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: TBD

Automatically Generated Cyber Security Compliance Engine

by James D'Alton

30 November 2019

There are hundreds of cyber security compliance standards, and many businesses require their partners to comply with numerous standards. ”Unlike cybersecurity alone, cyber supply chain risk management focuses on gaining visibility and control not only over the focal organization but also over its extended enterprise partners, such as Tier 1/Tier 2 suppliers and customers. In addition, while cybersecurity emphasizes purely technical means of control, CSCRM seeks to engage both managerial and human factors engineering in preventing risks from disrupting IT systems operations.”(Boyson, S. (2014) Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems, Technovation, 34(7), pp. 342–353.) Keeping track of each companys compliance to a particular 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. (”Says who?”)

Most SMEs will not be able to afford this - due to the time and experience level required, it might not be something a system administrator can do on top of their other responsibilities, and a consultant might be too expensive.(”Says who?”)

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 partners compliance, or their own compliance, with multiple standards.(”Says who?”)

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 an admin, and accessible by users. This will include the ability to update the forms at a later date. This project is a client-server system only, not an application, and it will deal with cyber security compliance only - no other forms of compliance will be within the scope of this project.

Contents

List of Figures

List of Tables

Chapter 1

Project Description

1.1 Project Overview

There are hundreds of cyber security compliance standards, and many businesses require their partners to comply with numerous and varied standards. "Unlike cybersecurity alone, cyber supply chain risk management focuses on gaining visibility and control not only over the focal organization but also over its extended enterprise partners, such as Tier 1/Tier 2 suppliers and customers. In addition, while cybersecurity emphasizes purely technical means of control, CSCRM seeks to engage both managerial and human factors engineering in preventing risks from disrupting IT systems'operations."[?] Keeping track of each company's compliance to a particular 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.

Most SMEs will not be able to afford this - due to the time and experience level required, it might not be something a system administrator can do on top of their other responsibilities, and a consultant might be too expensive.

1.2 Project 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 an 'admin', and accessible by 'users'. This will include the ability to update the forms at a later date. This project is a client-server system only, not an application, and it will deal with cyber security compliance only - no other forms of compliance will be within the scope of this project.

Chapter 2

Background and Literature Review

2.1 Compliance

2.1.1 What is Compliance?

Compliance generally refers to the conformance to a set of laws, regulations, policies, best practices, or service-level agreements. Compliance governance refers to the set of procedures, methodologies, and technologies put in place by a corporation to carry out, monitor, and manage compliance. Compliance governance is an important, expensive, and complex problem to deal with. (Silveira, P. et al. (2012) Aiding Compliance Governance in Service-Based Business Processes, in Handbook of Research on Service-Oriented Systems and Non-Functional Properties: Future Directions, pp. 524548.)

2.1.2 Compliance in Cyber Security

Cybersecurity standards have existed over several decades as users and providers have collaborated in many domestic and international forums to effect the necessary capabilities, policies, and practices - generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s. (National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.)

2.2 The State of Compliance in the UK: Cyber Essentials

2.2.1 Cyber Essentials

The Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls to help organisations protect themselves against common online security threats. (Cyber Essentials Scheme: overview (2014) GOV.UK.)

2.2.2 Crime

We have seen a significant growth in cyber criminality in the form of high-profile ransomware campaigns over the last year. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud, while lives were put at risk and services damaged by the WannaCry ransomware campaign that affected the NHS and many other organisations worldwide. Tactics are currently shifting as businesses are targeted over individuals. (Cyber Crime (no date) NCA National Crime Agency.)

2.3 Supply Chains

2.3.1 Supply Chain Management

2.3.2 Supply Chain Security

Supply chain security is a program that focuses on the potential risks associated with an organizations suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organizations customer environments, some of which may be sensitive in nature. (Shackleford, D. (2015) Combatting Cyber Risks in the Supply Chain. SANS Whitepaper.)

2.4 Impacts

2.4.1 Security Breaches

Cyber attacks are financially devastating and disrupting and upsetting to people and businesses. (Cyber Crime (no date) NCA National Crime Agency.)

2.4.2 Loss of Confidence

2.4.3 Effect on Business

2.5 Case Studies(?)

Chapter 3

Requirements and Analysis

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

3.1 Use cases

Explanation

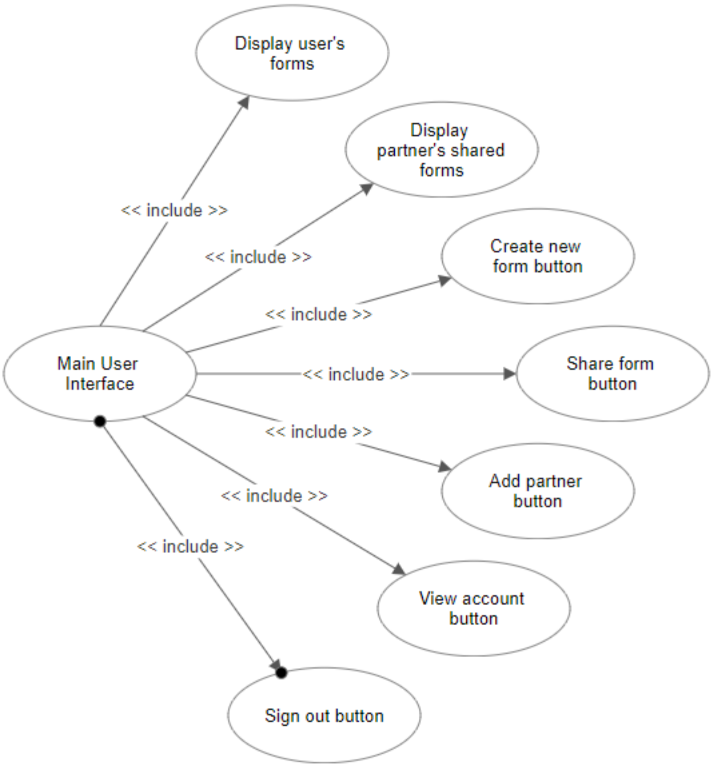

Figure 3.1: Use Case Diagram 1

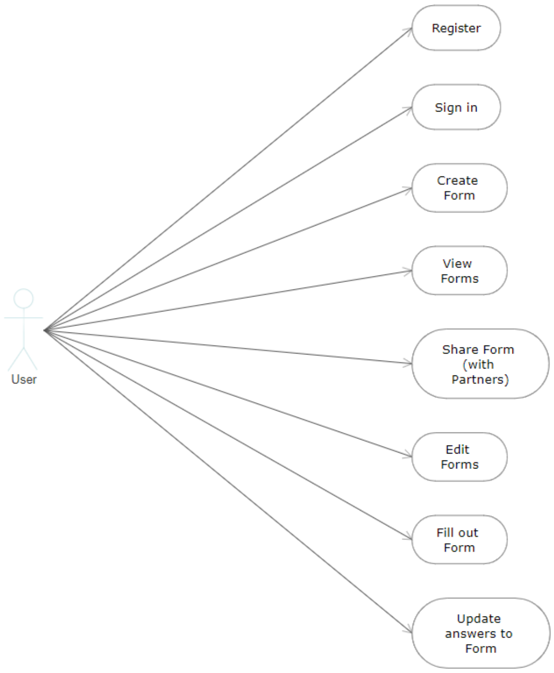

Figure 3.2: Use Case Diagram 2

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

Explanation

Requirement	Description
Register	New users will create an account before being allowed to use the application.
Log 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

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: Requirements analysis

3.3 Non-functional requirements

Explanation

table

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.

Table 3.5: Non-functional requirements

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	Low	Catastrophic	0.25	Follow good practice for secure deveopment of cloud applications.
Function error	Medium	Major	0.375	Implementation of test framework to ensure application is fully functional.
Interface error	Medium	Major	0.375	Implementation of test framework to ensure application is fully functional.

Table 3.7: Risk Analysis

3.4 Risk analysis

Explanation

tables

3.5 Functionality

3.6 Justification of the Approach (?)

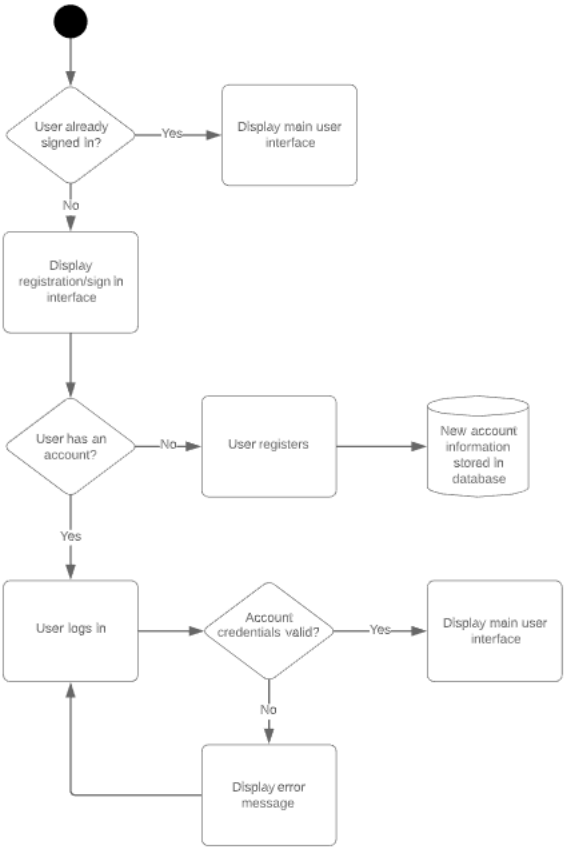
User already signed in?
Yes
Display main user interface
No
Display registration/sign in interface
User has an account?
No
User registers
New account information stored in database
Yes
User logs in
Account credentials valid?
Yes
Display main user interface
No
Display error message

Figure 3.3: Activity Diagram: Authentication

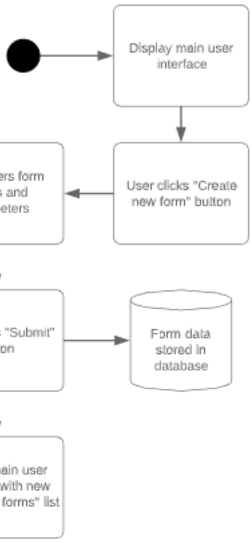
Display main user interface
User clicks "Create new form" button
User enters form details and parameters
User clicks "Submit" button
Form data stored in database
Display main user interface, with new form in "My forms" list

Figure 3.4: Activity Diagram: Form Creation

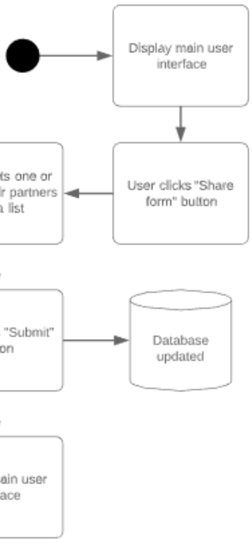
Display main user interface
User clicks "Share form" button
User selects one or more of their partners from a list
User clicks "Submit" button
Database updated
Display main user interface

Figure 3.5: Activity Diagram: Form Sharing

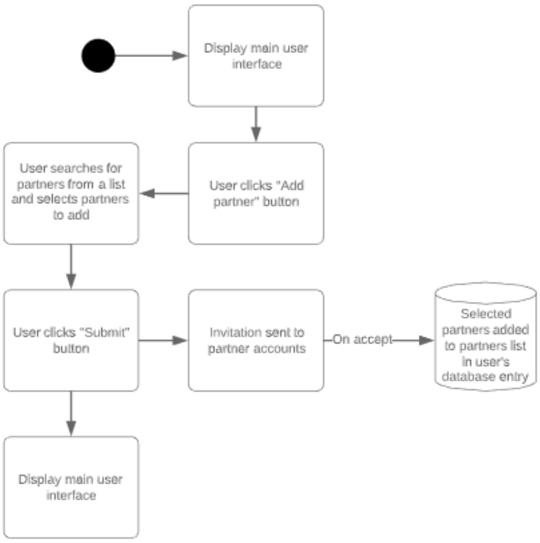
Display main user interface
User clicks "Add partner" button
User searches for partners from a list and selects partners to add
User clicks "Submit" button
Invitation sent to partner accounts
On accept
Selected partners added to partners list in user's database entry
Display main user interface

Figure 3.6: Activity Diagram: Partner Invitation

Chapter 4

Conclusions

It works.