UNIVERSITY OF SOUTHAMPTON
Faculty of Physical Sciences and Engineering

A project progress report submitted for the award of
BSc Computer Science

Supervisor: Professor Nawfal Fadhel
Examiner: Dr Jie Zhang

Automatically Generated Cyber Security Compliance Engine

by James D'Alton

30 November 2019

Contents

List of Figures

List of Tables

INTRODUCTION

1.1 Overview

Many businesses require their partners to comply with numberous and varied cyber security compliances, of which there are literally hundreds. Cyber supply chain risk management (CSCRM) differs from cyber security, by gaining a higher degree of governance over the company in question, and over its extended enterprise partners, such as all its suppliers and customers. Whereas cyber security only considers security of a technical nature, CSCRM attempts to encompass both managerial and human factors in preventing risks from disrupting IT systems' operations. [1]

Section two will go on to talk about compliance in cyber security, cyber crime, supply chains and the impacts of security breaches on businesses. Section three will look at use cases, requirements, risks and functionality for the proposed application. Section four will give an overview of the work completed so far, and the work remaining.

1.2 Problem

Keeping track of each company's compliance to a specific standard is a lengthy and potentially expensive task since it can be very difficult to maintain without the use of an external service or consultant. Due to the time and experience level required, it is unlikely to be something a system administrator will be able to do on top of their other responsibilities, and a specialist will, in all likelihood, be too expensive for most SMEs.

1.3 Aim

An automatically-generated cyber security compliance engine, could provide a low cost, time efficient solution for businesses that need a flexible, customisable way of tracking their partner's compliance - or their own compliance - with multiple standards.

The goal of this project is to create a client-server system that will generate and store compliance forms for the end-user. The forms will be automatically generated via an interface on the application by a user, and accessible by ‘partners’. Partners will be other users that can be added by the primary user, much like friends or followers on a social media application. Users will be able to update the forms’ parameters, and partners will be able to update their answers to the forms, at a later date. This project is a cloud-based application, and it will deal with cyber security compliance only - no other forms of compliance will be within the scope of this project.

BACKGROUND AND LITERATURE REVIEW

2.1 Compliance

Compliance is an important, expensive, and complex problem to deal with. [2] It relates to the conformance to a set of laws, regulations, policies or best practices. [2] These sets of rules are known as standards. Organisations can be required to take steps to put policies and controls in place that ensure conformity with the regulations outlined in their given compliance standard(s), the purpose of which is to safeguard the organisation against security threats.

2.1.1 Compliance in Cyber Security

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. [1] Cyber security standards have existed for a long time, affecting the necessary policies and practices of individuals and organisations over the last several decades. [3] Various regulations and legislation often struggle to keep up with the latest cyber threats due to the rapid evolution of the field. [4] As a result of the expanding pool of available tools, there is an ever-increasing number of people able to access the world of cyber crime. This makes it all the more crucial that conforming to the latest standards becomes an imperative for every company, regardless of the size of the enterprise. The hope for this project is that it will help to enable organisations to achieve compliance with any given standard in a cost effective manner.

2.1.2 Cyber Essentials

The UK Government worked with the a number of other institutions to develop Cyber Essentials, a set of basic standards to help organisations defend themselves from common security threats online. [5] The scheme is designed to prevent unskilled individuals from being able to find basic vulnerabilities in an organisation by providing advice, and two different levels of certification; “Cyber Essentials” and “Cyber Essentials Plus”. The former is a self-assessment designed to be light-weight and easy to follow, while in the latter, a certification body carries out the verification of the organisation’s cyber security, instead of it being done by the company in question.

2.2 Crime

There has been a significant increase in cyber criminal activity in recent years. [4] The methods used by criminals are currently changing as businesses begin to be targeted more frequently than individuals. [4] Cyber crime is growing at a rapid rate, making it increasingly troublesome for regulations and legislation to keep pace, resulting in outdated laws that are often unfit for purpose. [4]

2.3 Supply Chains

Supply chain management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. [1] It includes all logistics management activities as well as manufacturing operations, and it drives coordination of processes and activities within and across marketing, sales, product design, finance, and information technology. [1]

2.3.1 Supply Chain Security

Supply chain security focuses on the potential threats associated with an organisation’s suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organisation’s customer environments - some of which may be sensitive in nature. [6]

2.4 Impacts

Cyber attacks are financially devastating and disrupting to people and businesses. Successful attacks have the potential to expose personal information, leaving the victims of these security breaches vulnerable to fraud. [7] Victims are also left vulnerable to further attacks, using the information previously gathered by attackers.

2.4.1 The Effect on Business and Loss of Confidence

According to a survey by Ping Identity (a company that sells a number of cloud and software identity security solutions), 75% of people stop engaging with a brand online following a data breach, as well as 59% saying they were not willing to sign up to use an online service or application that had recently experienced a data breach. [8] In spite of this, 56% said they are not willing to pay anything to application or online service providers for added security to protect their personal information. [8]

2.4.2 Legal consequences

GDPR requires proper management of all the personal information held by an organisation. [9] If this information is compromised, and that organisation has neglected to deploy basic security measures, it is possible they will face fines and regulatory sanctions. [9]

2.5 Case Study: Pouring Pounds Ltd

Two cashback sites owned by Pouring Pounds Ltd were found to have leaked two terabytes worth of personally identifiable information and account data. This was made possible because of an unprotected database, which could be accessed through an exposed port on the company's server. The leak occured in October 2019 and has affected approximately 3.5 million individuals. [10]

REQUIREMENTS AND ANALYSIS

This section will analyse the requirements of the proposed application and inform the design decisions that have been made.

3.1 Use Cases

Use cases describe the various interactions between external actors and a given system as part of the Unified Modelling Language (UML). They are used in this section to define the interactions between users and the proposed application.

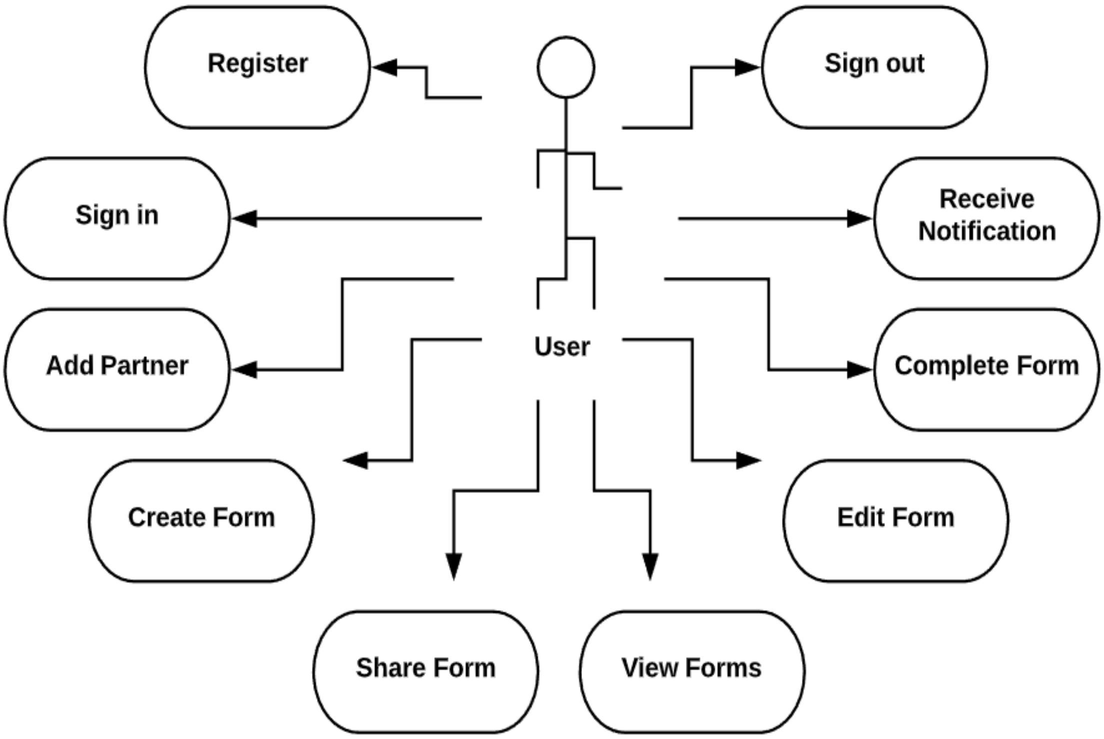

Figure 3.1: Use Case Diagram 1

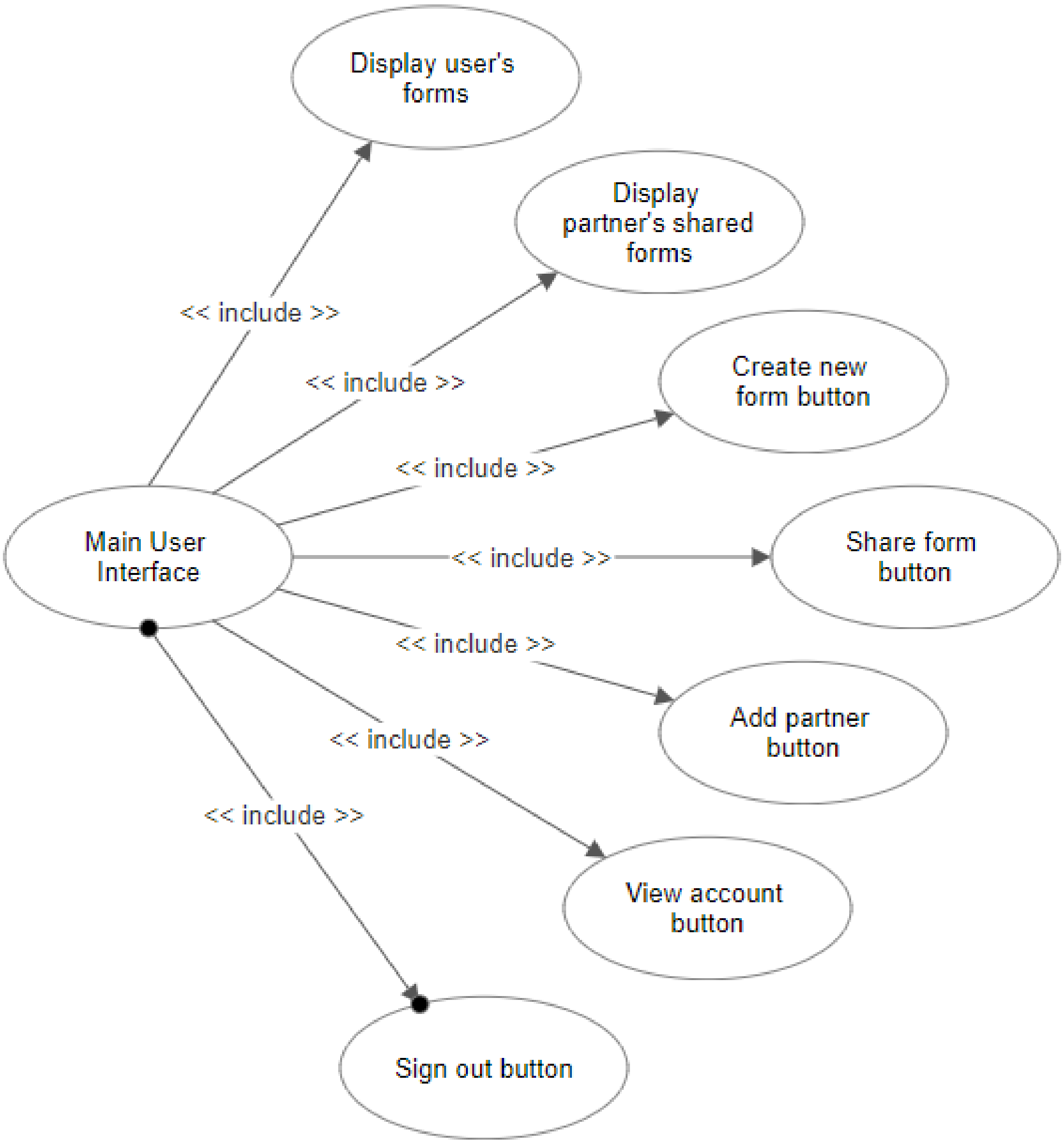

Figure 3.2: Use Case Diagram 2

3.1.1 Use Case Description

The following table explains the major use cases for the application:

Use Case	Description
Display user's forms	A list of forms created by the user will be displayed, with the form's name, owner and date of last modification.
Display partner's shared form	A list of forms shared with the user by a partner will be displayed, with the form's name, owner and date of last modification.
Create new form button	Takes the user to a page where they can design a new form.
Share form button	Allows the user to share forms they have created with partners.
Add partner button	Allows the user to search for other people's accounts on the application, and add them as partners. This should be done with other users that one would wish to share forms with and/or receive forms from.
View account button	Allows the user to view their account information and edit it if necessary. Details such as name, email, company and the abilityto change the account's password.
Sign out button	Allows the user to sign out from the application.

Table 3.1: Use Case Descriptions

3.2 Functional Requirements

A functional requirement defines the intended behaviour of a component or part of a system. In the table below, the major functional requirements have been described:

Requirement	Description
Register	New users will create an account before being allowed to use the application.
Sign in	Users will need to log in before they are able to access their account, create, share and complete forms.
Create a form	Users will be able to create a new form, which will be saved to their account.
Share a form	Users will be able to share a form that they have created with a partner.
Add a partner	Users will be able to view and edit their account information, including; name, email, company and password (not viewable).
Sign out	Users will be able to sign out of the application.
Notifications	Users will be notified of various changes, including their partners' answers to forms.

Table 3.2: Functional Requirements

3.2.1 Functional Requirements Analysis

An importance level has been assigned to each of the functional requirements, in order to effectively plan the work to be done in order to create the minimum viable product. An additional table shows how the importance levels have been determined.

Complexity/Time	Low	Medium	High
Short	0.0625	0.125	0.25
Medium	0.125	0.25	0.5
Long	0.25	0.5	0.75

Table 3.3: Importance Levels

Requirement	Complexity	Time	Importance Level
Register	Medium	Short	0.125
Log in	Low	Short	0.0625
Create a form	Medium	Medium	0.25
Share a form	High	Medium	0.5
Add a partner	Medium	Medium	0.25
Sign out	Low	Low	0.0625
Notifications	Medium	Short	0.125

Table 3.4: Functional Requirements Analysis

3.3 Non-Functional Requirements

Non-functional requirements are high-level requirements, that need to be considered during the development decisions for the entire application.

Requirement	Description
Internet connection	The application will be hosted online, therefore users will require a connection to the internet in order to access the application.
Confidentiality	The application will need to keep the personal information of its users safe from third parties and malicious individuals.
Integrity	The application must present accurate information in an easy-to-understand format.
Availability	The application must be accessible at all times. Loss of Availability could lead to users leaving the application for more reliable competitors.

Table 3.5: Non-Functional Requirements

3.4 Risk Analysis

The following risk analysis has been produced, based on the requirements above and potential risks to the application as a whole. A rating system, similar to that of the importance levels for the functional requirements, has been devised for the risk level.

Consequence/Likelihood	Negligible	Minor	Moderate	Major	Catastrophic
Impossible	0	0	0	0	0
Low	0	0.0625	0.125	0.1875	0.25
Medium	0	0.125	0.25	0.375	0.5
High	0	0.1875	0.375	0.5625	0.75
Certain	0	0.25	0.5	0.75	1

Table 3.6: Risk Levels

Risk	Likelihood	Consequence	Risk Rating	Mitigation
Network loss	High	Minor	0.1875	Frequent update of database.
Data loss	Low	Catastrophic	0.25	Redundant database.
Security breach	Medium	Catastrophic	0.5	Follow good practice for secure deveopment of cloud applications.
Function error	High	Major	0.5625	Implementation of test framework to ensure application is fully functional.
Interface error	High	Major	0.5625	Implementation of test framework to ensure application is fully functional.

Table 3.7: Risk Analysis

3.5 Functionality

Below is a series of diagrams which describe the flow of some of the primary pieces of functionality in the application. They show the logic behind various aspects of the application, as well as some of the infrastructure that will be in place.

3.5.1 Activity Diagrams

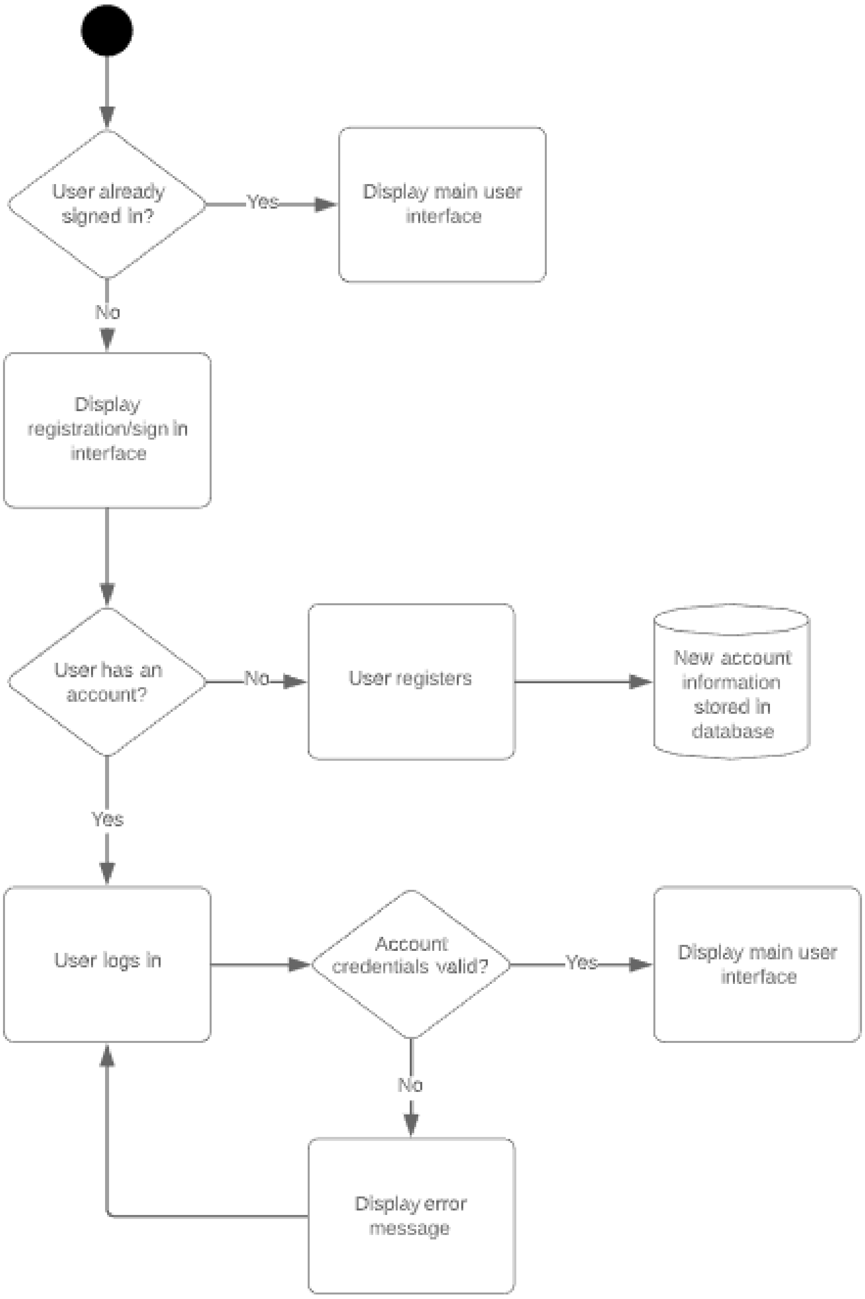
User already signed in?
Yes
Display main user interface
No
Display registration/sign in interface
User has an account?
No
User registers
New account information stored in database
Yes
User logs in
Account credentials valid?
Yes
Display main user interface
No
Display error message

Figure 3.3: Activity Diagram: Authentication

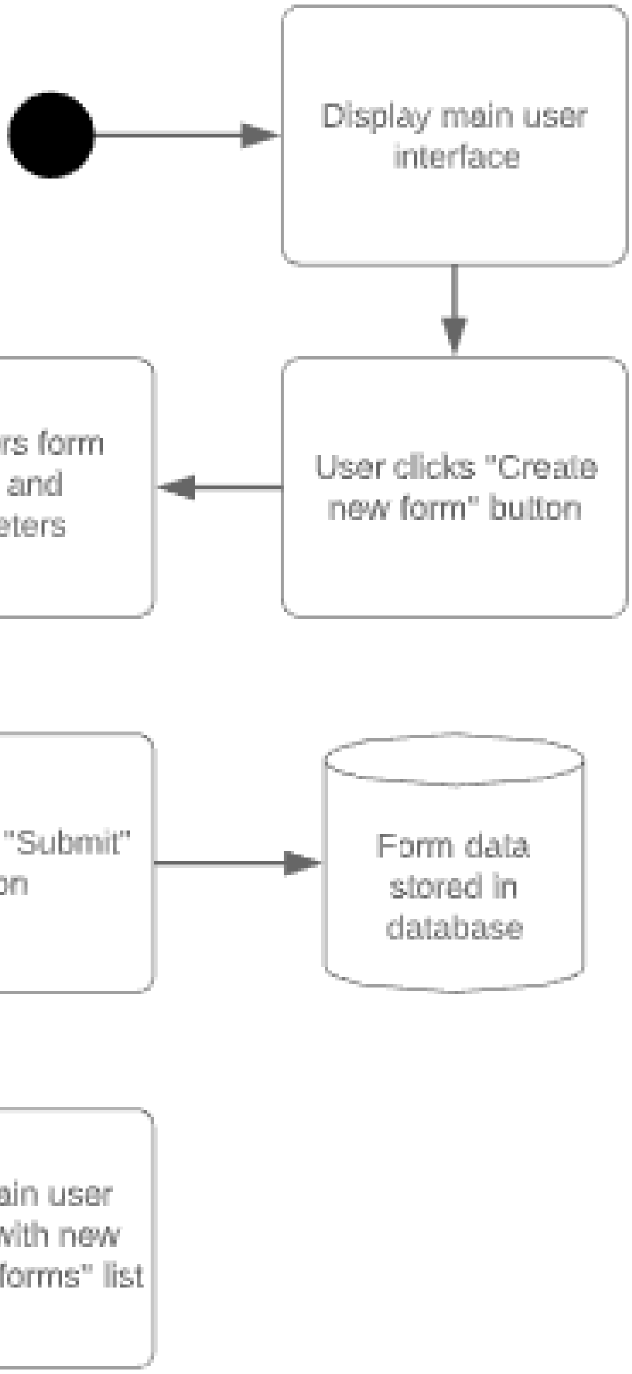
Display main user interface
User clicks "Create new form" button
User enters form details and parameters
User clicks "Submit" button
Form data stored in database
Display main user interface, with new form in "My forms" list

Figure 3.4: Activity Diagram: Form Creation

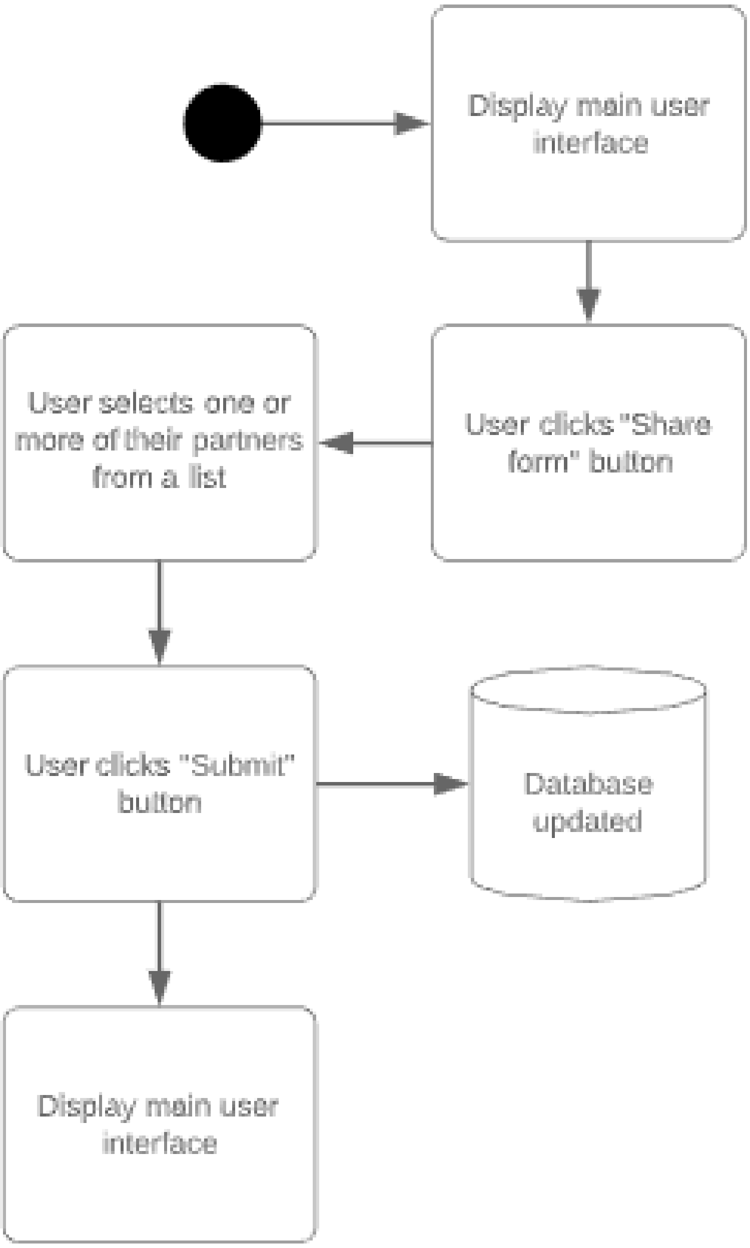
Display main user interface
User clicks "Share form" button
User selects one or more of their partners from a list
User clicks "Submit" button
Database updated
Display main user interface

Figure 3.5: Activity Diagram: Form Sharing

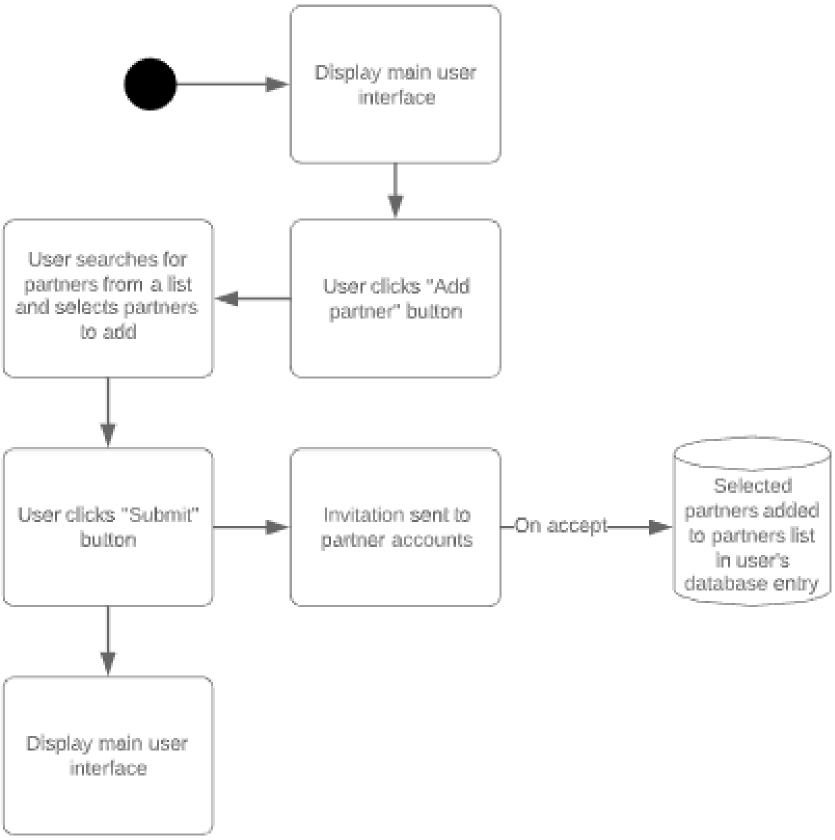
Display main user interface
User clicks "Add partner" button
User searches for partners from a list and selects partners to add
User clicks "Submit" button
Invitation sent to partner accounts
On accept
Selected partners added to partners list in user's database entry
Display main user interface

Figure 3.6: Activity Diagram: Partner Invitation

3.5.2 Model-View-Controller Diagram

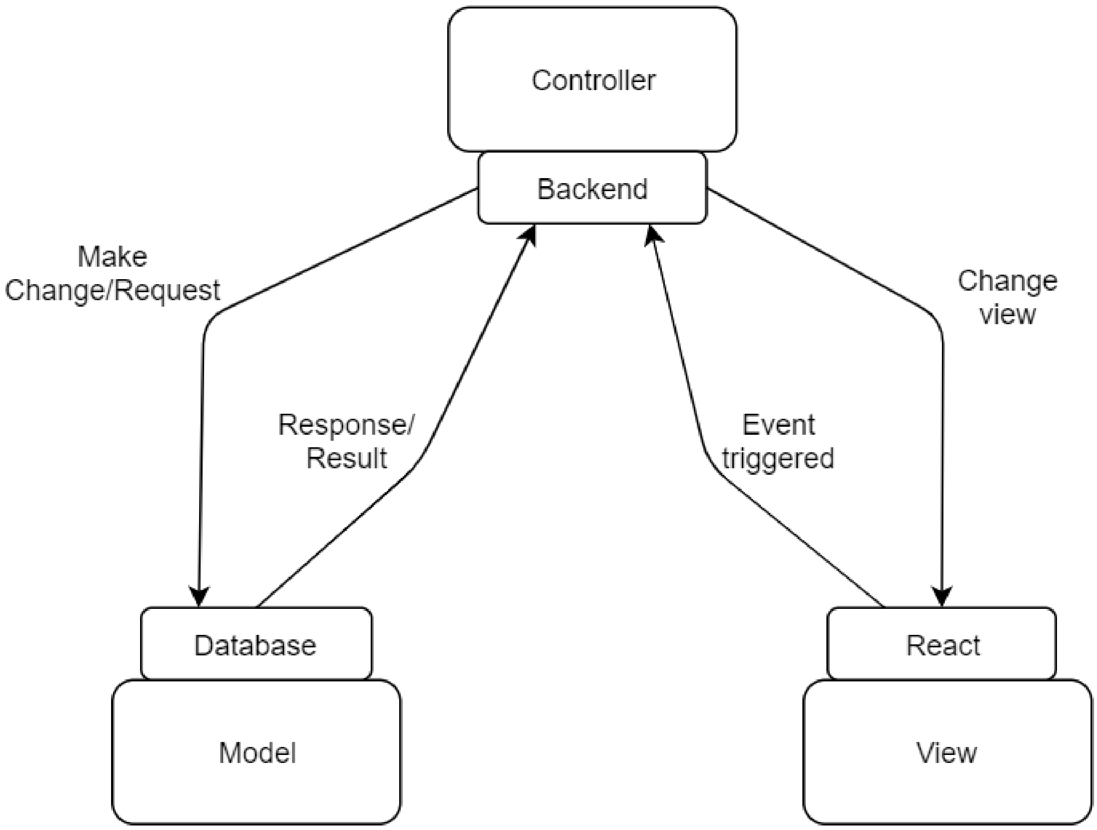

Figure 3.7: MVC Diagram

3.6 Validation

The testing and validation of the application will be done using Robot Framework. Robot Framework is a generic, open source, automation framework for acceptance testing [11], developed with Python. The framework has many libraries that extend its functionality, and one such library is Selenium, which will be used extensively to automatically drive the application's user interface. These tests will be written in conjunction with the application's features, and run alongside each check-in, as per the continuous integration methodology.

WORK COMPLETED AND REMAINING

4.1 Work to Date

At the time of writing, the project has just finished its design phase and will shortly be moving into implementation. So far, extensive background reading into compliance, cyber security, supply chains and cyber crime has been conducted, including the impacts and consequences of successful cyber attacks. A problem area has been identified in the cost of conforming to compliance standards, and the difficultly of SMEs in achieving said compliance. From this, a solution has been proposed, a list of requirements devised and a series of designs for the functionality of the solution have been produced.

4.2 A Plan for the Work Remaining

Remaining work includes the implementation of the application, the testing and validation of the completed product, and composing the final report. A plan of the all the work to be done has been made in the form of a Gantt chart, shown overleaf.

		October	November	December	January	February	March	April
Project Brief		▓						
	Background Research	░						
	Write up	░						
Time Management Planning		▓	▓	▓				
	Final Gantt Chart	░	░	░				
Research		▓	▓	▓				
	Further background research	░	░					
	Literature review		░	░				
Design			▓					
	Planning diagrams		░					
Progress Report			▓	▓				
	Write up		░	░				
Implementation				▓	▓	▓		
	Account creation (Register)			░				
	Sign in			░				
	Add a partner			░	░			
	Create a form				░			
	Share a form				░			
	Sign out				░	░		
	Notifications					░		

Table 4.1: Gantt Chart

		October	November	December	January	February	March	April
Testing and Validation					▓	▓		
	Robot Framework setup				░			
	Test Implementation				░	░		
Final Report					▓	▓	▓	▓
	Introduction				░			
	Background and Literature Review				░			
	Designs				░			
	Implementation				░	░		
	Testing and software validation					░	░	
	Results and Analysis					░	░	
	Evaluation						░	░
	Project management						░	░
	Conclusions						░	░
	Future work							░
	Bibliography							░
	Appendices							░
Project Viva								▓
	Viva							░

Table 4.2: Gantt Chart cont.

Bibliography

[1] S. Boyson, “Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems.” [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166497214000194

[2] S. et al., “Aiding compliance governance in service-based business processes,” in *Handbook of Research on Service-Oriented Systems and Non-Functional Properties: Future Directions*, 2012, pp. 524–548. [Online]. Available: https://www.igi-global.com/chapter/handbook-research-service-oriented-systems/60900

[3] e. a. Elliott, “Consrotium for research on information security and policy,” 1998-2001. [Online]. Available: https://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy

[4] J. Zerlang, “Gdpr: a milestone in convergence for cyber-security and compliance,” 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485817300600

[5] GOV.UK, “Cyber essentials scheme: Overview,” 2014. [Online]. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[6] D. Shackleford, 2015. [Online]. Available: https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_273005.pdf

[7] N. C. Agency, “Cyber crime.” [Online]. Available: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

[8] I. Governance, “Customers lose confidence - data breaches aren’t just about fines,” 2018. [Online]. Available: https://www.itgovernance.co.uk/blog/customers-lose-confidence-data-breaches-arent-just-about-fines

[9] p. b. I. N. I. nibusinessinfo.co.uk, “Cyber security for business.” [Online]. Available: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

[10] z6mag, “Two cashback sites leaked data of 3.5 million users.” [Online]. Available: https://z6mag.com/2019/10/16/two-cashback-sites-leaked-data-of-3-5-million-users/

[11] R. F. Foundation. [Online]. Available: https://www.robotframework.org/