<Enter team name here>

Findings and Reporting Information Console (FRIC)
Software Requirements Specification

Version 2.0
9/1/2020

Document Control

Approval

The Guidance Team and the customers shall approve this document.

Document Change Control

Initial Release:	0.1
Current Release:	2.0
Indicator of Last Page in Document:	&
Date of Last Review:	9/1/2020
Date of Next Review:	9/4/2020
Target Date for Next Update:	9/5/2020

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members:
Dr. Salamah
Elsa Tai Ramirez
Ben Robertson

Customers:
Dr. Oscar Perez
Vincent Fonseca
Herandy Denisse Vazquez
Theresa Provencio
Angel E. Avila
Juan Ulloa
John Rivers
Andres Cuevas

Software Team Members:
Team 1
Team 2
Team 3
Team 4
Team 5
Team 6
Team 7
Team 8
Team 9
Team 10
Team 11
Team 12
Team 13

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description

0.1	08/26/2020	Elsa Tai Ramirez	Created a draft document
1.0	9/1/2020	Elsa Tai Ramirez	Added the behavior requirements
2.0	9/1/2020	Vince Fonseca	Reviewed UI

Table of Contents

1. Introduction

1.1. Purpose and Intended Audience

The purpose of the Software Requirements Specification (SRS) is to give the customer a clear and precise description of the functionality of the Findings and Reporting Information Console (FRIC) System. The SRS divides the system requirements into two parts, behavioral and non-behavioral requirements. The behavioral requirements describe the interaction between the system and its environment. Non-behavioral requirements relate to the definition of the attributes of the product as it performs its functions. This includes performance requirements of the product. The intended audience of the SRS is Dr. Oscar Perez, Mr. Vincent Fonseca, Ms. Herandy Vazquez, Ms. Theresa Provencio, Mr. Angel E. Avila, Mr. Juan Ulloa, Mr. John Rivers, Mr. Andres Cuevas, and the Software Engineering teams. This document serves as an agreement between both parties regarding the product to be developed.

1.2. Scope of Product

The Cyber Experimentation & Analysis Division (CEAD) recognizes the complexity and the time it takes to manage task assignments, progress, vulnerability discovery during a cyber engagement and generate custom reports that presents the discovered vulnerabilities and potential issues to CEAD's target audience. They want a system that would aid the management of task, collection of evidence, and report generation during a cyber engagement.

The University of Texas at El Paso (UTEP) and CEAD are collaborating to develop Findings and Reporting Information Console (FRIC) system that will provide the ability to manage task assignment and progress, and facilitate the collection of evidence on existing vulnerabilities, and generation of custom reports.

1.3. Definitions, Acronyms, and Abbreviations

1.3.1. Definitions

The definitions in this section are given in the context of the product being developed. This intention is to assist the user in their understanding of the document.

Table 1: Definition of terms used in the report

TERM	DEFINITION
Actor	A representation in the use case diagram denoting external entities that interact with a system being modeled, e.g., the testbed management system.
Extend Relationship	Denotes insertion of optional behavior of another use case into the primary use case.
Generalization Relationship	Denotes a relationship between a general use case and a specific use case.
Include Relationship	Denotes the inclusion of behavior of another use case into the primary use case.
Use Case	A modeling technique that presents the basic functionality of a system and the actors that interact with each function.
Severity Category Codes	A classification of vulnerabilities used to assess a facility or system security posture from Defense Information Systems Agency (DISA).
Severity Category Codes I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability, or Integrity
Severity Category Codes II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity

Severity Category Codes III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity [2].

1.3.2. Acronyms

This section lists the acronyms used in this document and their associated definitions.

Table 2: Acronyms

TERM	DEFINITION
SRS	Software Requirements Specification
UTEP	The University of Texas at El Paso
CAT	Severity Category Codes
DISA	Defense Information Systems Agency
CEAD	Cyber Experimentation & Analysis Division

1.3.3. Abbreviations

This section provides a list of used abbreviations and their associated definitions.

Table 3: Abbreviations

TERM	DEFINITION
e.g.	For example
i.e.	That is
TBD	To be determined

1.4. Overview

The SRS is divided into three major sections: Introduction (Section 1), General Description (Section 2), and Specific Requirements (Section 3).

Section 1 includes five subsections. Section 1.1 provides the purpose and intended audience of the document. Section 1.2 describes the scope of the product. Section 1.3 provides the definitions, acronyms and abbreviations. Section 1.4 provides the organization of the document. Section 1.5 lists the references used in this document.

Section 2 includes five subsections. Section 2.1 contains a description of the product, its overall structure, and its functionality. Section 2.2 summarizes the main features of the system. Section 2.3 identifies each type of users of the system. This is accomplished through a summary of actors and use-cases. Section 2.4 states existing general constraints. Section 2.5 gives the assumptions and dependencies of the system.

Section 3 includes four major subsections. Section 3.1 contains requirements that are related to the external interface. Section 3.2 contains the functional requirements that are organized in the following categories: same class of user, related real-world objects, stimulus, related features, and limits and default settings. Section 3.3 contains non-behavioral requirements.

1.5. References

[1] O. Perez et al, Requirements Definition Document, Cyber Experimentation & Analysis Division, 2020.

2. General Description

2.1. Product Perspective

Findings and Reporting Information Console (FRIC) is a multi master replication system that facilitates management of task assignments, documentation of discovered vulnerabilities, and generation of custom reports.

2.2. Product Features

Figure 1 presents a level 1 use case diagram that provides an overview of the main functionalities provided by FRIC and the interactions between actors and FRIC. Figure 2 presents the notations used in a use case diagram. The actors, represented by stick figures, are external entities that interact with FRIC. The use case, represented by ovals, elucidates the actors' interactions with FRIC. Figure 3 presents a level 2 use case diagram that provides extensions of the functionalities, in particular the include, extend, and generalization interactions between the actors and the system. The include relationship denotes the inclusion of behavior of another use case into the primary use case. The extend relationship denotes insertion of optional behavior of another use case into the primary use case. The generalization relationship denotes a relationship between a general use case and a specific use case. These components are described next.

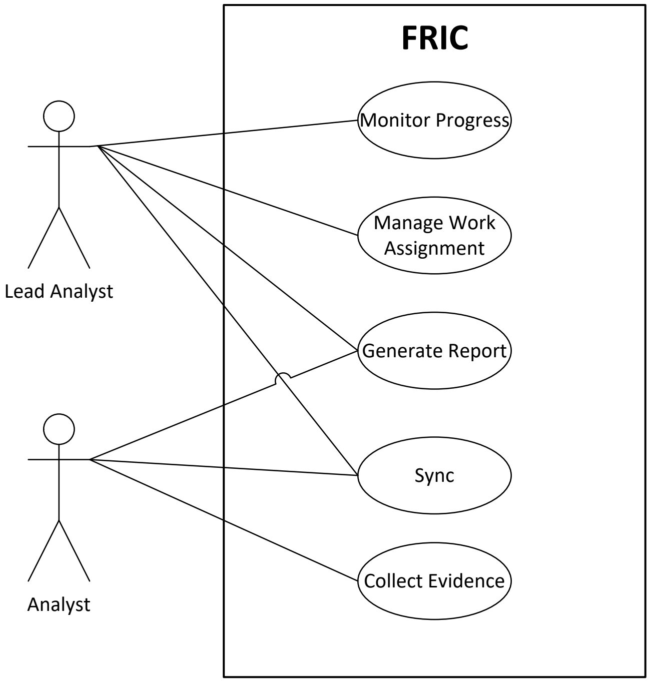


Figure 1: Level 1 Use Case Diagram

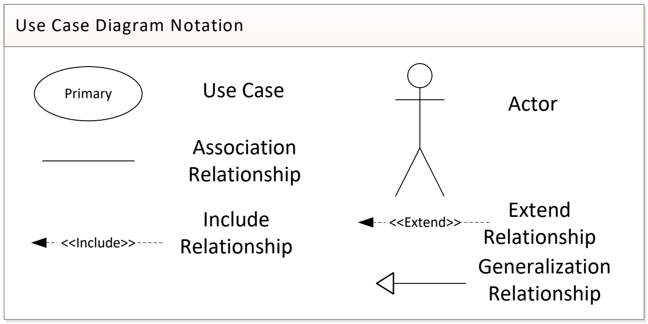


Figure 2: Use Case Diagram Notation

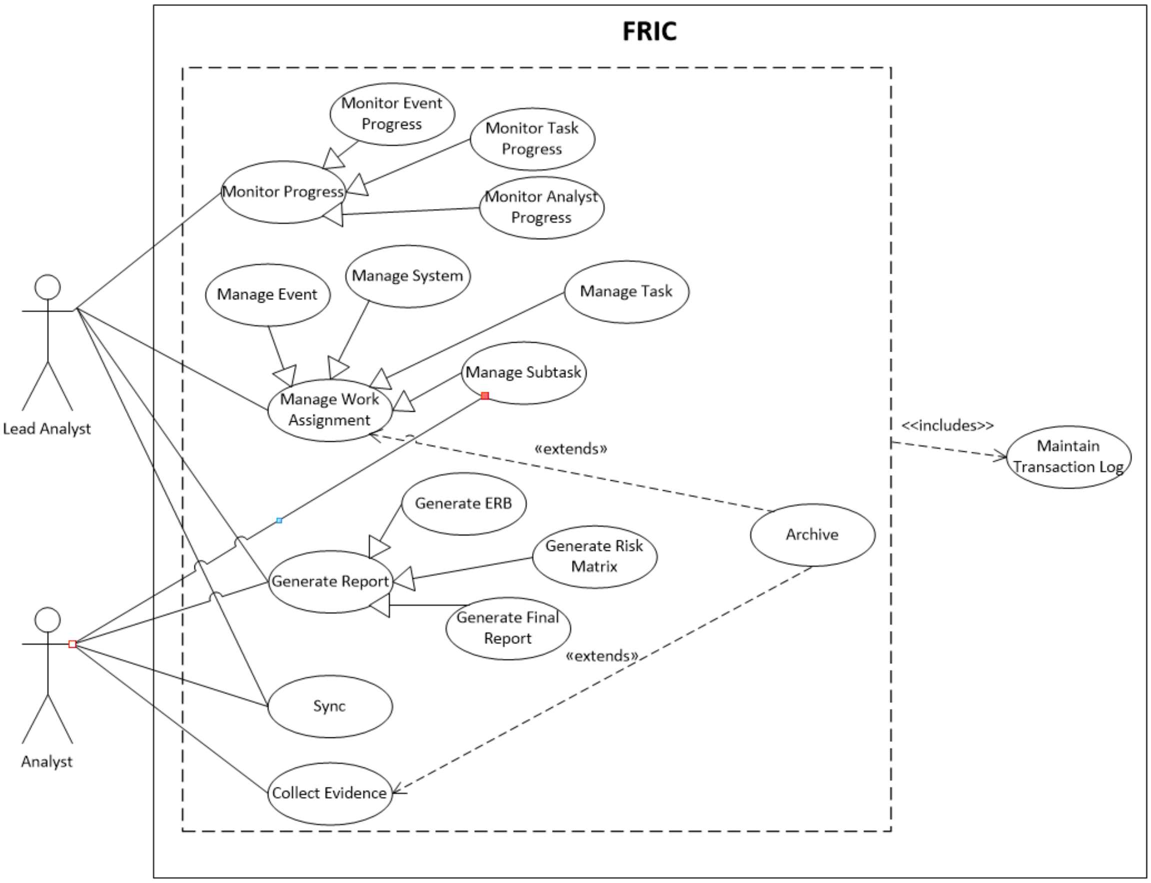


Figure 3: Level 2 Use Case Diagram

2.2.1. Actors Descriptions

FRIC classifies the actors into the following groups:

- Analyst: The principal user of the system.
- Lead Analyst: A user is in charge of managing the cyber engagement.

2.2.2. Use Case Descriptions

FRIC supports the following primary use cases:

- Generate report: Create a customizable report of findings.

- Monitor progress: Allow progress tracking at event, task, or analyst level and generate customizable notifications regarding task status.
- Sync: Send recent changes from user's repository to another user's repository and grab changes from lead's repository into the user's local repository
- Manage work assignment: Manage task and sub-tasks assignments and collaborations, event, and systems.
- Collect Evidence: Document findings and perform risk analysis on findings.

FRIC supports the following secondary use cases:

- Generate ERB: Create a powerpoint that includes information about findings.
- Generate risk assessment: Create an excel that includes information about findings.
- Generate final report: Create a word that includes information about findings.
- Monitor event progress: Track progress at event level.
- Monitor task progress: Track progress at task level.
- Monitor analyst's progress: Track progress by analyst.
- Archive: Store information regarding tasks, sub-tasks, findings, event, and system in an archive.
- Maintain log history: Maintain history of all transactions that take place in the system.
- Manage task: Handle task assignments and collaborations.
- Manage subtask: Handle sub-task assignments and collaborations.
- Manage system: Add systems.
- Manage event: Add a new event and configure the rules of engagement.

2.3. User Characteristics

The users of the system have a variety of computer usage skills and are immersed in the area of cybersecurity and network.

2.4. General Constraints

The general constraints on the development of FRIC are as follows:

- The system will be completed by the end of Fall 2020.
- The system will not be connected to the internet.
- The system will be run on Windows or Linux OS.

2.5. Assumptions and Dependencies

The assumptions and dependencies of FRIC are as follows:

- The system can be accessed as a web application.
- The system will save the data into provided hard drives.

3. Specific Requirements

3.1. External Interface Requirements

This section contains the specification of requirements for interfaces among different components and their external capabilities.

3.1.1. User Interfaces

This section describes the characteristics of each interface of FRIC. The interfaces listed below will be described in the following sections:

- General
- Event Content View
- Analyst Progress Summary Content View
- Systems Content View
- Tasks Content View
- Subtasks Content View
- Findings Content View
- Archive Content View
- Configuration Content View
- Notification Overlay
- Setup Content View

3.1.1.1. General

[SRS 1] For values of each drop-down box, please refer to the requirements in section 3.2.2.

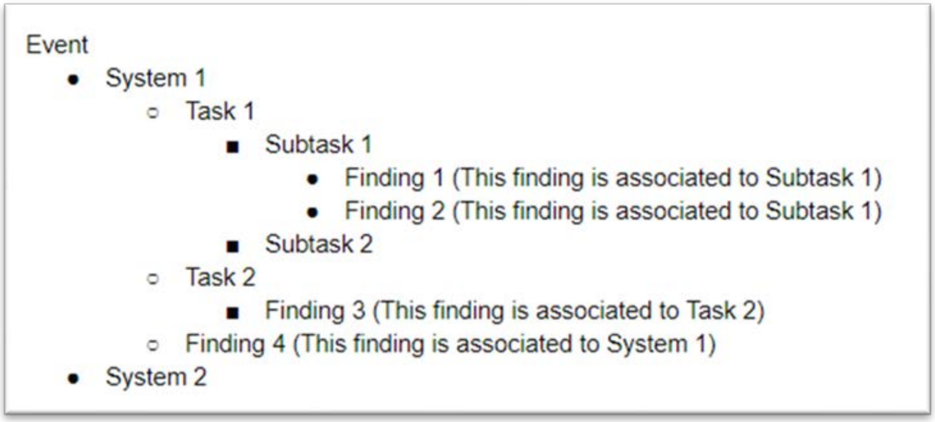
[SRS 2] The system shall have the following layout components:

a. FRIC menu
b. Event tree menu
c. Context view
d. Search box.

[SRS 3] The FRIC menu shall have the following options:

a. Event
b. Systems
c. Tasks
d. Subtasks
e. Findings
f. Archive
g. Configuration
h. Setup
i. Help.

[SRS 4] The event tree menu shall display event, system, task, subtask, and findings using a tree view as shown in Figure 4.



Event

- System 1
  - Task 1
    - Subtask 1
      - Finding 1 (This finding is associated to Subtask 1)
      - Finding 2 (This finding is associated to Subtask 1)
    - Subtask 2
  - Task 2
    - Finding 3 (This finding is associated to Task 2)
  - Finding 4 (This finding is associated to System 1)
- System 2

Figure 4: Event Tree Menu

3.1.1.2. Event Content View

[SRS 5] The event content view shall include the following components:

a. Event overview
b. Event detailed view
c. A button labeled as “Delete”
d. A button labeled as “Save”
e. A button labeled as “Cancel”.

[SRS 6] The event overview shall include the following components:

a. Event overview table
b. An add icon.

[SRS 7] The event overview table shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Event Name”
c. An upward/downward arrow within the column header labeled as “Event name”
d. A column of text fields with the column header labeled as “No. of Systems”
e. An upward/downward arrow within the column header labeled as “No. of Systems”
f. A column of text fields with the column header labeled as “No. of Findings”
g. An upward/downward arrow within the column header labeled as “No of Findings”
h. A column of text fields with the column header labeled as “Progress”
i. An upward/downward arrow within the column header labeled as “Progress”.

[SRS 8] The event detailed view shall include the following components:

a. A help icon
b. Event basic information
c. Event team information.

[SRS 9] The event basic information shall include the following components:

a. A title labeled as “Event Basic Information”
b. A text box labeled as “Event Name”
c. A text box labeled as “Event Description”
d. A dropdown box labeled as “Event Type”

e. A text box labeled as “Event Version”
f. A text box labeled as “Assessment Date”
g. A text box labeled as “Organization Name”
h. A text box labeled as “Security Classification Title Guide”
i. A dropdown box labeled as “Event Classification”
j. A text box labeled as “Declassification Date”
k. A text box labeled as “Customer Name”.

[SRS 10] The event team information shall include the following components:
a. A title labeled as “Event Team Information”
b. A title labeled as “Lead Analysts”
c. An add icon for adding Lead Analyst
d. A column of check boxes
e. A dropdown box with Remove, Edit, and Sync options
f. A column of text fields displaying the analyst initial
g. A title labeled as “Analysts”
h. An add icon for adding Analyst
i. A column of check boxes
j. A dropdown box with Remove, Edit, and Sync options
k. A column of text fields displaying the analyst initial.

[SRS 11] The add/edit overlay shall include the following components:
a. A label labeled as “Add/Edit”
b. A text box labeled as “First Name”
c. A text box labeled as “Last Name”
d. A text box labeled as “Initial”
e. A text box labeled as “Title”.

[SRS 12] The sync overlay shall include the following components:
a. A label labeled as “Sync”
b. A label labeled as “From:”
c. A dropdown box with analyst initials
d. A text box labeled as “IP Address”
e. A column of check boxes
f. A label labeled as “Delete”
g. A column of text fields displaying the analyst initial
h. A column of text box labeled as “IP Address”
i. A button labeled as “Sync”.

3.1.1.3. Analyst Progress Summary Content View

[SRS 13] The analyst progress summary content view shall include the following components:
a. Tasks overview table
b. Subtasks overview table
c. Findings overview table
d. Systems overview table.

3.1.1.4. Systems Content View

[SRS 14] The systems content view shall include the following components:
a. Systems overview
b. System detailed view
c. A button labeled as “Archive”
d. A button labeled as “Save”
e. A button labeled as “Cancel”.

[SRS 15] The systems overview shall include the following components:
a. Systems overview table
b. An add icon.

[SRS 16] The systems overview table shall include the following components:
a. A column of check boxes
b. A column of text fields with the column header labeled as “System”
c. An upward/downward arrow within the column header labeled as “System”
d. A column of text fields with the column header labeled as “No. of Tasks”
e. An upward/downward arrow within the column header labeled as “No. of Tasks”
f. A column of text fields with the column header labeled as “No. of Findings”
g. An upward/downward arrow within the column header labeled as “No of Findings”
h. A column of text fields with the column header labeled as “Progress”
i. An upward/downward arrow within the column header labeled as “Progress”.

[SRS 17] The systems detailed view shall include the following components:
a. A help icon
b. System information
c. System categorization.

[SRS 18] The system information shall include the following components:
a. A title labeled as “System Information”
b. A text box labeled as “System Name”
c. A text box labeled as “System Description”
d. A text box labeled as “System Location”
e. A text box labeled as “System Router”
f. A text box labeled as “System Switch”
g. A text box labeled as “System Room”
h. A text box labeled as “Test Plan”.

[SRS 19] The system categorization shall include the following components:
a. A dropdown box labeled as “Confidentiality”
b. A dropdown box labeled as “Integrity”
c. A dropdown box labeled as “Availability”.

3.1.1.5. Tasks Content View

[SRS 20] The tasks content view shall include the following components:
a. Tasks overview
b. Task detailed view
c. A button labeled as “Archive”
d. A button labeled as “Demote”
e. A button labeled as “Save”
f. A button labeled as “Cancel”.

[SRS 21] The tasks overview shall include the following components:
a. Tasks overview table
b. An add icon.

[SRS 22] The tasks overview table shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Title”
c. An upward/downward arrow within the column header labeled as “Title”
d. A column of text fields with the column header labeled as “System”
e. An upward/downward arrow within the column header labeled as “System”
f. A column of text fields with the column header labeled as “Analyst”
g. An upward/downward arrow within the column header labeled as “Analyst”
h. A column of text fields with the column header labeled as “Priority”
i. An upward/downward arrow within the column header labeled as “Priority”
j. A column of text fields with the column header labeled as “Progress”
k. An upward/downward arrow within the column header labeled as “Progress”
l. A column of text fields with the column header labeled as “No. of Subtasks”
m. An upward/downward arrow within the column header labeled as “No. of Subtasks”
n. A column of text fields with the column header labeled as “No. of Findings”
o. An upward/downward arrow within the column header labeled as “No. of Findings”
p. A column of text fields with the column header labeled as “Due Date”
q. An upward/downward arrow within the column header labeled as “Due Date”.

[SRS 23] The task detailed view shall include the following components:

a. A help icon
b. A title labeled as “Task Detailed View”
c. A text box labeled as “Title”
d. A text box labeled as “Description”
e. A dropdown box labeled as “System”
f. A dropdown box labeled as “Priority”
g. A dropdown box labeled as “Progress”
h. A date picker labeled as “Due Date”
i. A multiple selection dropdown box labeled as “Analyst(s)”
j. A multiple selection dropdown box labeled as “Collaborator(s)”
k. A multiple selection dropdown box labeled as “Related Task(s)”
l. A file selection box labeled as “Attachments”.

3.1.1.6. Subtasks Page

[SRS 24] The subtasks content view shall include the following components:

a. Subtasks overview
b. Subtask detailed view
c. A button labeled as “Archive”
d. A button labeled as “Promote”
e. A button labeled as “Save”
f. A button labeled as “Cancel”.

[SRS 25] The subtasks overview shall include the following components:

a. Subtasks overview table
b. An add icon.

[SRS 26] The subtasks overview table shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “Title”
c. An upward/downward arrow within the column header labeled as “Title”
d. A column of text fields with the column header labeled as “Task”
e. An upward/downward arrow within the column header labeled as “Task”
f. A column of text fields with the column header labeled as “Analyst”
g. An upward/downward arrow within the column header labeled as “Analyst”
h. A column of text fields with the column header labeled as “Progress”
i. An upward/downward arrow within the column header labeled as “Progress”
j. A column of text fields with the column header labeled as “No. of Findings”
k. An upward/downward arrow within the column header labeled as “No. of Findings”
l. A column of text fields with the column header labeled as “Due Date”
m. An upward/downward arrow within the column header labeled as “Due Date”.

[SRS 27] The subtask detailed view shall include the following components:

a. A help icon
b. A title labeled as “Subtask Detailed View”
c. A text box labeled as “Title”
d. A text box labeled as “Description”
e. A dropdown box labeled as “Progress”
f. A date picker labeled as “Due Date”
g. A multiple selection dropdown box labeled as “Analyst(s)”
h. A multiple selection dropdown box labeled as “Collaborator(s)”
i. A multiple selection dropdown box labeled as “Task(s)”
j. A multiple selection dropdown box labeled as “Subtask(s)”
k. A file selection box labeled as “Attachments”.

3.1.1.7. Findings Content View

[SRS 28] The findings content view shall include the following components:

a. Findings overview
b. Finding detailed view
c. A button labeled as “Delete”
d. A button labeled as “Save”
e. A button labeled as “Cancel”.

[SRS 29] The findings overview shall include the following components:

a. Findings overview table
b. An add icon
c. A button labeled as “ERB Report”
d. A button labeled as “Risk Matrix”
e. A button labeled as “Final Report”.

[SRS 30] The findings overview table shall include the following components:

a. A column of check boxes
b. A column of text fields with the column header labeled as “ID”
c. A column of text fields with the column header labeled as “Title”
d. An upward/downward arrow within the column header labeled as “Title”
e. A column of text fields with the column header labeled as “System”
f. An upward/downward arrow within the column header labeled as “System”
g. A column of text fields with the column header labeled as “Task”
h. An upward/downward arrow within the column header labeled as “Task”
i. A column of text fields with the column header labeled as “Subtask”
j. An upward/downward arrow within the column header labeled as “Subtask”
k. A column of text fields with the column header labeled as “Analyst”
l. An upward/downward arrow within the column header labeled as “Analyst”
m. A column of text fields with the column header labeled as “Status”
n. An upward/downward arrow within the column header labeled as “Status”
o. A column of text fields with the column header labeled as “Classification”
p. An upward/downward arrow within the column header labeled as “Classification”
q. A column of text fields with the column header labeled as “Type”
r. An upward/downward arrow within the column header labeled as “Type”
s. A column of text fields with the column header labeled as “Risk”
t. An upward/downward arrow within the column header labeled as “Risk”.

[SRS 31] The finding detailed view shall include the following components:

a. Help icon
b. Finding information
c. Finding impact
d. Analyst information
e. Mitigation
f. Threat
g. Countermeasure
h. Impact
i. Severity
j. Risk
k. Finding system level impact.

[SRS 32] The finding information shall include the following components:

a. A help icon
b. A title labeled as “Finding Information”
c. A text field labeled as “ID”
d. A text box labeled as “Host Name”
e. A text box labeled as “IP Port”
f. A text box labeled as “Description”
g. A text box labeled as “Long Description”
h. A dropdown box labeled as “Status”
i. A dropdown box labeled as “Type”
j. A dropdown box labeled as “Classification”
k. A file selection box labeled as “Evidence”.
l. A dropdown box labeled as “System”
m. A label labeled as “OR”
n. A dropdown box labeled as “Task”
o. A label labeled as “OR”
p. A dropdown box labeled as “Subtask”
q. A multiple selection dropdown box labeled as “Related Finding(s)”.

[SRS 33] The finding impact shall include the following components:

a. A help icon
b. A title labeled as “Finding Impact”
c. A dropdown box labeled as “Confidentiality”
d. A dropdown box labeled as “Integrity”
e. A dropdown box labeled as “Availability”.

[SRS 34] The analyst information shall include the following components:

a. A help icon
b. A title labeled as “Analyst Information”
c. A multiple selection dropdown box labeled as “Analyst”
d. A multiple selection dropdown box labeled as “Collaborator”
e. A dropdown box labeled as “Posture”

[SRS 35] The mitigation shall include the following components:

a. A help icon
b. A title labeled as “Mitigation”
c. A text box labeled as “Brief Description”
d. A text box labeled as “Long Description”.

[SRS 36] The threat relevance shall include the following components:

a. A help icon
b. A title labeled as “Threat Relevance”
c. A dropdown box labeled as “relevance”.

[SRS 37] The countermeasure shall include the following components:

a. A help icon
b. A title labeled as “Countermeasure”
c. A dropdown box labeled as “Effectiveness Rating”.

[SRS 38] The impact shall include the following components:

a. A help icon
b. A title labeled as “Impact”
c. A text box labeled as “Impact Description”
d. A dropdown box labeled as “Impact Level”.

[SRS 39] The severity shall include the following components:

a. A help icon
b. A title labeled as “Severity”
c. A text field labeled as “Severity Category Score”
d. A text field labeled as “Vulnerability Severity”
e. A text field labeled as “Quantitative Vulnerability Severity”.

[SRS 40] The risk shall include the following components:

a. A help icon
b. A title labeled as “Risk”
c. A text field labeled as “Risk”
d. A text field labeled as “Likelihood”.

[SRS 41] The finding system level impact shall include the following components:

a. A help icon
b. A title labeled as “Finding System Level Impact”
c. A text field labeled as “Confidentiality Finding Impact on System”
d. A text field labeled as “Integrity Finding Impact on System”
e. A text field labeled as “Availability Finding Impact on System”
f. A text field labeled as “Impact Score”.

3.1.1.8. Archive Content View

[SRS 42] The archive content view shall include the following components:

a. Archived tasks
b. Archived subtasks
c. Archived findings
d. Archived systems.

[SRS 43] The archive tasks shall include the following components:

a. A title labeled as “Archived Tasks”
b. Tasks Overview Table
c. A button labeled as “Restore”.

[SRS 44] The archive subtasks shall include the following components:

a. A title labeled as “Archived Subtasks”
b. Subtasks Overview Table
c. A button labeled as “Restore”.

[SRS 45] The archive findings shall include the following components:

a. A title labeled as “Archived Findings”
b. Findings Overview Table
c. A button labeled as “Restore”.

[SRS 46] The archive systems shall include the following components:

a. A title labeled as “Archived Systems”
b. Systems Overview Table
c. A button labeled as “Restore”.

3.1.1.9. Notification Overlay

[SRS 47] The notification overlay shall include the following components:

a. A label labeled as “Notification”
b. A column of text fields with the column header labeled as “Task Title”
c. A column of text fields with the column header labeled as “Task Due Date”
d. A column of text fields with the column header labeled as “Subtask Title”
e. A column of text fields with the column header labeled as “Subtask Due Date”
f. A button labeled as “Ok”.

3.1.1.10. Setup Content View

[SRS 48] The initial view shall have the following components:

a. A label labeled as “Finding and Reporting Information Console (FRIC)”
b. A text field labeled as “There is no existing event in your local system”
c. A text field labeled as “Please enter your initial:”
d. A label labeled as “Please select an option:”
e. A selection box labeled as “Create a new event (any existing event will be archived)”.
f. A selection box and text field labeled as “First time sync with lead analyst. Please enter the lead analyst’s IP”
g. A button labeled as “Submit”.

h. A button labeled as “Cancel”.

3.1.1.11. Configuration Content View

[SRS 49] The configuration content view shall have the following components (Please see the related real object section for the rows and columns for each table):

a. A finding type table
b. A posture table
c. A threat level table
d. An impact level table
e. A finding classification table
f. A countermeasure table
g. An event classification table
h. A level table
i. An event type table
j. A finding impact level table
k. A severity category code table
l. A progress table
m. An event rules table
n. A report template table
o. A notification table.

3.1.2. Hardware Interfaces

There are no hardware interface requirements specified at this time.

3.1.3. Software Interfaces

There are no software interface requirements specified at this time.

3.1.4. Communications Interfaces

There are no communication interface requirements specified at this time.

3.2. Behavioral Requirements

This section describes the behavioral requirements of the system.

3.2.1. Same Class of User

This section describes requirements associated with a particular class of user.

[SRS 50] The system shall have the following classes of users:

a. Lead
b. Analyst
c. Collaborator.

[SRS 51] The system shall have four type of access privileges:

a. Write access
b. Read access
c. Append access
d. Associate access.

[SRS 52] Lead shall have read and write access to the following:

a. Task
b. Subtask
c. Findings
d. Event

e. System.

[SRS 53] Role assignment shall propagate down from task to subtask by default.

[SRS 54] The system shall allow users to access privileges at the following access levels as defined in Table 4:

a. Lead access level
b. Analyst access level
c. Collaborator access level (Please see the stimulus section).

Table 4: Privileges by Access Level

Privileges\Classes of Users	Lead Analyst	Analyst
Create event	Yes.	No.
Create system	Yes.	No.
Generate report	Yes	Yes
Create task	Yes.	No.
Create subtask	Yes.	Analyst shall have the ability to create subtask(s) under a task that has been assigned to the analyst.
Assign task	Yes.	No.
Assign subtask	Yes.	No.
Sign up for task	N/A	Analyst shall have the ability to sign up for task only if the lead has allowed analyst to sign up for task.
Add collaborator to a task	Yes	Analyst shall have the ability to add collaborator to a task only if the lead has allowed analyst to sign up for task and the task has been assigned to the analyst. If the lead has opted to assign tasks, then only the lead shall have the ability to add collaborators.
Add collaborator to a subtask	Yes. The collaborator’s initial shall be propagated up to the parent of the subtask.	Analyst shall have the ability to add collaborator to a subtask only if the analyst has write-access to the subtask. The collaborator’s initial shall be propagated up to the parent of the subtask.
Add collaborator to a finding	Yes. The collaborator’s initial shall be propagated up to the parent subtask and task.	Analyst shall have the ability to add collaborator to a finding only if the analyst has write-access to the finding. The collaborator’s initial shall be propagated up to the parent subtask and task.
Associate finding (original finding) to another finding (associated finding)	Yes. Lead shall have the ability to establish association between any findings. If the associated finding has a different initial compared to the original finding, then the collaborator’s initial shall be propagated up to the parent subtask and task of the original finding.	Analyst shall have the ability to associate finding to another finding only if the analyst has write-access or append-access to the finding. If the associated finding has a different initial compared to the original finding, then the collaborator’s initial shall be propagated up to the parent subtask and task of the original finding.

Associate task to another task	Yes	Analyst shall have the ability to associate task to another task only if the analyst is assigned to both tasks.
Associate subtask to another task	Yes	Analyst shall have the ability to associate subtask to another task only to task that the analyst is assigned to.
Associate subtask to another subtask	Yes	Analyst shall have the ability to associate subtask to another task only if the analyst has write-access to the subtask.

3.2.2. Related Real-world Objects

This section describes related real-world object requirements of the system.

3.2.2.1. Event

[SRS 55] The system shall have one active event.

[SRS 56] The system shall store the attributes as defined in Table 5 for an event.

Table 5: Event

Attribute	Data Type	Values and Constraints	Description
Event Name	String	Required; Editable	Name of the cyber engagement
Event Description	String	Editable	Description of the cyber engagement
Event Type	Enumeration	Required; {Cooperative Vulnerability Penetration Assessment (CVPA) Cooperative Vulnerability Investigation (CVI) Verification of Fixes (VOF)}; Editable	Type of cyber engagement
Event Version	Number	Required; Editable	Number of times this cyber engagement is conducted
Assessment Date	Date	Required; Editable	Date of the assessment
Organization Name	String	Required; Editable	Name of the organization that performed the cyber engagement
Security Classification Title Guide	String	Required; Editable	Name of the instruction guide used to set out the classification of a cyber engagement
Event Classification	Enumeration	Required; {Top secret, Secret, Confidential, Classified, Unclassified}	Security classification of a cyber engagement
Declassification Date	Date	Required; Editable	Date of declassification
Customer Name	String	Required; Editable	Name of the customer who requested a cyber engagement
Archive Status	Boolean	Required; Editable; {Y = archived, N = active};	State of a cyber engagement

		There shall only be one active event in the local hard drive.	
Event Team	List	Required; Editable	Team of analysts who participate in a cyber engagement

3.2.2.2. Analyst

[SRS 57] The system shall store the attributes as defined in Table 6 for an analyst.

Table 6: Analyst

Attribute	**Data Type**	**Values and Constraints**	**Description**
First Name	String	Required; Editable	First name of an analyst
Last Name	String	Required; Editable	Last name of an analyst
Initial	String	Required; Editable; Unique	Unique initial to represent an analyst in a cyber engagement
Title	List	Required; Editable	Official title(s) of an analyst
Role	Enumeration	Required; Editable; {Lead, Analyst, Collaborator}	Role of an analyst in a cyber engagement

3.2.2.3. System

[SRS 58] The system shall store the attributes as defined in Table 7 for a system.

Table 7: System

Attribute	**Data Type**	**Values and Constraints**	**Description**
System Name	String	Required; Editable	Name of a system
System Description	String	Editable	Description of a system
System Location	List	Required; Editable	List of locations where a system is physically located
System Router	List	Required; Editable	List of routers that are accessed
System Switch	List	Required; Editable	List of switches that are accessed
System Room	List	Required; Editable	List of rooms that are accessed
Test Plan	String	Required; Editable	Name of the test plan
Archive Status	Boolean	Required; Editable; {Y = archived, N = active}	State of a system

[SRS 59] The system shall store the attributes as defined in Table 8 for a system categorization.

Table 8: System Categorization

Attribute	**Data Type**	**Values and Constraints**	**Description**
Confidentiality	Enumeration	Required; {Low, Medium, High, Information}	Confidentiality level of a system
Integrity	Enumeration	Required; {Low, Medium, High, Information}	Integrity level of a system

Availability	Enumeration	Required; {Low, Medium, High, Information}	Availability level of a system

[SRS 60] Each system shall have one set of system categorization.

[SRS 61] Each system shall be associated to one active event.

3.2.2.4. Task

[SRS 62] The system shall store the attributes as defined in Table 9 for a task.

Table 9: Task

Attribute	Data Type	Values and Constraints	Description
Task Title	String	Required; Editable	Name of a task
Task Description	String	Required; Editable	Description of a task
Task Priority	Enumeration	Required; Editable; {Low, Medium, and High}	Priority status of a task
Task Progress	Enumeration	Required; {Not started, assigned, transferred, in progress, complete, and not applicable}; Editable if the task has no subtask. Derived: If a task has at least one subtask, the system shall calculate the progress of a task from the progresses of all its' subtasks.	Progress of a task
Task Due Date	Date	Required; If a task has at least one subtask, the due date of the task shall be greater than the due date of the latest due date of all the subtasks.	Due date of a task
Attachment	File	Optional; Editable	Supplementary information regarding a task
Association to Task	List	Optional; The original task and the associated task shall belong to the same system.	Relationship of a task to another task
Analyst Assignment	List	Editable	Analysts who are assigned to the task
Collaborator Assignment	List	Editable	Collaborators who are assigned to the task
Archive Status	Boolean	Required; Editable; {Y = archived, N = active}	State of a task

[SRS 63] Each task shall be associated to one active system.

3.2.2.5. Subtask

[SRS 64] The system shall store the attributes as defined in Table 10 for a subtask.

Table 10: Subtask

Attribute	Data Type	Values and Constraints	Description
Subtask Title	String	Required; Editable; Appendable	Title of a subtask
Subtask Description	String	Required; Editable; Appendable	Description of a subtask
Subtask Progress	Enumeration	Required; Editable; {Not started, assigned, transferred, in progress, complete, and not applicable}	Progress of a subtask
Subtask Due Date	Date	Required; Editable; The subtask due date shall be less than the task due date.	Due date of a subtask
Attachment	File	Optional; Editable; Appendable	Supplementary information regarding a task
Association to Subtask	List	Optional; The original subtask and the associated subtask shall have the same parent task.	Relationship of a subtask to another subtask
Analyst Assignment	List	Editable	Analysts who are assigned to the subtask
Collaborator Assignment	List	Editable	Collaborators who are assigned to the subtask
Archive Status	Boolean	Required; Editable; {Y = archived, N = active}	State of a subtask

[SRS 65] A subtask shall have one parent task.

3.2.2.6. Finding

[SRS 66] The system shall store the attributes as defined in Table 11 for a finding.

Table 11: Finding Information

Attribute	Data Type	Values and Constraints	Description
Finding ID	Number	System generated	Unique identifier of a vulnerability/potential issue
Host Name	String	Required; Editable	Host name where the vulnerability/potential issue resides
IP Port	String	Required; Editable	IP port where the vulnerability/ potential issue resides
Finding Description	String	Required; Editable; Appendable	Short description of a vulnerability/ potential issue
Finding Long Description	String	Optional; Editable; Appendable	Long description of a vulnerability/ potential issue
Finding Status	Enumeration	Required; Editable; {Open, Closed}	Status that describes whether the vulnerability

			has been patched by the customer
Finding Type	Enumeration	Required; Editable; {Credentials Complexity, Manufacturer Default Creds, Lack of Authentication, Plain Text Protocols, Plain Text Web Login, Encryption, Authentication Bypass, Port Security, Access Control, Least Privilege, Privilege Escalation, Missing Patches, Physical Security, Information Disclosure}	Type of vulnerability/ potential issue
Finding Classification	Enumeration	Required; Editable; {Vulnerability, Information}	Classification that determines if the discovery is a vulnerability or potential issue
Association to Finding	List	Optional; The original finding and the associated finding shall belong to the same system.	Relationship of a finding to another finding
Evidence	File	Required; Editable; Appendable	Evidence that proves the existence of vulnerability
Archive Status	Boolean	Required; Editable; {Y = archived, N = active}	State of a vulnerability or potential issue

[SRS 67] Each finding shall have one association to one of the following:

a. System
b. Task
c. Subtask.

[SRS 68] The system shall store the attributes as defined in Table 12 for a finding impact.

Table 12: Finding Impact

Attribute	**Data Type**	**Values and Constraints**	**Description**
Confidentiality	Enumeration	Required; {Low, Medium, High, Information}	Confidentiality level of a finding
Integrity	Enumeration	Required; {Low, Medium, High, Information}	Integrity level of a finding
Availability	Enumeration	Required; {Low, Medium, High, Information}	Availability level of a finding

[SRS 69] Each finding shall have one set of finding impact.

[SRS 70] The system shall store the attributes as defined in Table 13 for analysts who work on a finding.

Table 13: Analyst Information

Attribute	**Data Type**	**Values and Constraints**	**Description**
Analyst Assignment	List	Required; Editable	Analysts who create and work on the finding
Collaborator Assignment	List	Optional; Editable	Collaborators who are assigned to the finding
Posture	Enumeration	Required; Editable; {Insider Insider-nearsider Outsider Nearsider Nearsider-outsider}	Security posture an analyst plays when completing a task/subtask

[SRS 71] The system shall store the attributes as defined in Table 14 for a mitigation.

Table 14: Mitigation

Attribute	**Data Type**	**Values and Constraints**	**Description**
Brief Description	String	Required; Editable; Appendable	Brief description of a mitigation for a vulnerability/potential issue
Long Description	String	Required; Editable; Appendable	Detailed description of a mitigation for a vulnerability/potential issue

[SRS 72] Each finding shall have at least one mitigation.

[SRS 73] The system shall store the attributes as defined in Table 15 for a threat relevance.

Table 15: Threat Relevance

Attribute	**Data Type**	**Values and Constraints**	**Description**
Relevance	Enumeration	Required; Editable; {Confirmed, Expected, Anticipated, Predicted Possible}	Threat relevance

[SRS 74] Each finding shall have one threat relevance.

[SRS 75] The system shall store the attributes as defined in Table 16 for a countermeasure.

Table 16: Countermeasure

Attribute	**Data Type**	**Values and Constraints**	**Description**
Effectiveness Rating	Enumeration	Required; Editable; {Very high (10), High (7-9), Moderate (4-6), Low (1-3) Very low (0)} (See Table 17)	Mechanism the system has in place to prevent the found vulnerability from being exploited

Table 17: Countermeasure Value

Qualitative Value	**Semi-Quantitative Value**	**Description**
Very High	10	Countermeasure not implemented
High	7-9	Countermeasure is implemented but MINIMALLY effective
Moderate	4-6	Countermeasure is implemented but MODERATELY effective
Low	1--3	Countermeasure is implemented HIGHLY effective but can be improved.
Very Low	0	Countermeasure implemented is effective

[SRS 76] Each finding shall have one countermeasure.

[SRS 77] The system shall store the attributes as defined in Table 18 for an impact.

Table 18: Impact

Attribute	**Data Type**	**Values and Constraints**	**Description**
Impact Description	String	Required; Editable; Appendable	Description of an impact
Impact Level	Enumeration	Required; Editable; {VH, H, M, L, VL, Information}	Impact Level

[SRS 78] Each finding shall have one impact.

[SRS 79] The system shall store the attributes as defined in Table 19 for severity.

Table 19: Severity

Attribute	**Data Type**	**Values and Constraints**	**Description**
Severity Category Code	Enumeration	Required; Editable; {I, II, III} (See Table 20)	A classification of vulnerabilities used to assess a facility or system security posture from Defense Information Systems Agency
Severity Category Score	Number	Derived; The system shall return the following: 10 if the severity category code is I; 7 if the severity category code is II; 4 if the severity category code is III. (See Table 21)	Calculated severity category score
Vulnerability Severity	Number	Derived; The system shall calculate the vulnerability severity by multiplying the severity category score, impact score, countermeasure and divide the total by 10.	Vulnerability Metric
Quantitative Vulnerability Severity	String	Derived; The system shall return the following: Very High if 95 <= Vulnerability Severity <= 100; High if 80 <= Vulnerability Severity	Quantitative Vulnerability Metric

		<= 95; Moderate if 20 <= Vulnerability Severity <= 80; Low if 5 <= Vulnerability Severity <= 20; Very low if 0 <= Vulnerability Severity <= 5; (See Table 22)	

Table 20: CAT Codes

CAT Code	DISA Severity Code Guideline
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in the loss of Confidentiality, Integrity, or Availability
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Integrity or Availability
CAT III	Any vulnerability, the existence of which **degrades a measure** to protect against loss of Confidentiality, Integrity or Availability

Table 21: CAT Score Conversion Table

Qualitative Value	Semi-Quantitative Value
CAT I	10
CAT II	7
CAT III	4

Table 22: Assessment Scale

Qualitative Values	Semi-Quantitative Values
Very High	$95 \leq V_S \leq 100$
High	$80 \leq V_S < 95$
Moderate	$20 \leq V_S < 80$
Low	$5 \leq V_S < 20$
Very Low	$0 \leq V_S < 5$

[SRS 80] Each finding shall have one set of severity values.

[SRS 81] The system shall store the attributes as defined in Table 23 for risk.

Table 23: Risk

Attribute	Data Type	Values and Constraints	Description
Risk	String	Derived; The system shall return the following: If impact score = 0, risk is Info. Otherwise, if impact score != 0, determine risk using likelihood and impact level (See Table 24)	Risk level

Likelihood	String	Derived; The system shall return the following: If impact score = 0, likelihood is Info. Otherwise, if impact score != 0 and determine the likelihood using relevance of threat and quantitative vulnerability severity (See Table 25)	Likelihood Level

Table 24: Risk Table

Assessed Risk							
Likelihood	*Impact$_{Tier3}$*						
		VL	**L**	**M**	**H**	**VH**	**INFO**
		2	**3**	**4**	**5**	**6**	**INFO**
	VH	VL	L	M	H	VH	INFO
	H	VL	L	M	H	VH	INFO
	M	VL	L	M	M	H	INFO
	L	VL	L	L	L	M	INFO
	VL	VL	VL	L	L	L	INFO
	INFO	INFO	INFO	INFO	INFO	INFO	Info

Table 25: Likelihood Table

Likelihood							
Relevance of Threat	*Vulnerability Severity*						
		VL	**L**	**M**	**H**	**VH**	**INFO**
		2	**3**	**4**	**5**	**6**	**INFO**
	Confirmed	VL	L	M	H	VH	INFO
	Expected	VL	L	M	H	VH	INFO
	Anticipated	VL	L	M	M	H	INFO
	Predicted	VL	L	L	L	M	INFO
	Possible	VL	VL	L	L	L	INFO

[SRS 82] The system shall store the attributes as defined in Table 26 for a finding system level impact.

Table 26: Finding System Level Impact

Attribute	**Data Type**	**Values and Constraints**	**Description**
ConfidentialityFindingImpactOnSystem	Enumeration	Return Value: {Low, Medium, High, X}; Derived: The system shall do the following: if findingimpact.confidentiality = Y, then return system.confidentiality.	Confidentiality level of a finding on system
IntegrityFindingImpactOnSystem	Enumeration	Return Value: {Low, Medium, High, X}; Derived:The system shall do the following: if findingimpact.integrity = Y, then return system.integrity.	Integrity level of a finding on system
AvailabilityFindingImpactOnSystem	Enumeration	Return Value: {Low, Medium, High, X}; Derived:The system shall do the following:	Availability level of a

		if findingimpact.availability = Y, then return system.availability.	finding on system
Impact Score	Number	Derived: The system shall compare ConfidentialityFindingImpactOnSystem(), IntegrityFindingImpactOnSystem(), AvailabilityImpactOnSystem() to Impact Score Table to get the impact score. (See Table 27)	Impact score of a finding

Table 27: Impact Conversion Table

Number of Finding System Level Impacted (n)	Finding System Level (High, Moderate, Low)	Semi-Quantitative Value	Description
3	HHH	10	Three security objectives are impacted and all three are ranked High
2	HHx	9	Two security objectives are impacted and both objectives are ranked High
1	Hxx	8	One security objective is impacted and the objective is ranked High
3	MMM	7	Three security objectives are impacted and all three are ranked Moderate
2	MMx	6	Two security objectives are impacted and both objectives are ranked Moderate
1	Mxx	5	One security objective is impacted and the objective is ranked Moderate
3	LLL	4	Three security objectives are impacted and all three are ranked Low
2	LLx	3	Two security objectives are impacted and both objectives are ranked Low
1	Lxx	2	One security objective is impacted and the objective is ranked Low

[SRS 83] Each finding shall have one set of finding system level impact.

3.2.2.7. Report

[SRS 84] The risk matrix report shall include the attributes as defined in Table 28.

Table 28: Risk Matrix

Attribute	Data Type	Values and Constraints	Description
Finding	List	Required	List of selected finding from the cyber engagement

System Categorization	List	Required	System categorization of the finding
Event Name	String	Required	Name of the cyber engagement
Event Type	String	Required	Type of the cyber engagement

[SRS 85] The risk matrix report shall be in excel format.

[SRS 86] The emergent result brief report shall include the attributes as defined in Table 29.

Table 29: ERB Report

Attribute	Data Type	Values and Constraints	Description
Lead Analyst Name	String	Required	Name of lead analyst
Title	String	Required	Title of lead analyst
Event Name	String	Required	Name of the cyber engagement
Event Type	String	Required	Type of the cyber engagement
Summary Table	List	Required; Summary table includes finding description, system name, impact, and risk.	Summary table that displays finding description, system name, impact, and risk.
Finding	List	Required	List of selected finding from the cyber engagement

[SRS 87] The emergent result brief report shall be in powerpoint format.

[SRS 88] The final technical result shall include the attributes as defined in Table 30.

Table 30: Final Technical Report

Attribute	Data Type	Values and Constraints	Description
Analyst Name	List	Required	Name of analyst who participated in the cyber engagement
Summary Table	List	Required; Summary table includes finding description, likelihood, impact, and risk.	Summary table that displays finding description, likelihood, impact, and risk.
Finding	List	Required	List of selected finding from the cyber engagement

[SRS 89] The emergent result brief report shall be in word format.

3.2.2.8. Transaction Log

[SRS 90] The system shall store the attributes as defined in Table 31 for transaction log.

Table 31: Transaction Log

Attribute	Data Type	Values and Constraints	Description

DateTime	DateTime	Required; Not editable	Time and date of when the action was performed
Action Performed	String	Required; Not editable	Action performed
Analyst	String	Required; Not editable	Initial of analyst

3.2.2.9. Notification

[SRS 91] The system shall store the attributes as defined in for notification.

Table 32: Notification

Attribute	Data Type	Values and Constraints	Description
Duration	String	Required; Editable	Time before the threshold
Frequency	String	Required; Editable	Recurring time a notification should appear.

3.2.3. Stimulus

This section describes the stimulus requirements of the FRIC.

3.2.3.1. System Stimulus

3.2.3.1.1. Task/Subtask/Finding

[SRS 92] When the task assignment to an analyst is complete, the following shall be true:

a. The analyst has read access to all attributes of a task.
b. If the task has no subtask, the analyst has write access to the progress attribute of a task.
c. If the task has subtask, the analyst is assigned to each subtask.

[SRS 93] When the subtask assignment to an analyst is complete, the following shall be true:

a. The analyst has read access to all attributes of a task.
b. The analyst has read access to all attributes of a subtask.
c. The analyst has write access to the following attributes of a subtask:

i. Progress
ii. Collaborator.

[SRS 94] When the ability to sign up for a task is enabled, the analyst shall have the ability to sign up for a task.

[SRS 95] When the task sign up is complete, the following shall be true:

a. The analyst has read access to all attributes of the task.
b. If the task has no subtask, the analyst has write access to the progress attribute of the task.
c. If the task has subtask, the analyst is assigned to each subtask.

[SRS 96] When an analyst creates a subtask, the analyst shall be the creator of the subtask.

[SRS 97] When an analyst is a creator of a subtask, the following shall be true:

a. The analyst has read access to all attributes of the subtask.
b. The analyst has write access to all attributes of the subtask.

[SRS 98] When an analyst is a creator of a finding, the following shall be true:

a. The analyst has read access to all attributes of the finding.
b. The analyst has write access to the attributes of the finding.
c. The analyst has the ability to delete the finding.

[SRS 99] When an analyst is added as a collaborator to a task, the following shall be true:

a. The analyst has read access to all attributes of the task.
b. If the task has no subtask, the analyst has write access to the progress attribute of the task.
c. If the task has findings, the analyst is added as a collaborator to each finding of the task.
d. If the task has subtasks, the analyst is added as a collaborator to each subtask of the task.

[SRS 100] When an analyst is added as a collaborator to a subtask, the following shall be true:
a. The analyst has read access to all attributes of a subtask.
b. The analyst is added as a collaborator to the parent of the subtask.
c. The analyst has write access to the progress attribute of a subtask.
d. If the subtask has findings, the analyst is added as a collaborator to each finding of the subtask.

[SRS 101] When an analyst is added as a collaborator to a finding, the following shall be true:
a. The analyst is added as a collaborator to the subtask associated to the finding.
b. The analyst has read access to all attributes of the finding.
c. The analyst has the associate access to related finding attribute of a finding.
d. The analyst has append access to appendable attributes of the finding.

3.2.3.1.2. Archive

[SRS 102] When the archive operation of a system is complete, the following shall be true:
a. Archive status of the system is “archived”.
b. If the system has tasks, the system applies the archive operation on each task.
c. If the system has findings, the archive status of each finding (“active”) and the association between each finding and the system remains unchanged.

[SRS 103] When the archive operation of a task is complete, the following shall be true:
a. Archive status of the task is “archived”.
b. If the task has subtasks, the system applies the archive operation on each subtask.
c. If the task has findings, the archive status of each finding (“active”) and the association between each finding and the task remains unchanged.

[SRS 104] When the archive operation of a subtask is complete, the following shall be true:
a. Archive status of the subtask is “archived”.
b. If the subtask has findings, the archive status of each finding (“active”) and the association between each finding and the subtask remains unchanged.

3.2.3.1.3. Delete

[SRS 105] When the delete operation of an event is complete, the following shall be true:
a. Each system of the event is deleted.
b. Each task associated to the deleted system of the event is deleted.
c. Each subtask associated to the deleted task is deleted.
d. Archive status of each finding is “archived”.

[SRS 106] When the delete operation of a finding is requested and the requester is the creator of the finding, the following shall be true:
a. The finding is deleted.

3.2.3.1.4. Promote/Demote

[SRS 107] When the demotion of a task with no subtask is complete, the following shall be true:
a. The task becomes a subtask.
b. If the former task has findings, the finding association for the former task becomes finding association for the subtask.
c. The former task is associated to a task.

[SRS 108] When the promotion of a subtask is complete, the following shall be true:

a. The subtask becomes a task.
b. If the former subtask has findings, the finding association for the former subtask becomes finding association for the task.
c. If the former subtask is associated to a subtask, the subtask association for the former subtask becomes subtask association for the task.

3.2.3.1.5. Sync

[SRS 109] When the bi-directional sync operation is complete, the following shall be true:
a. The initiator merges changes from the target.
b. The target merges changes from the initiator.
c. Merge conflict is sent to initiator and target.

3.2.3.1.6. Notification

[SRS 110] When the due date is within the notification duration, the following shall be true:
a. The system generates a notification for all upcoming due dates.
b. The notification is set to active until the notification frequency expires.

[SRS 111] When the due date has passed, the system shall generate a notification regarding the missed due date.

3.2.3.2. User Interface Related Stimulus

3.2.3.2.1. General

[SRS 112] When the user presses the “OK” button on the overlay, the system shall close the overlay.

[SRS 113] When the user presses the “X” button on the overlay, the system shall dismiss the overlay.

[SRS 114] When the user presses the “downward arrow” at the column header, the system shall display the content of the column in descending order.

[SRS 115] When the user presses the “upward arrow” at the column header, the system shall display the content of the column in ascending order.

[SRS 116] When the user presses the add icon in the overview, the following shall be true:
a. A row in the overview table is added.
b. All input fields in the detailed view is enable.

[SRS 117] When the initial launch of FRIC is complete, the system shall display the Setup content View.

[SRS 118] If the launch of FRIC is complete and the launch is not an initial launch, the system shall display the Event content view.

3.2.3.2.2. Event Content View

[SRS 119] When the user presses the add icon in event team information, the system shall display the Add/Edit overlay.

[SRS 120] When the user selects the edit option in the event team information, the system shall display the Add/Edit overlay with prefilled information of the selected analyst:
a. First Name
b. Last Name
c. Initial
d. Title.

[SRS 121] When the user selects the sync option in the event team information, the system shall display the Sync overlay.

[SRS 122] When the user clicks on the analyst initial, the system shall display the Analyst Progress Summary Content View.

3.3. Non-behavioral Requirements

This section describes performance, availability, and usability requirements of the system.

TBD

&