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.

User Stories

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

- I can create new users.
- I can revoke existing users.
- I can edit existing users.
- I can change system configurations.

As an **ISO** of InfoSafe:

- I can create users and roles
- I can update users and roles
- I can revoke users and roles.
- I can update data-scopes.
- I can revoke data-scopes.
- I may be assigned to a task within a data-scope.
- I can approve or reject requests inside a data-scope.
- I can update access requests.
- I can revoke access requests.
- I may be assigned to access requests.
- I can approve or reject access requests.
- I can create assets.
- I can update assets.
- 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.
- I may be assigned to tasks on a compliance matrix.
- I can update support requests.
- I can assign tasks to support.
- I can create a new risk.
- I can update a risk.
- I can assign risks
- I may be assigned to a risk.
- I can approve or reject a risk.

As a **DISO** of InfoSafe:

- I can create users and roles
- I can update users and roles
- I can revoke users and roles.
- 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 to access requests.
- I can approve or reject access requests.
- 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.
- I can update support requests.
- I can assign tasks to support.
- I may be assigned to a support task.
- I can create a new risk.
- I can update a risk.
- I can assign tasks to risks.
- I may be assigned to a risk.

As a **Data Custodian** of InfoSafe:

- I can create data scopes.
- I can revoke data scopes.
- I can update data scopes.
- I may be assigned to a task within a data scope.
- I can create an access request.
- I can update access requests.
- I can revoke access requests.
- I may be assigned access request tasks.
- I may be assigned to tasks on the compliance matrix.
- I can create a new risk.
- I can update a risk.
- I may be assigned to a risk.

As an **Asset Manager** of InfoSafe:

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

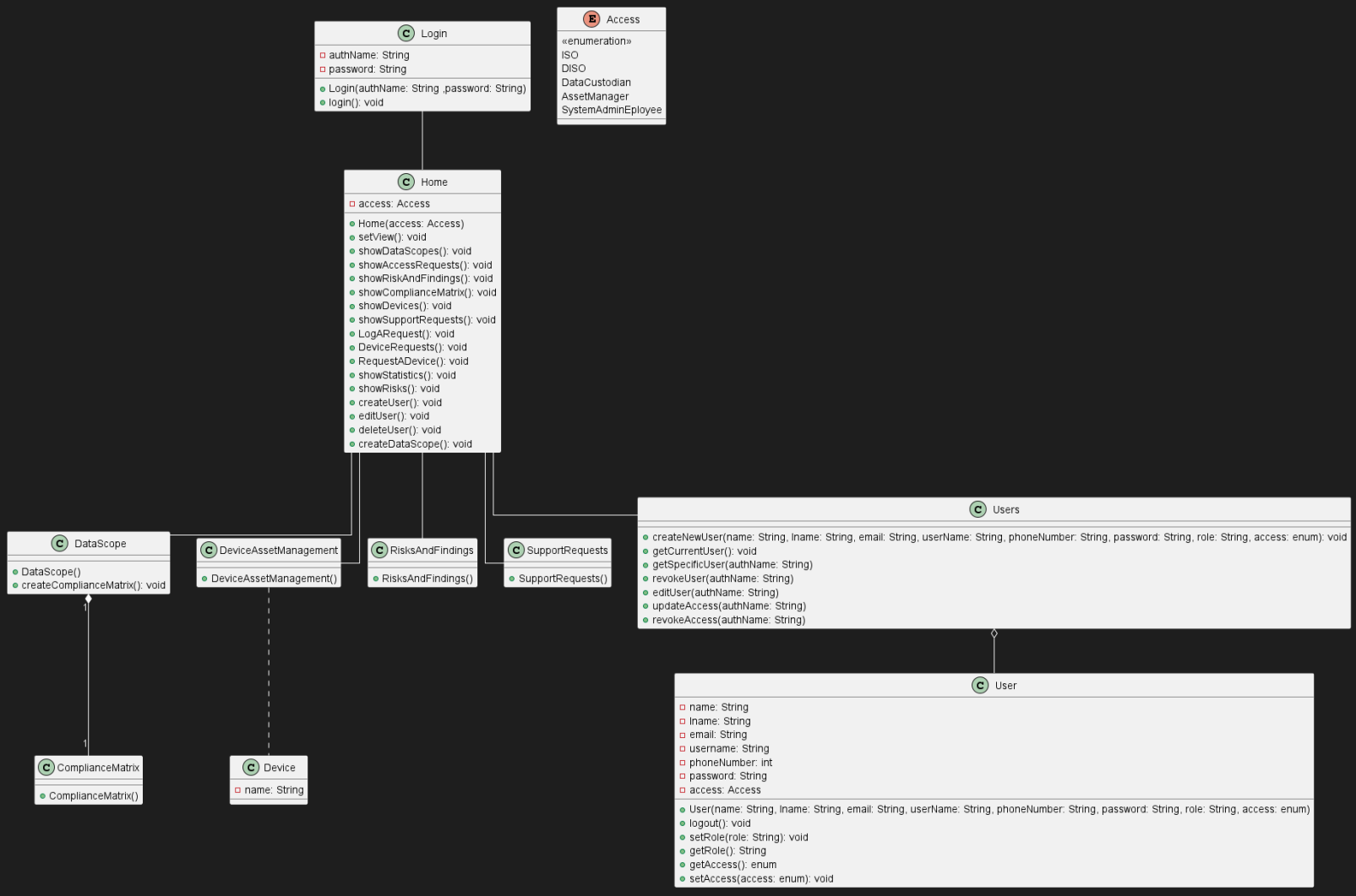
As a **Support Entity** of InfoSafe:

- I may be assigned to support related tasks.

As an **Any User** of InfoSafe:

- I can create support requests.
- I may be assigned to support related tasks.

UML Class Diagram



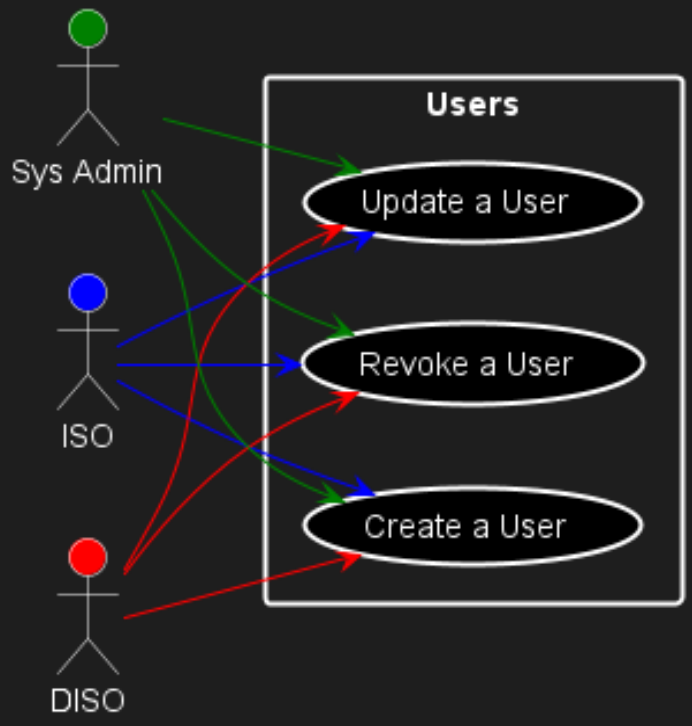
Functional Requirements

1. Users and Roles Subsystem

a. Users and Roles Requirements

- An existing system administrator will be able to create users and supply them with a generic password for initial system access.
- 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.
- Users must then be able to login to the system from a web browser whenever they wish.
- 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.
- 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.
- 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.
- 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.
- Users will be able to apply for access requests to a data scope.
- Asset Managers will be able to manage assets, request for new assets and remove old assets.

b. Users and Roles Use-case Diagram

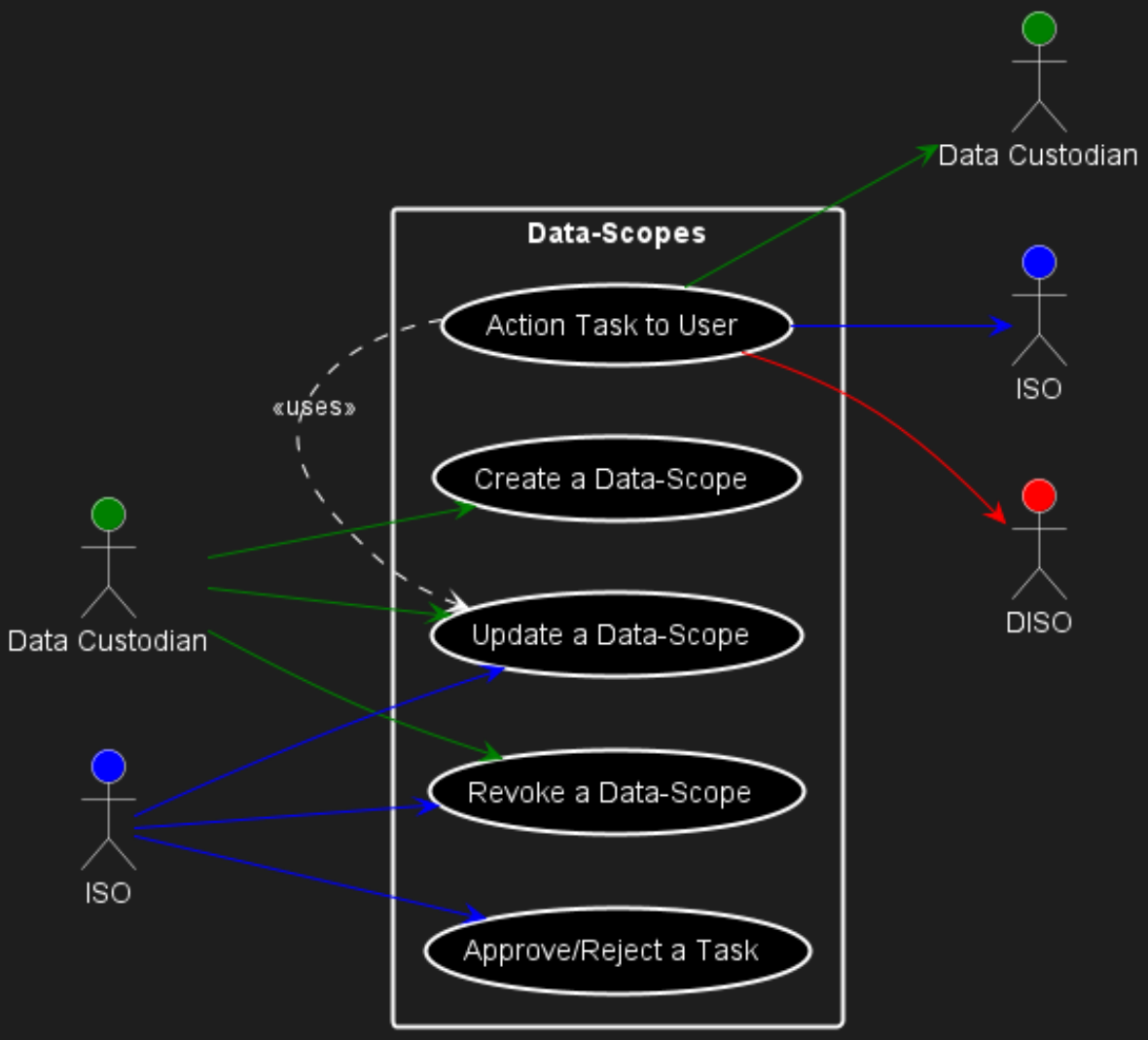


2. Data-Scope Subsystem

a. Data-Scope Requirements

- Data scopes can be created by a data custodian.
- Data scopes can be updated by a data custodian or the ISO.
- Users can be added or removed from a data scope by a data custodian or the ISO.
- Tasks can be assigned to users within a data scope.
- Once data scopes are created they can be approved or rejected by the ISO.

b. Data-Scope Use-case Diagram

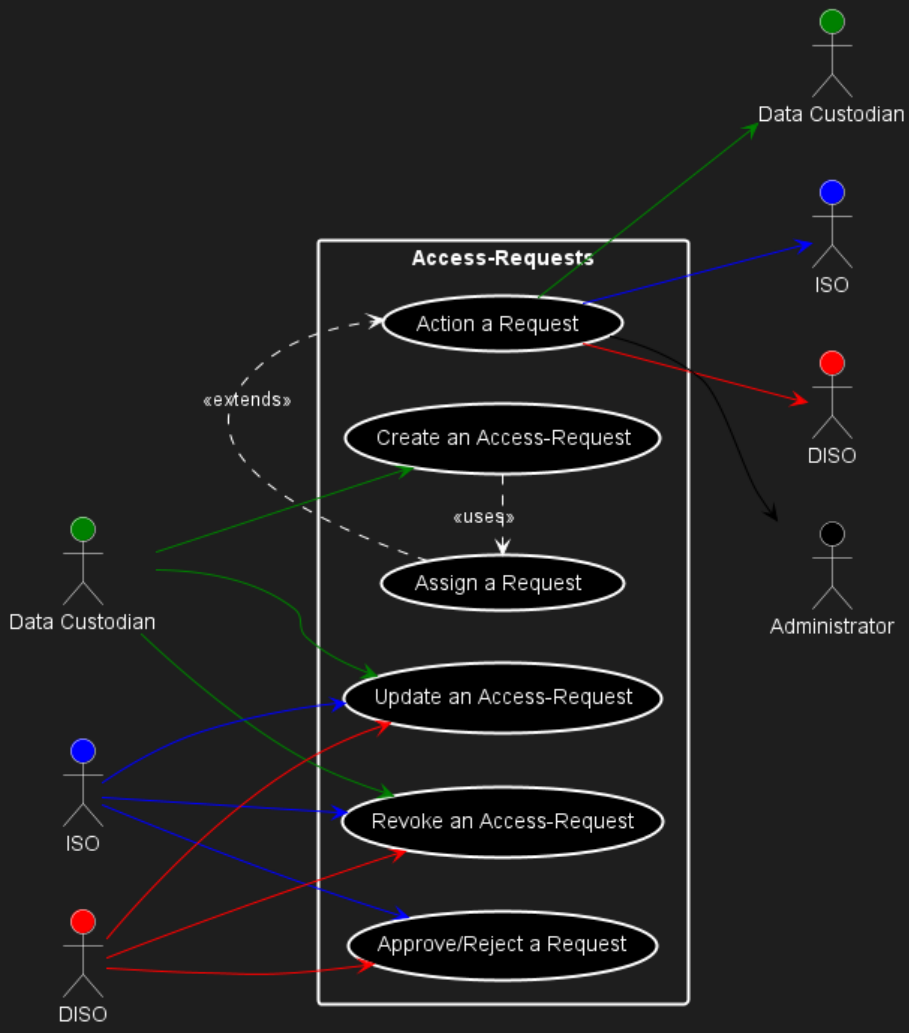


3. Access Requests Subsystem

a. Access Requests Requirements

- All users can log a support request.
- Data custodians, ISO and DISO capture the request for processing and update if necessary.
- The ISO or DISO can approve or deny a request.
- The system will notify the system administrator if a request is approved so that the system administrator can grant the relevant permissions and access.
- The system will notify the user of the status of their request.
- 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

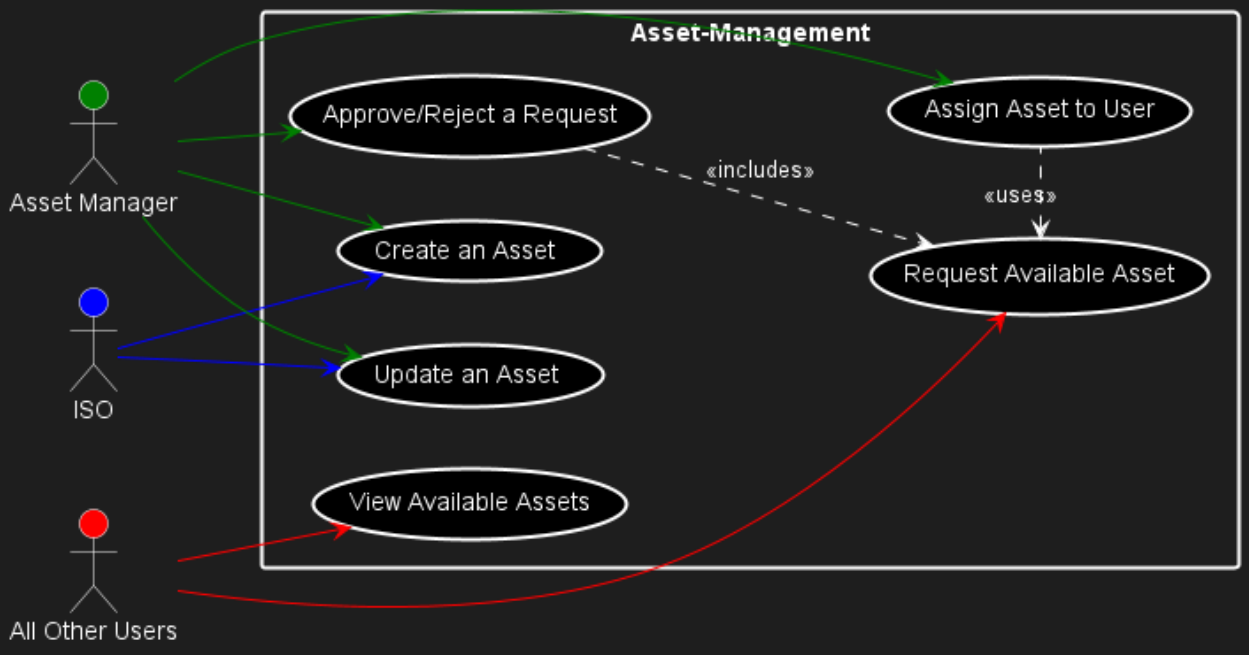


4. Asset Management Subsystem

a. Asset Management Requirements

- Assets can be added to the system by the ISO or asset manager.
- Assets can be updated by the ISO or asset manager.
- Assets can be assigned to users.
- Users can view a list of types of hardware devices they may request.
- Users can make requests for an asset.
- Asset managers can approve or deny requests for assets by users.
- Asset managers can remove hardware from the system once it has been disposed of.

b. Asset Management Use-case Diagram

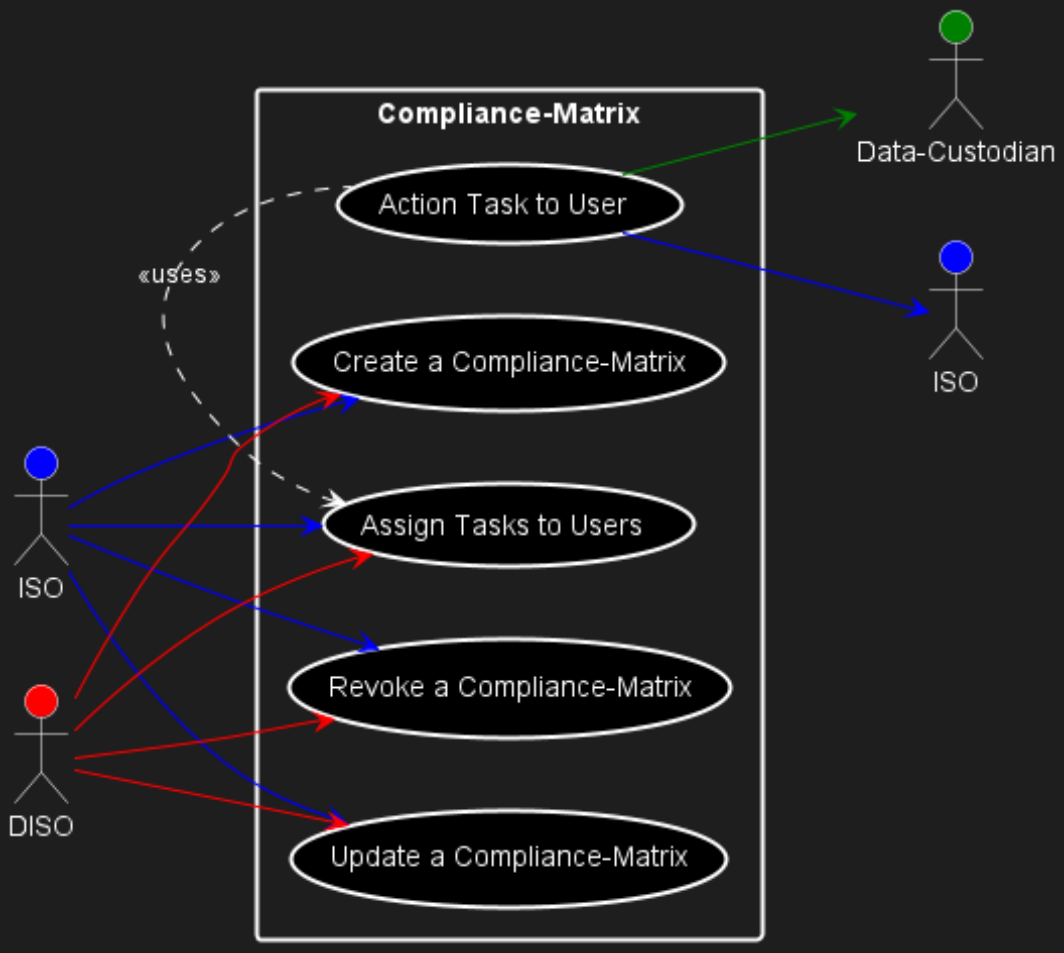


5. Compliance Matrix Subsystem

a. Compliance Matrix Requirements

- The ISO or DISO can assign information security compliance tasks to users.
- The ISO or DISO can create and assign a task to anyone.
- The ISO or DISO can update or remove tasks in the compliance matrix.
- Tasks will have due dates.
- Users can view all their tasks and update their status.
- Tasks once completed will be approved or denied by the ISO.
- Denied Tasks will need to be sent to the data custodian for reassignment.
- Documents and emails related to a task will need to be stored.

b. Compliance Matrix Use-case Diagram

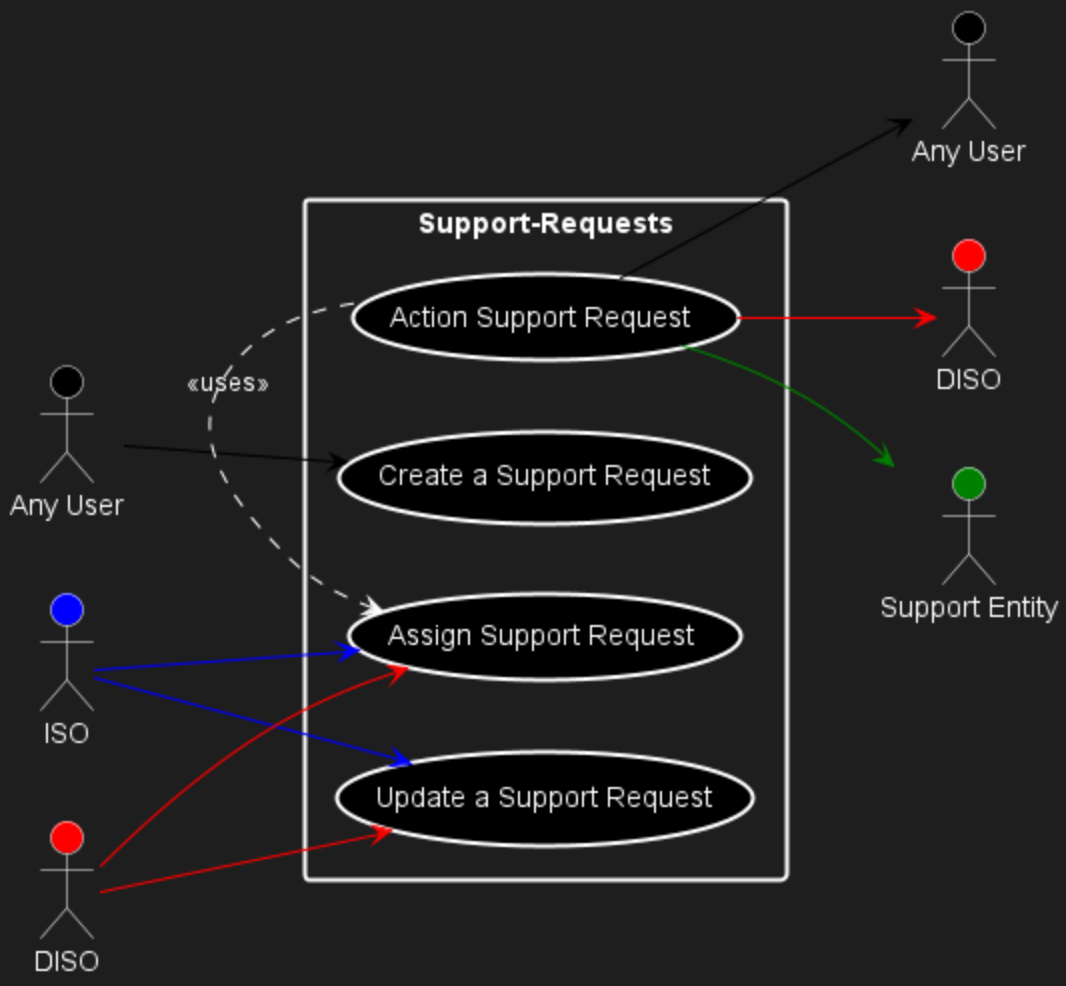


6. Support Requests Subsystem

a. Support Requests Requirements

- All user types can log support requests.
- 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.
- The ISO or DISO will receive the request for review.
- The ISO or DISO can approve, deny or reassign the request to the relevant role.
- The ISO or DISO can update a request.
- Users will receive updates on the status of their request.

b. Support Requests Use-case Diagram

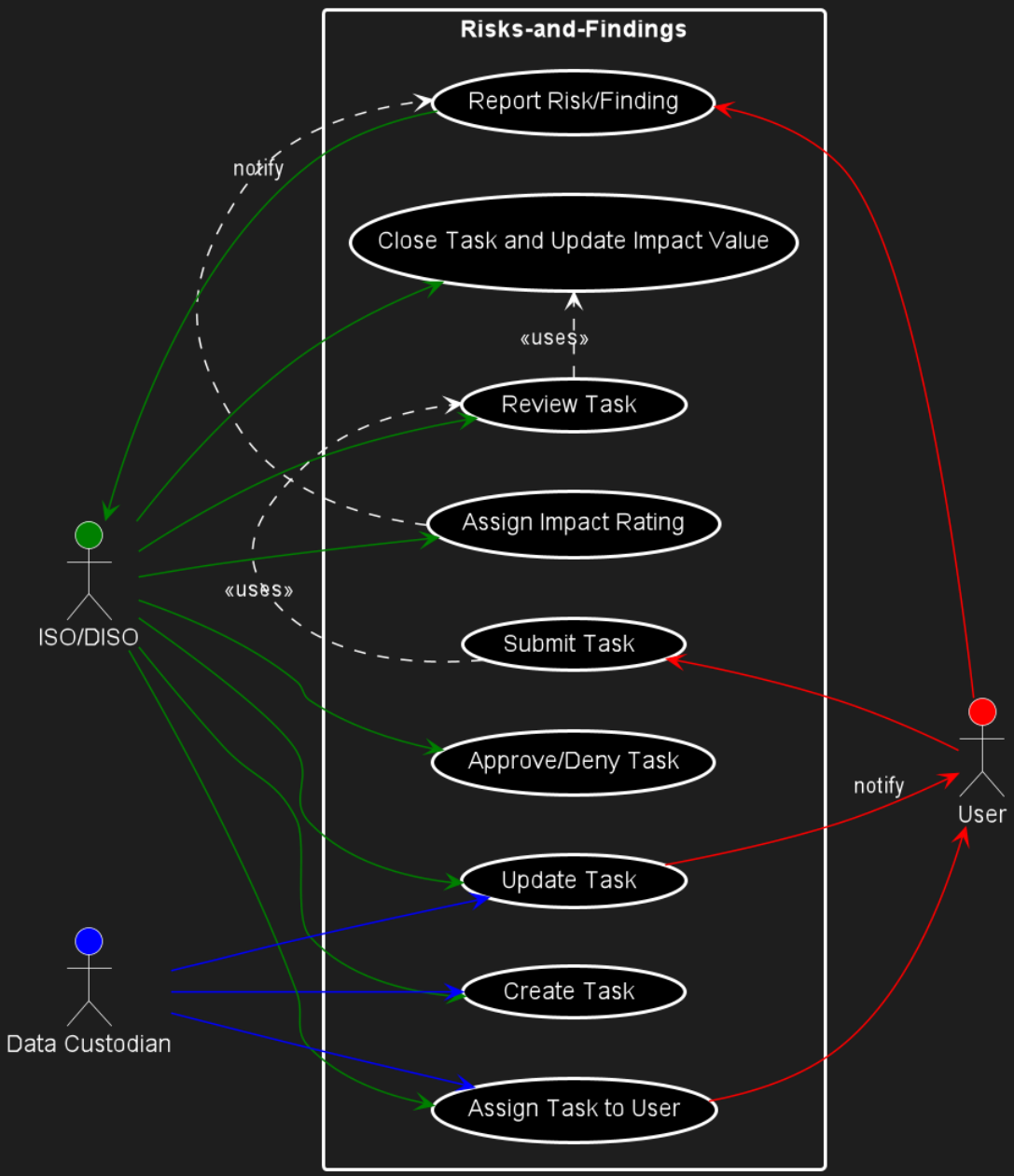


7. Risks and Findings Subsystem

a. Risks and Findings Requirements

- Users can log potential risks or findings within a data scope.
- 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.
- Based on these risks that are logged the ISO or DISO can assign tasks to users that will review and assess these risks.
- The ISO will approve or deny the risk findings reports and may update if necessary.
- The ISO can set the status of the risks to Accepted, Avoided, Transferred or Mitigate.
- 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.
- Assigned users will receive notifications from their tasks.
- Assigned tasks will have a status to track progress.
- 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



Quality Requirements

- Functional Suitability
    - The system will meet the specified functional requirements as laid out by the client and the functions will perform as intended, effectively and correctly. All features will support the necessary needs of the user as intended.
- Performance Efficiency
    - The system should run with an appropriate response time and the performance levels of the system will be in an acceptable range of the clients specifications. Scalability and storage will not be an issue as AWS automatically scales and accounts for load balancing when the system traffic is high and the database can be scaled infinitely to accommodate all the clients storage requirements.
- Compatibility
    - The system will be compatible on all major web browsers as per the client's request and will contain open source software that will allow the system to be compatible with other hardware and networks. There should be no disruptions or conflicts to service due to compatibility issues.
- Usability
    - One of the main aims of the system is to supply a user-friendly and easy to navigate user interface that offers ease of access and very little time to become familiar with. The users should be satisfied with the layout of the system as they will be using the system for long periods throughout the work day and the interaction of the system should help the user achieve their goals.
- Reliability
    - The system should be reliable at all times as it is essential for a business utilizing the system to be able to access it at all times. This should also account for error handling, availability and recovery of the system. There should not be any unexpected interruptions or failures that could compromise a business' productivity.
- Security

    - Security is of the utmost importance in the system as we will be dealing with lots of personal data and data related to a company's proprietary work. The system should be protected from unauthorized access, disclosure of personal or company data or destruction of the system. It is thus essential to include the relative access authorisations, data encryption, vulnerability management and be comp;onat with ISO security standards.
- Maintainability
    - The system should be easy to maintain and update in order to give the user the best possible experience when using the system. The code should be modularized for ease of updating and enhancements and well documented so it is easy to read and understand. The system should ensure it is easy to manage over its development lifecycle and that changes and enhancement can be made effectively and easily.
- Portability
    - The system should be able to use any web browser on various different hardware options. This will involve making sure the system factors to different viewport styles and screen size options.

Architectural Patterns

Design Patterns

Constraints

Technology Requirements