INFOSAFE

Systems Requirements and Specifications

InfoSafe

Seed Analytics

Team Name: FrAgile

Team Members: Christof Steyn
Chris Mittendorf
Karel Smit
Yané van der Westhuizen
Alistair Ross

Team Contact: fragile.cos301@gmail.com

Table Of Contents

Introduction

InfoSafe is an application that is used by the Information Security team, System Administrators, Managers and other employees to automate the data security process. It is a single tool that can be used to monitor and manage any and all operations involving a company's data and projects within its Information Security Management System (ISMS).

The vision for this project is to create an easy to use application with a user friendly interface where an organization can have access to all their users, data scopes, support related queries/issues, risk reports and tasks.

Users will be assigned certain roles when their profile has been created on the application. These roles are defined by a set of permissions within the application, this is to manage data access as well as to assign administrative rights to certain users.

A specific terminology will be used throughout this document to describe the system and its functions. This terminology is defined below:

System Administrator	Full control over the system, hosting and databases.
ISO (Information Security Officer)	Full privileges in the system with abilities to create, edit and delete users and data scopes.
DISO (Deputy Information Security Officer)	Same as ISO above.
Data Scope	A system or set of data that is processed, with defined rules on how it may be processed.
Data Custodian	A manager of a data scope who can manage users and assets within a data scope and the progress of the data scope.
Compliance Matrix	This refers to a task/requirement tracker that is specific to a Data-scope or person

Objectives

The high-level objectives of the project include:

- Implement a system where new users can be created by an already existing “system-admin” user. The system should only allow users to log into the system and not register themselves.
- Implement an RDS database to securely store all the users data and system data that will be used throughout the project.
- Store all relevant data and permissions for each of the roles that are defined within our scope for this project.
- Implement a Home-page where a user can navigate to projects, assets and personal info.
- Create an interactive front-end that will display all relevant data and profile information to the user. The front-end should make use of a service to fetch the needed data from the RDS database.
- Setup AWS to deploy and host the system.
- Allow for the creation of data-scopes and the assignment of roles to a data-scope by the system administrator.
- Ensure a high level of system security to protect user and company information.
- Create thorough documentation of the system for easy understanding and thorough assessment

Business Need

Information Security Management is something that has become very important in the modern world as more and more people and companies value their data privacy and security online. Companies specifically take this very seriously if they would like to comply with the rules and regulations that are set out by various security and online privacy frameworks such as ISO 27001 (Information Security Management Systems), GDPR (General Data Protection Regulation) and the POPI Act. It has in the past proven to be a challenge to keep a handle on data and security measures and it is very important that companies do not have a data breach or unauthorized personnel gaining access to company files or hardware. Thus the opportunity presents itself to be able to streamline their Information Security Management Systems.

This project will benefit the company greatly in terms of efficiently managing projects and data scopes as well as keeping track of assets and hardware within the

organization. The application will neatly store all the relevant data of users, tasks, data-scopes, risks and assets all in one place. It will also help alleviate admin intensive tasks, repetitive and work tedious tasks, help streamline important workflows and thus allow employees to spend their time on more important tasks within the business.

Links To Supporting Documentation

Below are links to the supporting documentation of the Infosafe project:

User Manual

The User Manual describes in depth how a user can use the system and what they can expect based on their system role.

System Architecture

Describes the system architecture, styles, patterns, constraints and technology choices.

Database Design

The Database Design document describes the process of designing the database and normalizing the data to be stored in the database. It shows the table structure of the database.

Coding Standards

This document describes the file structure of the system and the coding standards and naming conventions followed.

Team Contributions

This contains all the contributions made by the team members for the demo

User Stories and Characteristics

There are six main types of users within the Infosafe system that are the System Administrator, The ISO (Information Security Officer), The DISO (Deputy Information Security Officer), A Data Custodian, The Asset Manager and the General User.

System Administrator

The System Administrator has full access, control and privileges over the system. They are able to edit and control the hosting and deployment of the system and will be able to make changes to the database. Although the System Administrator has the most access controls over the system they are hierarchically below the ISO and DISO and any and all changes they wish to make will need to be approved by these individuals.

ISO

The ISO is the highest ranked user in the system. They have the ability to create users and data scopes, approve access and service requests as well as assign tasks. As mentioned above they do not have as much access as the System Administrator but the System Administrator will need approval of any changes by the ISO. The ISO is mainly in charge of day to day operation in the company and uses the Infosafe system to administer the daily operations.

DISO

The DISO is ranked directly under the ISO. They will have much of the same system access as the ISO and will mainly fill the role of the ISO when the ISO is unavailable. They however cannot create data scopes or action tasks.

Data Custodian

The Data Custodian is in charge of looking after data scopes. They will be able to create data scopes and administer them. They will also create and assign roles within a data scope. These roles are different to systems roles and should not be confused. These roles can be named anything and a description will be provided as well as the functionality these roles have within the data scope.

Asset Manager

The Asset Manager is in charge of the Assets subsystem in Infosafe. They will maintain a list of assets and be able to create tasks with reference to assets and assign them to users. They will also handle asset requests.

General User

The General User (or standard company employee) will be able to interact with existing elements in the system but cannot create new elements, apart from service and access requests. They can interact with existing data scopes, be assigned tasks, make requests for access and assets and log risks and findings to name a few.

User Stories

As a **System-Administrator** of InfoSafe:

Users:

- I can create new users
- I can revoke existing users
- I can edit existing users

System Configuration:

- I can change system configurations

General:

- I can do everything a General User can do

As an **ISO** of InfoSafe:

Users:

- I can create users and roles
- can update users and roles
- I can revoke users and roles

Data Scopes:

- I can update data-scopes
- I can revoke data-scopes
- I can approve or reject requests inside a data-scope
- I may be assigned to a task within a data-scope

Access Requests:

- I can update access requests
- I can revoke access requests
- I can approve or reject access requests
- I may be assigned to access requests

Assets:

- I can create assets
- I can update assets

Compliance Matrix:

- I can create a task
- I can update a task
- I can assign tasks to other users
- I may be assigned to tasks
- I can revoke a task

Support Requests:

- I can update support requests
- I can assign tasks to support

Risks and Findings:

- I may be assigned to access requests
- I may be assigned to a risk

- I may be assigned to access requests
- I may be assigned to access requests
- I can assign risks
- I can approve or reject a risk
- I can create a new risk
- I can update a risk

General:

- I can do everything a General User can do

As a **DISO** of InfoSafe:

Users:

- I can create users and roles
- I can update users and roles
- I can revoke users and roles

Data Scopes:

- I may be assigned to a task within a data-scope

Access Requests:

- I can update access requests
- I can revoke access requests
- I may be assigned to access requests
- I can approve or reject access requests

Compliance Matrix:

- I can create a compliance matrix task
- I can update a compliance matrix task
- I can revoke a compliance matrix task
- I can assign tasks to other users on a compliance matrix

Support Requests:

- I can update support requests
- I can assign tasks to support
- I may be assigned to a support task

Risks and Findings:

- I can create a new risk
- I can update a risk
- I can assign tasks to risks
- I may be assigned to a risk

General:

- I can do everything a General User can do

As a **Data Custodian** of InfoSafe:

Data Scopes :

- I can update data scopes
- I may be assigned to a task within a data scope

- I can update access requests
- I can revoke access requests
- I may be assigned access request tasks
- I may be assigned to tasks
- I can create a new risk
- I can update a risk
- I may be assigned to a risk
- I can create a data scope

General

- I can do everything a General User can do

As an **Asset Manager** of InfoSafe:

Assets:

- I can create assets
- I can update assets
- I may be assigned tasks that are asset related

General:

- I can do everything a General User can do

As a **General User** of InfoSafe:

Data Scopes:

- I can be assigned tasks within a data
- I can request access to a data scope

scope

Tasks:

- I can be assigned tasks
- I can submit tasks for approval

Support Requests:

- I can request support on assets and systems
- I can create support requests
- I can be assigned support related tasks

Assets:

- I can request an asset

Risks and Findings:

- I can log risks
- I can submit risks for approval

System Configuration:

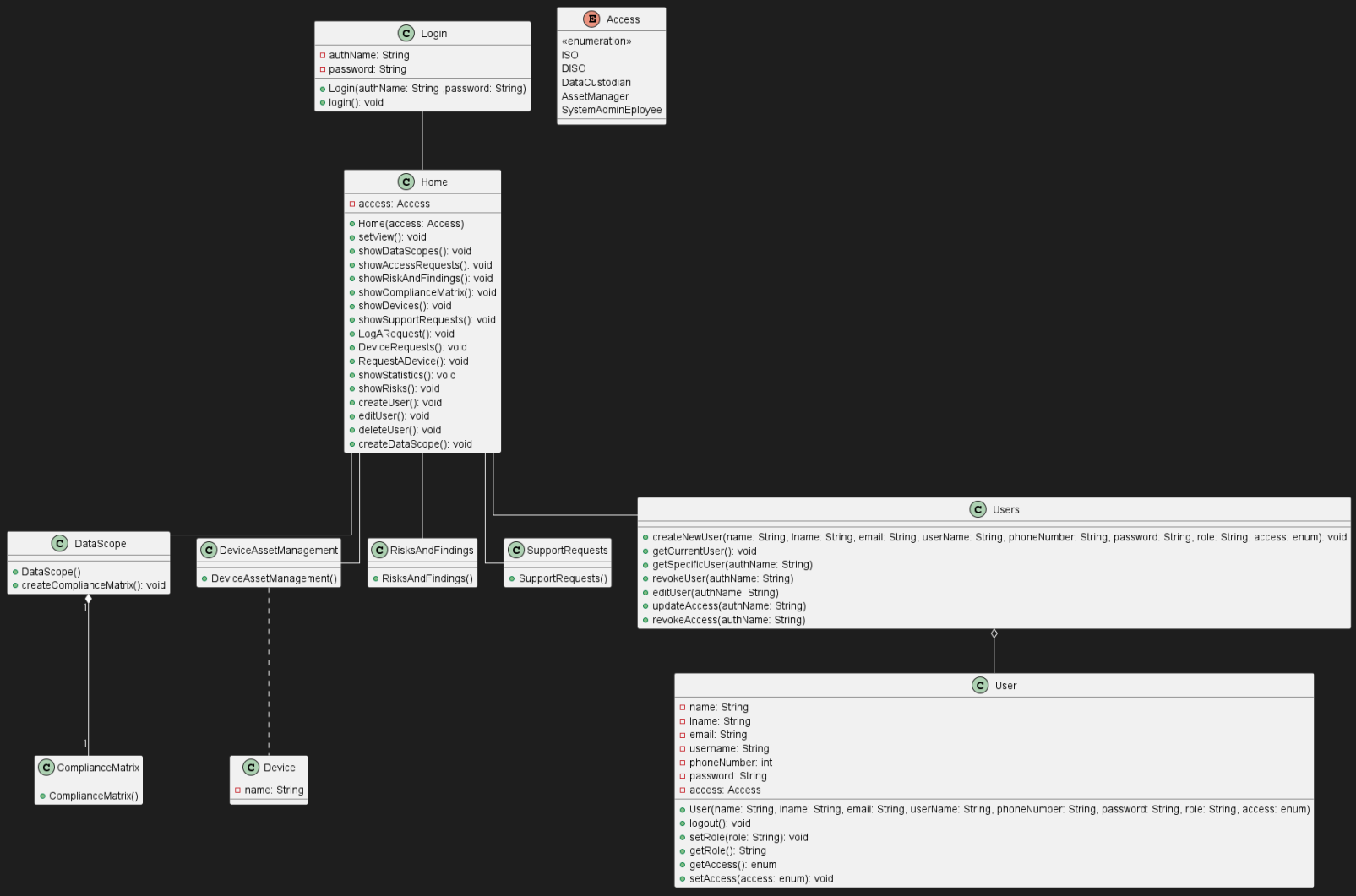
- I can change my password
- I can log in and out

As a **Support Entity** within a Data Scope of InfoSafe:

Data Scopes (Limited to the one they are assigned) :

- I may be assigned to support related tasks

UML Class Diagram



Functional Requirements

R1. Users and Roles Subsystem

a. Users and Roles Requirements

R1.1: An existing system administrator will be able to create users and supply them with a generic password for initial system access.

R1.2: Existing users will be supplied with a password to login to the system. They may then add their personal details to be captured in the database and change their password to one of their liking.

R1.3: Users must then be able to login to the system from a web browser whenever they wish.

R1.4: The supplied password will be a random generated password which the system will email to the user. The password needs to follow certain criteria in order to be a secure and valid password.

R1.5: Users must be able to navigate the system from the home page to view data , scopes, access their assigned data scopes, update their personal details, log support requests, manage assets and risks.

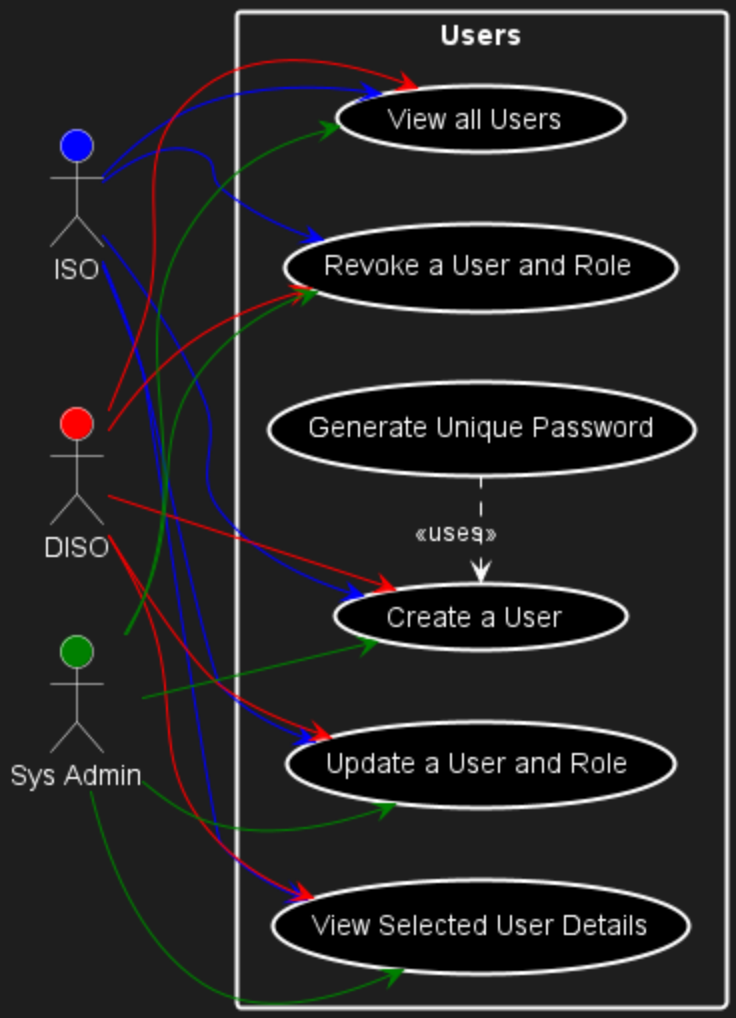
R1.6: The ISO, DISO and data custodians (described above) will be able to create data scopes and assign users specific roles within this data scope. A user can be assigned different roles in different data scopes and also be assigned more than one role in a single data scope.

R1.7: Anyone can view the data scopes but only the ISO and data scope's Data Custodian are able to update the data scope. (See User stories for different roles.

R1.8: Users will be able to apply for access requests to a data scope.

R1.9: Asset Managers will be able to manage assets, request for new assets and remove old assets.

b. Users and Roles Use-case Diagram



R2. Data-Scope Subsystem

a. Data-Scope Requirements

R2.1: Data scopes can be created by a data custodian.

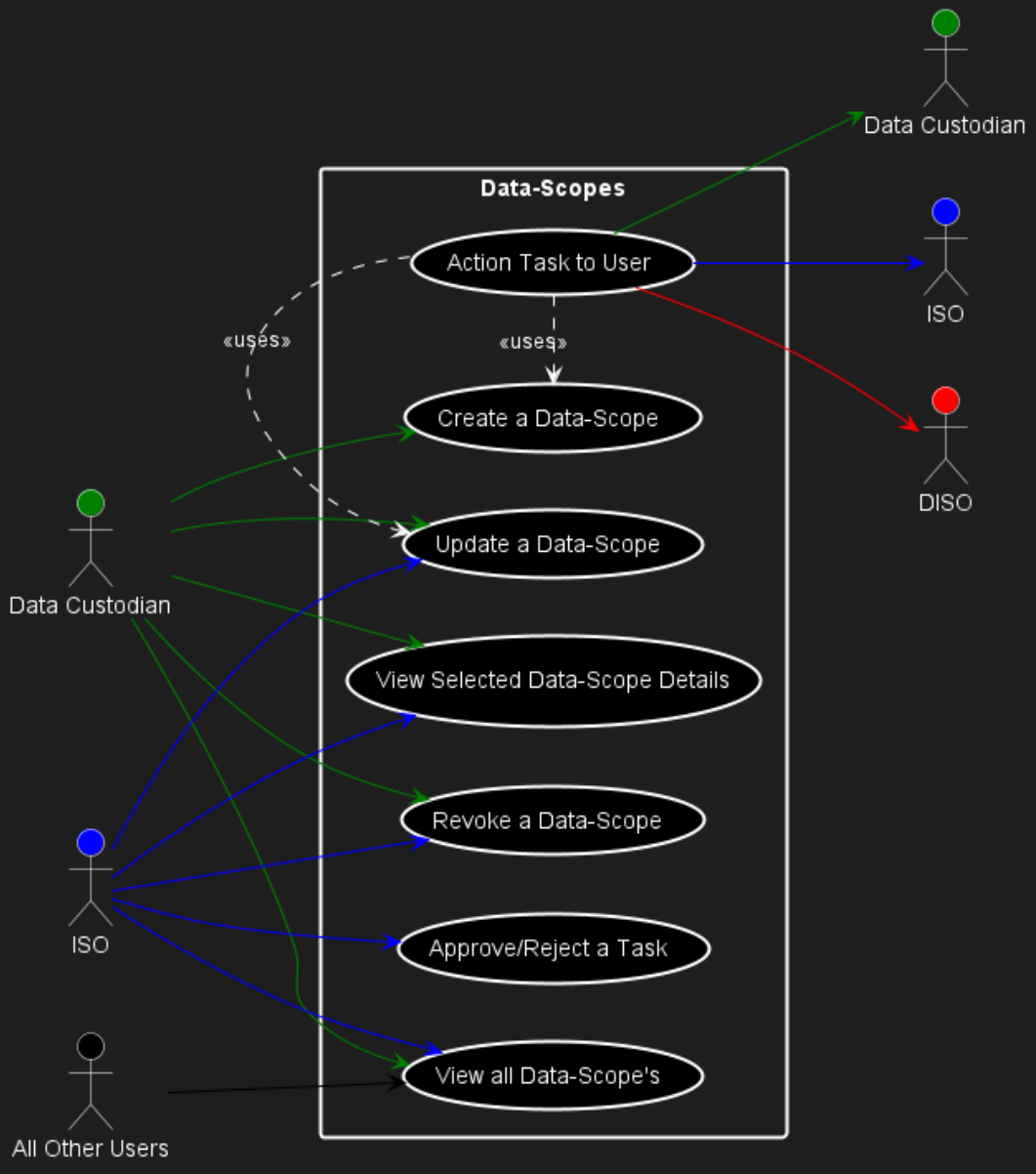
R2.2: Data scopes can be updated by a data custodian or the ISO.

R2.3: Users can be added or removed from a data scope by a data custodian or the ISO.

R2.4: Tasks can be assigned to users within a data scope.

R2.5: Once data scopes are created they can be approved or rejected by the ISO.

b. Data-Scope Use-case Diagram



R3. Access Requests Subsystem

a. Access Requests Requirements

R3.1: All users can log a support request.

R3.2: Data custodians, ISO and DISO capture the request for processing and update if necessary.

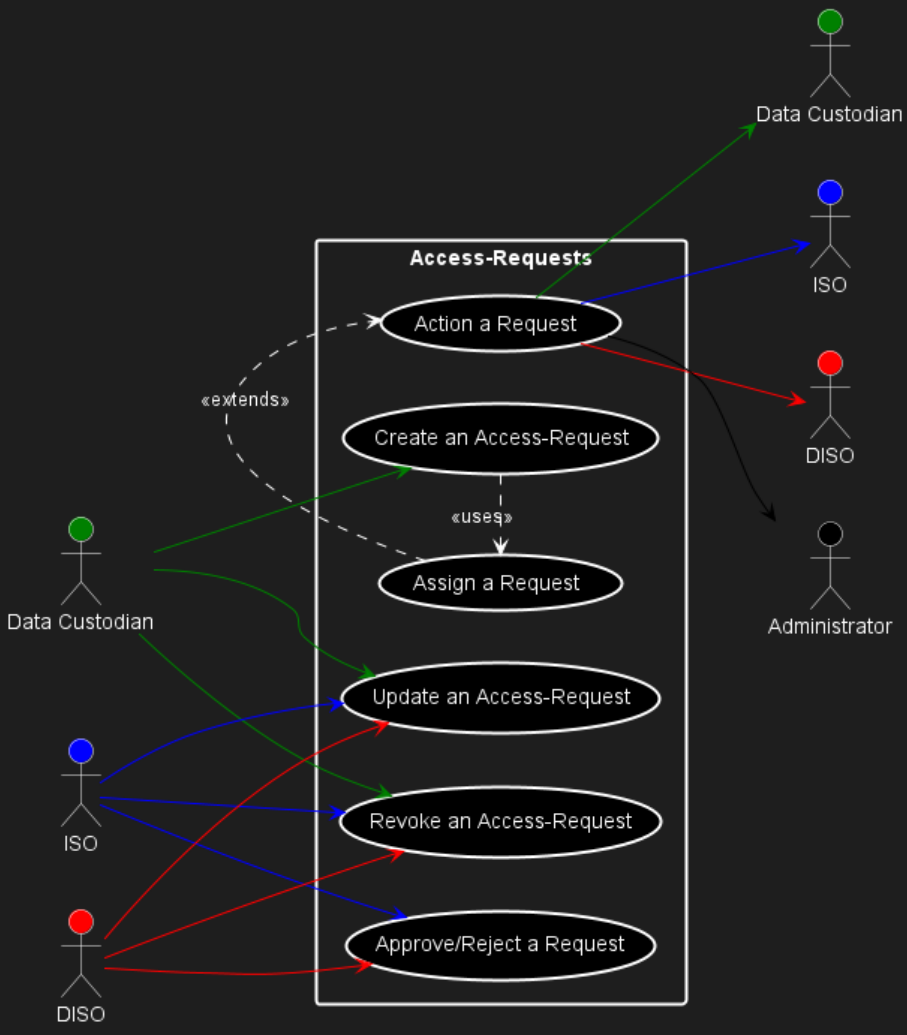
R3.3: The ISO or DISO can approve or deny a request.

R3.4: The system will notify the system administrator if a request is approved so that the system administrator can grant the relevant permissions and access.

R3.5: The system will notify the user of the status of their request.

R3.6: A Data custodian of the data scope will be notified when a user's access or permissions have been updated.

b. Access Requests Use-case Diagram



R4. Asset Management Subsystem

a. Asset Management Requirements

R4.1: Assets can be added to the system by the ISO or asset manager.

R4.2: Assets can be updated by the ISO or asset manager.

R4.3: Assets can be assigned to users.

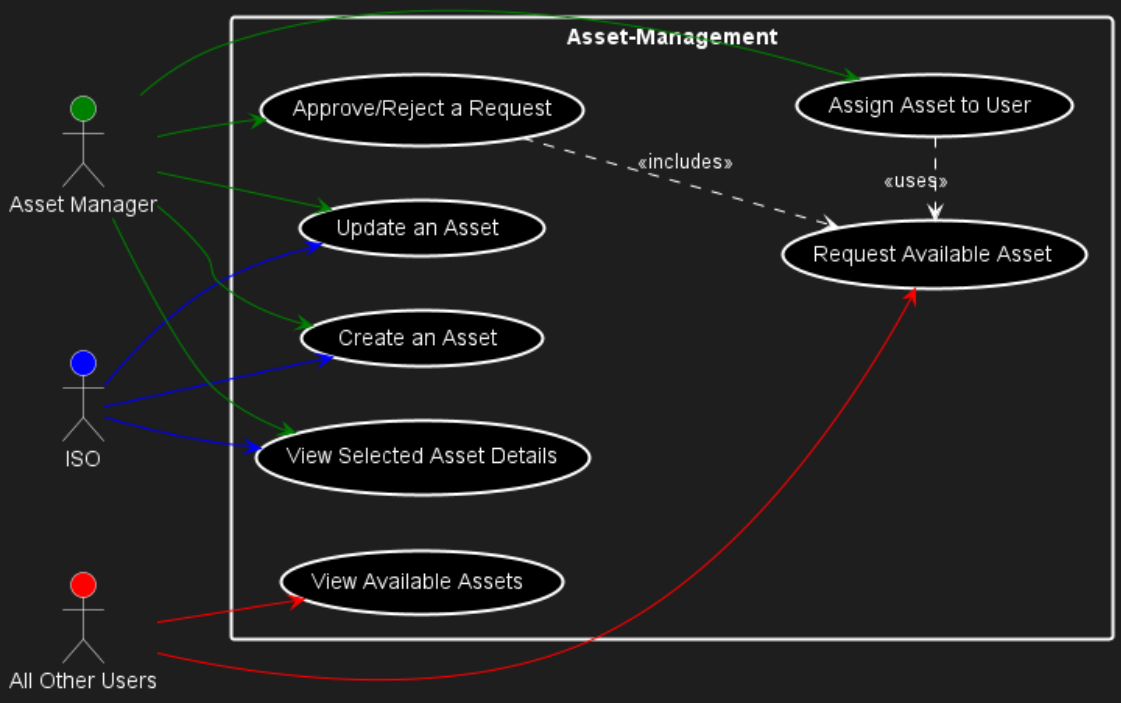
R4.4: Users can view a list of types of hardware devices they may request.

R4.5: Users can make requests for an asset.

R4.6: Asset managers can approve or deny requests for assets by users.

R4.7: Asset managers can remove hardware from the system once it has been disposed of.

b. Asset Management Use-case Diagram



R5. Compliance Matrix Subsystem

a. Compliance Matrix Requirements

R5.1: The ISO or DISO can assign information security compliance tasks to users.

R5.2: The ISO or DISO can create and assign a task to anyone.

R5.3: The ISO or DISO can update or remove tasks in the compliance matrix.

R5.4: Tasks will have due dates.

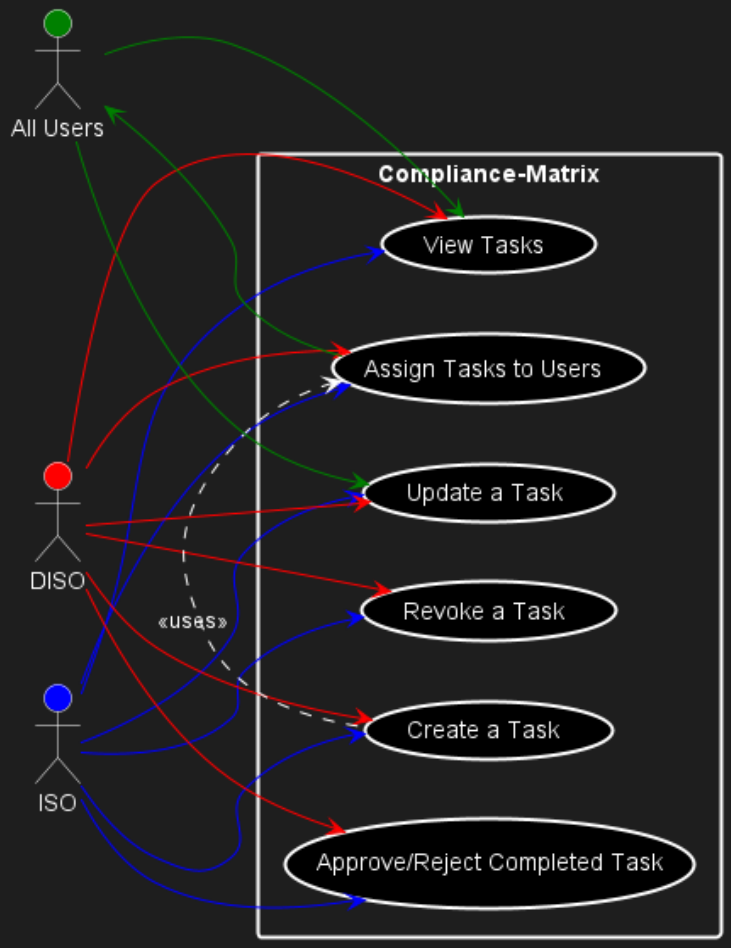
R5.5: Users can view all their tasks and update their status.

R5.6: Tasks once completed will be approved or denied by the ISO.

R5.7: Denied Tasks will need to be sent to the data custodian for reassignment.

R5.8: Documents and emails related to a task will need to be stored.

b. Compliance Matrix Use-case Diagram



R6. Support Requests Subsystem

a. Support Requests Requirements

R6.1: All user types can log support requests.

R6.2: Support requests can be for laptop hardware, Microsoft Applications, Microsoft Accounts, working of applications rolled-out to laptops by Microsoft EndPoint Manager, working of any applications that may be as a result of policies rolled-out by End-Point Manager.

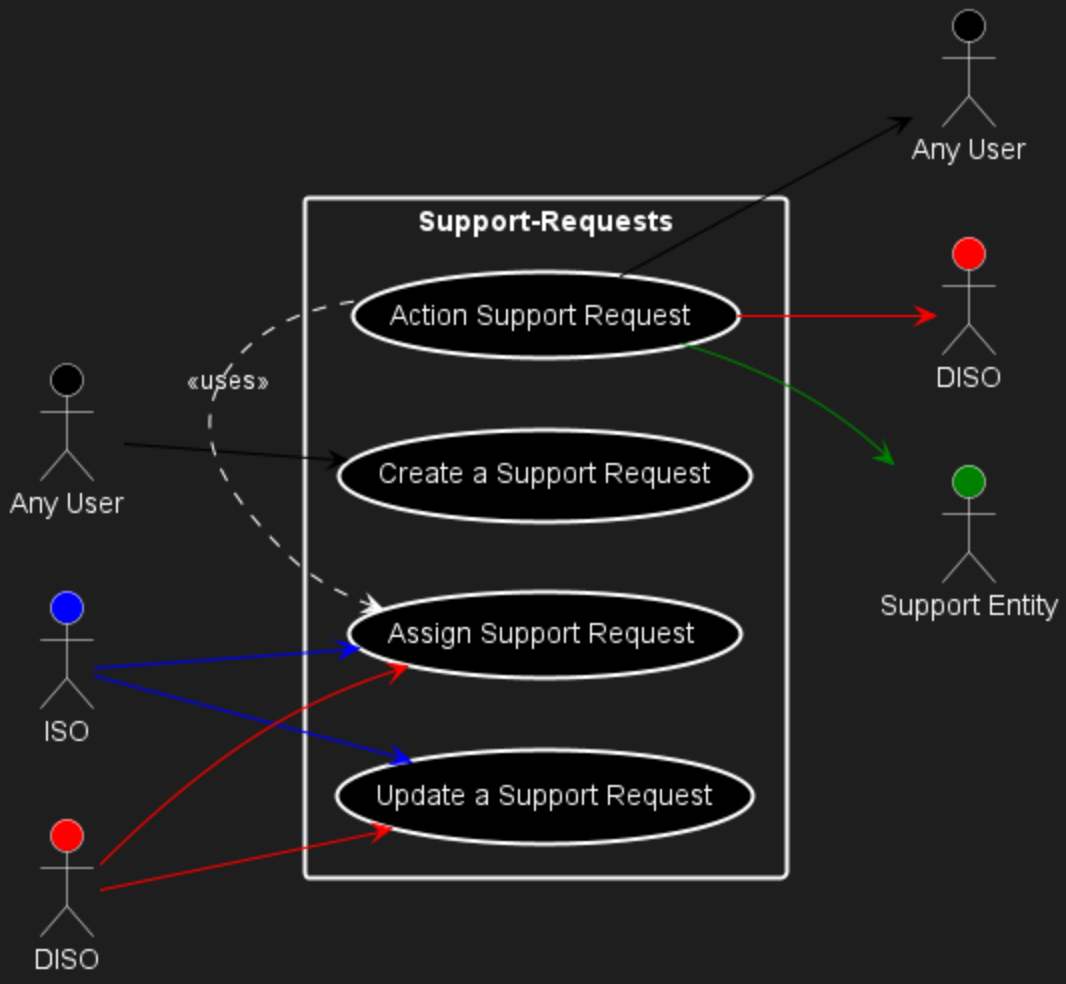
R6.3: The ISO or DISO will receive the request for review.

R6.4: The ISO or DISO can approve, deny or reassign the request to the relevant role.

R6.5: The ISO or DISO can update a request.

R6.6: Users will receive updates on the status of their request.

b. Support Requests Use-case Diagram



R7. Risks and Findings Subsystem

a. Risks and Findings Requirements

R7.1: Users can log potential risks or findings within a data scope.

R7.2: These risks can be assigned an impact rating from 1 to 5, with 1 being an acceptable/low risk and 5 being a critical risk.

R7.3: Based on these risks that are logged the ISO or DISO can assign tasks to users that will review and assess these risks.

R7.4: The ISO will approve or deny the risk findings reports and may update if necessary.

R7.5: The ISO can set the status of the risks to Accepted, Avoided, Transferred or Mitigate.

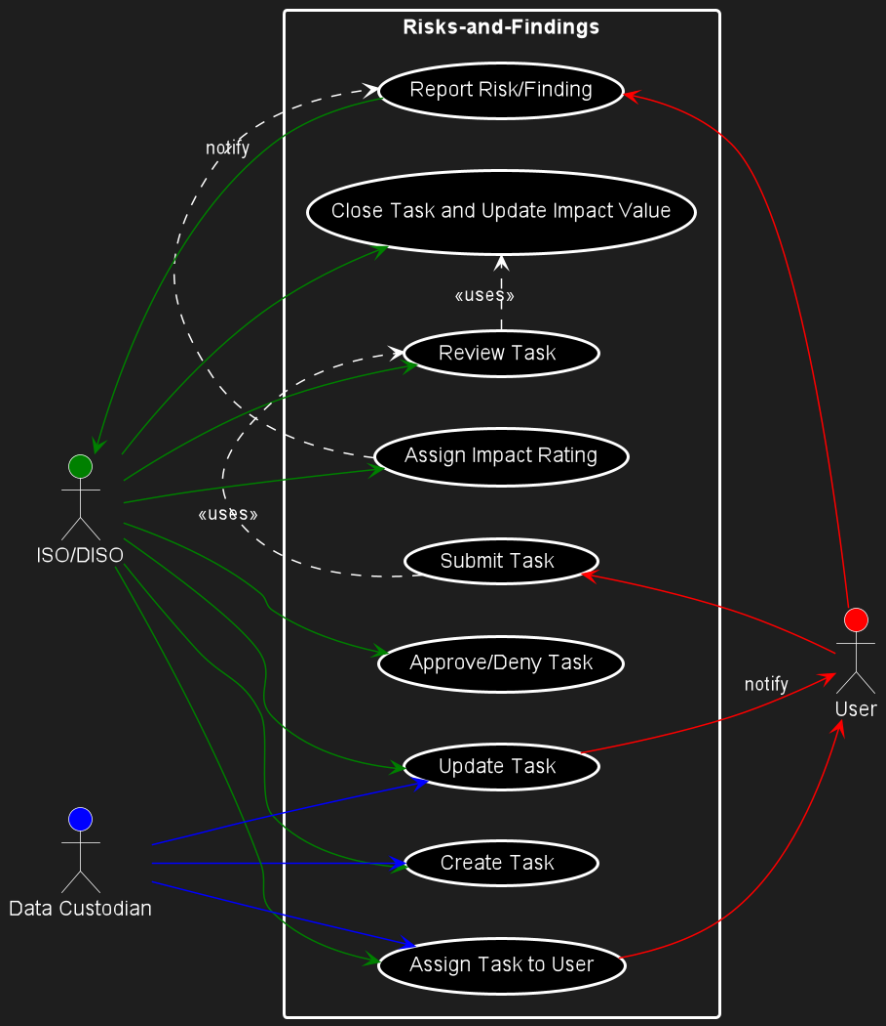
R7.6: If approved risks are assigned the “Mitigate” status, tasks can be created and assigned to a user with a due date to resolve the risk.

R7.7: Assigned users will receive notifications from their tasks.

R7.8: Assigned tasks will have a status to track progress.

R7.9: Once assigned tasks are completed they are sent to the ISO for review to confirm if tasks were completed successfully to mitigate the risk and then approve or reject the task. The ISO will also update the impact value for the risk.

b. Risks and Findings Use-case Diagram



Appendix A

Changes made to document since demo 1 :

- Appendix added
- Title Added
- Links to supporting documentation added
- User Characteristics added
    - System Administrator
    - ISO and DISO
    - Asset Manager
    - General User
- User Stories updated and tabularised
- Functional Requirements
- Updated User Use-Case Diagram
    - Added the “View User” use-case.
    - Added the “View Selected User Details” use-case.
    - Changed “View a User” to “View all users”
    - Added “Generate Password” use-case.
- Updated Data-Scope Use-Case Diagram
    - Added the “View all Data-Scope’s” use-case.
    - Added the “View Selected Data-Scope Details” use-case.
    - Added “All Other Users” actor.
- Updated Asset-Management Use-Case Diagram
    - Added “View Selected Asset Details” use-case.
- Updated Compliance Matrix Use-Case Diagram
    - Added the “View Tasks” use-case.
    - Renamed the use-cases to the correct naming format(using tasks instead of compliance matrix).
    - Removed “Action Task” use-case due to repeating use-cases.
    - Added “Complete/Reject Completed Task” use-case.
- System Architecture
    - Quality requirements were removed
    - Headings for system architectures and such were removed
    - The above items were removed as they have been added to the System Architecture document that has been linked