following will be provided over the life of the project:

* Support for Project Management
* Software Design and Development
* System Testing
* Cybersecurity Testing and Remediation
* Performance & Regression Testing
* System and Software Documentation
* Risk and Defect Management
* Release and Deployment
* Support for Authority to Operate (ATO), and A&A assessment

## Technical Approach

AbleVets shall provide VistA adaptive maintenance by providing enhanced Veteran data security via comprehensive VistA RPC content audit and monitoring so that all VAEC-deployed VistA systems are adequately secured.

AbleVets shall:

1. Complete the analysis of the MUMPS code for the remainder of the 5500 RPC interfaces and perform modeling to identify, for each RPC:
2. Types, categories, and volumes of data it accesses (e.g., does the RPC affect pharmacy, laboratory or other clinical applications only or does it affect all/most VistA applications?)
3. Actions it performs (e.g., does it perform read only functions or does it also allow write access to the patient record?)
4. Sensitivity of the data it handles (e.g., is the data Protected Health Information (PHI) or is it non-PHI?)
5. End-users, applications, and clients accessing the system (e.g., is it a legitimate end user, or a rogue client/intruder?)
6. Provide and document the comprehensive audit of the complete VistA RPC Interface (all 5,500 MUMPS RPC calls), and translation of this MUMPS code into a machine-processable form that is implementable within the VAEC-resident CloudWatch tool.
7. Deliver a MUMPS RPC to JSON model data definition that represents the outcome of the audit and MUMPS to JSON model translation.
8. Provide a quarterly Version Description Document (VDD) which details the progress to
9. completion of the complete audit and model translation for all 5,500 VistA RPCs.
10. Scale the interface monitor for production deployment.
11. Provide an Automated CloudWatch Configuration which automates the capture, storage, monitoring and audit of all RPC traffic in the VAEC-resident CloudWatch COTS tool on a continuous and fully automated basis.
12. Pull RPC traffic from CloudWatch, and based on comprehensive audit, automatically classify and quantify RPC traffic to:
13. Identify all clients accessing VistA data via the RPC interface.
14. Identify all users accessing VistA data via the RPC interface
15. Identify and audit all types, volumes and categories of data being accessed via the RPC interface, with an indication of sensitivity
16. Configure CloudWatch to generate real-time alerts and alarms based on identified vulnerability and sensitivity conditions of RPC traffic. Demonstrate the success of the Automated CloudWatch Configuration operational performance by providing a fully automated validation of the completeness and correctness of the RPC interface audit.
17. Produce a Security Vulnerability Report including:
18. Number and type of clients accessing Veteran data
19. Number and type of users accessing Veteran data
20. Volumes and types of data being accessed, and an indication of sensitivity of data accessed

## Goals and Objectives

As VA continues to strengthen its cybersecurity profile, the VAM effort will provide the following benefits:

* Reducing the cost and complexity of maintenance of VistA systems
* Resolving severe security vulnerabilities of all VistA systems migrated to VAEC
* Taking full advantage of the features and scaling of VA’s new commercial cloud capabilities
* Ensuring the safe, secure, and seamless continuity of veteran care and services as VistA systems are migrated to the VAEC

## Stakeholders and Key Personnel

Stakeholders (**Table 2**) have different interests and expectations for the VAM project; they must be identified in the beginning of the project and continuously validated in order to meet all Stakeholder requirements. Identifying Stakeholder expectations:

* Provides the VAM team with an understanding of the Stakeholders’ perspective
* Ensures all of the Stakeholders’ expectations are being addressed
* Instills Stakeholders’ trust and cooperation
* Defines the project’s approach to meet requirements and validate the design throughout the project lifecycle

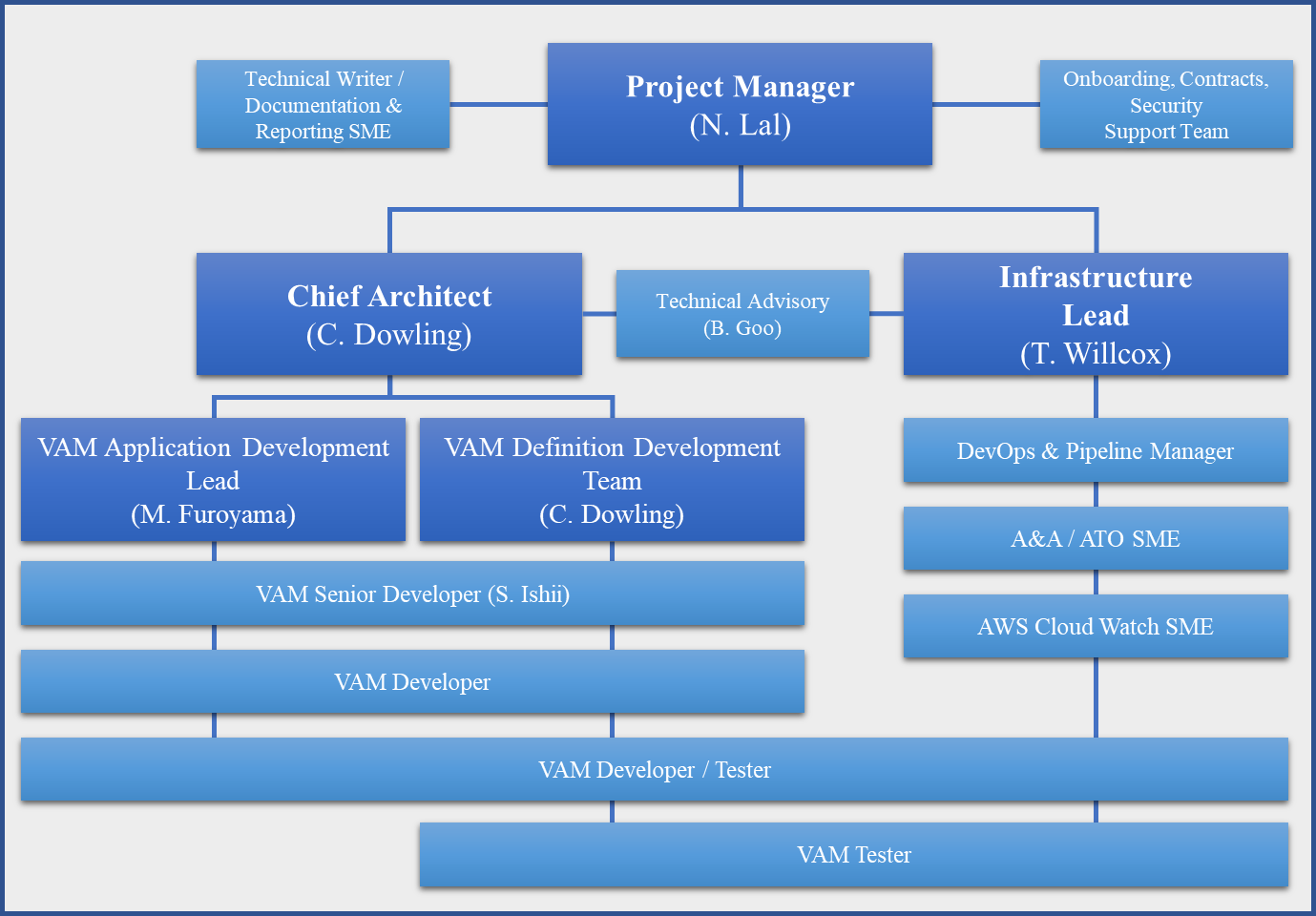
Table 2: Stakeholders

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Office of Information and Technology (OI&T)** | | | | |
| **Team Member** | **VA Email** | **Proxy** | **Phone** | **Responsibility** |
| Dr. Rafael Richards | [Rafael.Richards@va.gov](mailto:Rafael.Richards@va.gov) | Cheryl Owsley | 202-469-1527 | Business Owner |
| Christopher Brown | Christopher.brown1@va.gov | Cheryl Owsley |  | System Owner |
| Cheryl Owsley | [Cheryl.Owsley@va.gov](mailto:Cheryl.Owsley@va.gov) | Dr. Richards |  | VA PM |
| Dana Newcomb | [Dana.Newcomb@va.gov](mailto:Dana.Newcomb@va.gov) | Michael Weckescar | 732-440-9680 | Contracting Officer |
| Michael Weckesser | [Michael.Weckesser@va.gov](mailto:Michael.Weckesser@va.gov) |  | 732-795-1097 | Contract Specialist |
| Robert Goode | [Robert.Goode@va.gov](mailto:Robert.Goode@va.gov) | Tom Spinelli | 202-461-4304 | Contracting Officer’s Representative (COR) |
| Bobbi Begay | Bobbi.Begay@va.gov | Chery Owsley |  | Information Security Officer |
| **AbleVets** | | | | |
| **Team Member** | **VA E-mail Address** | **Proxy** | **Phone** | **Responsibility** |
| Jeff Miller | [Jeffrey.Miller7@va.gov](mailto:Jeffrey.Miller7@va.gov) | Avinay Vaswani | 703-400-6859 | Account Executive, AbleVets |
| Tom Willcox | [Tom.Willcox@ablevets.com](mailto:Tom.Willcox@ablevets.com) | Nilesh Lal | 703-915-7688 | CIO, AbleVets |
| Christy Lentile | [Nancy.Lentile@va.gov](mailto:Nancy.Lentile@va.gov) | Avinay Vaswani |  | Portfolio Director, AbleVets |
| Nilesh Lal | [Nilesh.Lal@va.gov](mailto:Nilesh.Lal@va.gov) | Christy Lentile | 240-476-5359 | PM, AbleVets |
| Conor Dowling | [Conor.Dowling@va.gov](mailto:Conor.Dowling@va.gov) | Mike Furoyama | 310-980-7954 | Software Architect, Caregraf |
| Renton Nip | RNip@hawaiirg.com | Mike Furoyama | 808-927-0999 | Manager, HRG |
| Mike Furoyama | [Michael.Furoyama@va.gov](mailto:Michael.Furoyama@va.gov) | Conor Dowling |  | Sr. Developer, HRG |

# Project Organization

The organizational structure, as illustrated in **Figure 1**, is designed to ensure that appropriate management and technical leadership is provided in all key areas of the effort.

Figure 1: Project VAM Organizational Chart



At a strategic level, the VA PM is responsible for providing the overall programmatic direction to Team AbleVets. The VA PM and COR are the final approval authority for all VAM deliverables. In addition, VA PM is responsible for:

* Monitoring the contract to ensure that obligations are successfully met and maintained by Team AbleVets
* Monitoring Team AbleVets’ performance to ensure that our services meet the required standards, as set out in the contract
* Managing any and all changes permitted under the contract
* Managing changes that are not provided for in the contract

At the operational level, the PM and Chief Architect are responsible for leading the development and delivery of all contractual project deliverables. They are accountable for the program, for ensuring the quality delivery of artifacts, and for supporting the client throughout all contractual activities.

# Testing

Details for VAM testing activities can be found in the *VAM Master Test Plan* (CLIN 0003AA).

The *VAM Master Test Plan* summarizes the testing approach, key objectives, test tools, and test data output for the VAM project. The document introduces:

* Test Strategy: The rules upon which testing will be based, and the process for establishing valid tests to output sound test data. The project’s test strategy will address the scheduling of test events, entry and exit criteria, and test data management.
* Execution Strategy: Details how testing activities will be performed.
* Test Management Plan: Describes the design, execution, and the process for test event issue resolution.

As noted in the Testing and Reporting segment of the VAM *Monthly Progress Report*, an RPC interface test suite has been created for developer-level tests and execution schemes for the following functional segments:

* RPC Monitor
* RPC Mirror
* RPC Definition Models

# Monitoring and Control Mechanisms

The purpose of monitoring and control mechanisms is to provide an understanding of the project’s progress so that appropriate corrective actions can be taken when the project’s performance deviates significantly from the plan.

## Budget Monitoring

The AbleVets Estimate at Completion (EAC) tool (**Figure 2**) is used to define the cost to complete any given level of effort in the Work Breakdown Structure (WBS), and depicts planned financial elements (number/type of project staff, projected number of hours per week/month, labor rate) throughout the duration of the contract. After the contract award, the budget is updated monthly, displaying planned financial information against actuals. The PM reviews the VAM EAC tool (budget) each month to ensure the project stays within allocated funding limits.

Figure 2: EAC Tool Example



## Schedule Monitoring

The VAM project schedule will be monitored weekly to ensure activities are performed on the dates prescribed by the schedule. Performing regular reviews of the schedule allows for the early identification of possible issues before they become problems. Other benefits to monitoring the schedule include better use of resources, the ability to mange unexpected changes, ensuring the project team is focused on tasking, and ensures that related tasks are executed in the correct order. The monitoring of the schedule includes:

* Updating tasks; due dates, dependencies, resources and percentage complete
* Entering additional tasks, as needed
* Ensuring the critical path is not impacted by any changes
* Calculating the amount of slack on the critical path
* Ensuring there is sufficient time to complete high risk tasks
* Validating that project milestones are met

## Risk Monitoring

Monitoring risks involves continuous evaluation of the risks. All team members are responsible for the identification, mitigation, and monitoring of project risks. The PM is responsible for tracking and validating risk mitigation plans and updating the Risk Registry based on input from the project team.

# High-Level Build Schedule

The high-level build schedule can be found within the [GitHub](https://github.com/vistadataproject/RPCDefinitionToolkit/blob/master/README.md) tool.

# Project Success Criteria

The success of the VAM contract is based on meeting contractual requirements, exceeding VA management expectations, and developing positive working relationships with all Stakeholders. Project success criteria includes, but is not limited to:

* Customer satisfaction
* Effective decision making
* Managing change
* Crafting project schedules with realistic and obtainable delivery dates
* Minimal/no scope creep
* Effective coordination with subcontractors
* Effective communication with the integrated project team
* Immediate communication of project issues
* Open discussions surrounding resolution
* Meeting user requirements
* Executing the project within budget
* Meeting project milestones
* Meeting quality criteria
* Producing an easily maintainable product
* Meeting client expectations

# Communication Management Plan

AbleVets will use a comprehensive bi-directional communication approach that strategically engages Stakeholders. Establishing and maintaining formal and informal communication channels with our clients and team is a key to success. AbleVets understands that quality communication includes formal and informal mechanisms, both face-to-face and through electronic media, and will ensure Stakeholder involvement via multiple communications mechanisms for each task.

Intra-project communication is crucial, due to staggered sequencing and interdependencies among project tasks, and potential geographic separation amongst AbleVets and government Stakeholders. AbleVets will conduct weekly status meetings to:

* Review of any strategic or enterprise news impacting project (i.e., VA-wide policies, new direction, etc.)
* Review status of Actions from Last Meeting – go thru each action and convey or solicit status from team
* Review Technical Status – review of key milestones/activities from previous week, and plan for this week at high-level
* Review the Deployment/Infrastructure Status – review of key milestones/activities from previous week, and plan for this week at high-level
* Review Management Processes (GitHub Tools) – Review of key milestones/activities from previous week, and plan for next week
* Discuss contractual or other items warranting discussion
* Review action items captured during status meetings

# Risk Management Plan

Risk is defined as an uncertain event or condition that has a probability of occurring and could have either a positive or negative impact to at least one of the project’s objectives should that risk occur. A risk may have one or more causes and, if it occurs, one or more impacts. All projects assume some element of risk, and it is through risk management where tools and techniques are applied to monitor and track those events that have the potential to impact the outcome of a project.

Risk management focuses on identifying potential problems before they occur. Proper planning for and handling risks help avoid adversely impacting the project’s objectives and goals. The risk management process includes the following four steps:

* Identify Risk: The effort associated with determining whether or not a risk event might affect the project and the documentation of the risk’s characteristics. Team members provide information on suspected event occurrence. The entire project staff is responsible for communicating the likelihood of risks and the associated characteristics of that risk.
* Analyze Risk: The effort associated with evaluating the probability of a risk occurring and the impact to the project and with determining a risk severity ranking.
* Response Planning: The effort associated with developing the mitigation and contingency plans to minimize or eliminate the impact of a risk. Mitigation strategies are developed for risks determined to have an impact on the project. Plans for mitigation are tracked until either the risk exposure has been satisfactorily reduced or the risk averted.
* Monitoring and Control: The effort associated with making decisions regarding initiating appropriate controls and tracking a risk until the risk is no longer a threat. Risk status is tracked and monitored throughout the lifecycle of a project.

These processes are performed on an ongoing, continuous basis throughout the project’s period of performance.

## Identify Risks

The primary purpose of Risk Management is to identify potential impacts early so that they may be mitigated to help ensure project success. Risk management ensures risks are formally addressed at the beginning (Sprint planning) and end (Sprint Review and Retrospective) of each Sprint; risks are part of the meeting agenda. Risks will be identified and documented by the entire team. During the daily scrum meetings only risks that need to be updated or newly identified will be discussed.

For new risks, the Project team will be asked to estimate the probability and the impact. Based on the probability and impact; the risk severity will be determined. High severity risks will be documented and tracked in the Risk Registry.

## Risk Analysis

Risk Analysis encompasses evaluation of probability, impact, severity, and prioritization. The purpose of risk analysis is to bolster the risk definition into becoming decision making information. During this process, risks are analyzed in detail to assess the amount of risk, to identify which ones are most important, and how they relate to each other. Response to minimize the risks will be determined and documented.

### Risk Probability

The probability of the risk event occurring in a selected unit of time (e.g. per day, per two-week Sprint, per month, during the project) is a subjective estimation based on an analysis of the team or Risk Owner. The probability estimate requires knowledge of the activity, experience or historical data. The Risk Probability Matrix is shown in **Table 3**. The distribution of the 20-40-60-80 rule provides the basic five probability categories necessary for quantitative analysis.

Table 3: Risk Probability Matrix

| Risk Probability Rank | Likelihood of Event |
| --- | --- |
| 5 – Almost Certain | > 80% – Risk event expected to occur |
| 4 – Likely | 60-80% – Risk event more likely to occur |
| 3 – Moderate | 40-60% – Risk event may or may not occur |
| 2 – Unlikely | 20-40% – Risk event less likely to occur |
| 1 – Rare | < 20% – Risk event not expected |

### Risk Impact

The impact to the project if a risk occurs is estimated in terms of the criteria that are important the stakeholders. The Risk Impact Matrix assists with rating the impact of each risk relating to safety, financial, schedule, adverse image/publicity and customer service/business interruption. The Risk Impact Matrix (**Table 4**) reflects IT Engineering Support project’s criteria.

Table 4: Risk Impact Matrix

| Risk Impact Rank | Cost or Schedule impact | Scope or Quality |
| --- | --- | --- |
| 5 – Potentially Catastrophic | GREATER THAN 20% | Final contract deliverables fail to meet customer needs. |
| 4 – Major | 10 – 20% | Final contract deliverables content and quality unacceptable to customer. |
| 3 –Moderate | 5 – 10% | Major impact in final contract deliverables content and quality requiring customer approval. |
| 2 – Minor | LESS THAN 5% | Relatively minor impact to contract deliverables content and quality. |
| 1 – Insignificant | No or negligible variance | Very minor impact to contract deliverables content and quality. |

### Risk Severity

Using the Risk Severity Matrix, the risk severity will be calculated by the likelihood and the impact. Risks that fall in the red zone (high risk) will be documented and a response from Program Management will determine if the issue requires a code change. If the risk response requires development work it will be added to the backlog.

Probability and impact information is used to determine risk severity. The Risk Probability Matrix is illustrated in **Table 5**.

Table 5: Risk Severity Matrix

|  |  | Risk Consequence (Severity) | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Insignificant | Minor | Moderate | Major | Severe |
| Risk Consequence (Severity) | Almost Certain | LOW | MEDIUM | HIGH | HIGH | HIGH |
| Likely | LOW | MEDIUM | MEDIUM | HIGH | HIGH |
| Moderate | LOW | LOW | MEDIUM | MEDIUM | HIGH |
| Unlikely | LOW | LOW | LOW | MEDIUM | MEDIUM |
| Rare | LOW | LOW | LOW | LOW | MEDIUM |