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

Abstract

Abstract goes here.

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 [specifications]. Cyber supply chain risk management (CSCRM) differs from cyber security, by means of gaining a higher degree of governance over the company in question, and also 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] 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 is unlikely to be something a system administrator will be able to do on top of their other responsibilities, and a consultant will, in all likelihood, 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 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 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.

Chapter 2

Background and Literature Review

2.1 Compliance

2.1.1 What is Compliance?

Compliance relates to the conformance to a set of laws, regulations, policies or best practices. Compliance is an important, expensive, and complex problem to deal with. [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 the given compliance standard(s). The purpose of the compliance standards is to safeguard the organisation against security threats.

2.1.2 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]

2.1.3 Compliance in Cyber Security

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 legislation and regulations often struggle to keep up with the latest cyber threats due 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 each enterprise. The hope for this project is that it will enable organisations to achieve this in a cost effective manner.

2.2 The State of Compliance in the UK

2.2.1 Cyber Essentials

The UK 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. [5] The scheme is design to prevent unskilled individuals from being able to find basic vulnerabilities in an organisation, by providing advice and 2 levels of certification; "Cyber Essentials" and "Cyber Essentials Plus". The former is a self-assessment designed to be light-weight and easy to follow, the latter is similar, but the verification of the organisation's cyber security is carried out by a certification body instead of the organisation itself.

2.2.2 Crime

We have seen a significant increase in cyber criminal activity in recent years. The methods used by criminals are currently changing as businesses begin to be targeted more frequently than individuals. 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

2.3.1 Supply Chain Management

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. 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]

2.3.2 Supply Chain Security

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

2.4 Impacts

2.4.1 Security Breaches

Cyber attacks are financially devastating and disrupting to people and businesses. Security breaches have the potential to leak personal information on a large scale, leaving victims vulnerable to fraud [7] and further attacks using the information gained by attackers, which could be sold on to others.

2.4.2 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 would 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 recently experienced a data breach. However, 56% said they are not willing to pay anything to application or online service providers for added security to protect their personal information. [8]

2.5 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

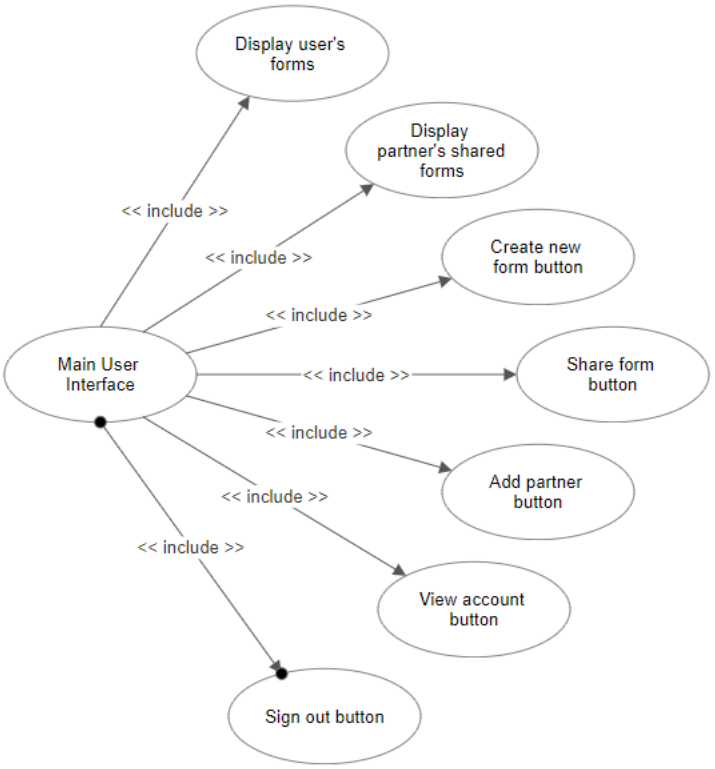

Figure 3.1: Use Case Diagram 1

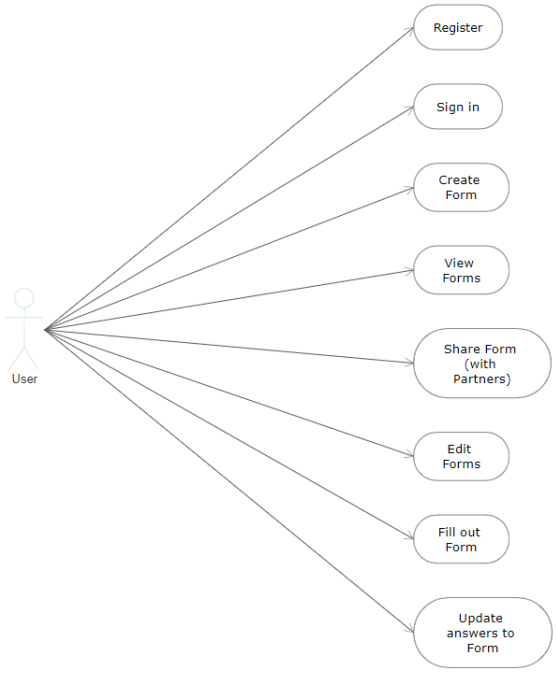

Figure 3.2: Use Case Diagram 2

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 (?)

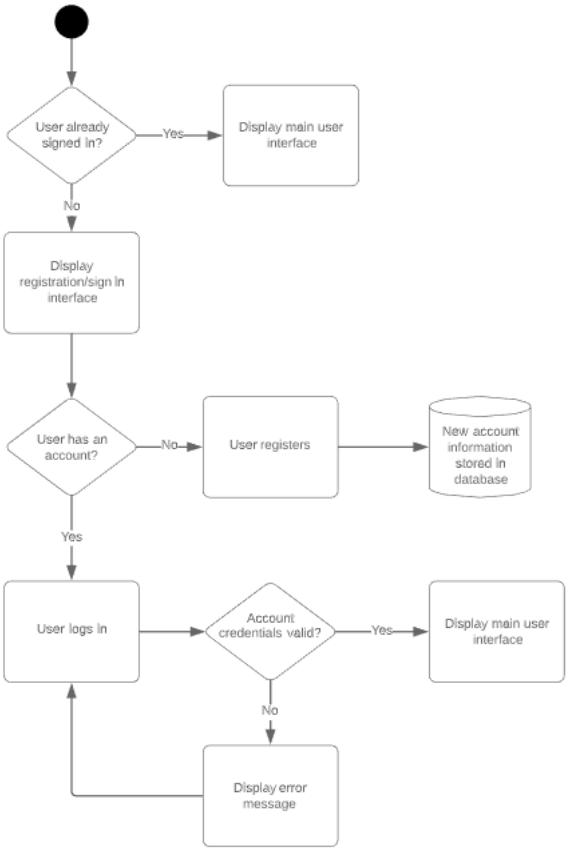

Figure 3.3: Activity Diagram: Authentication

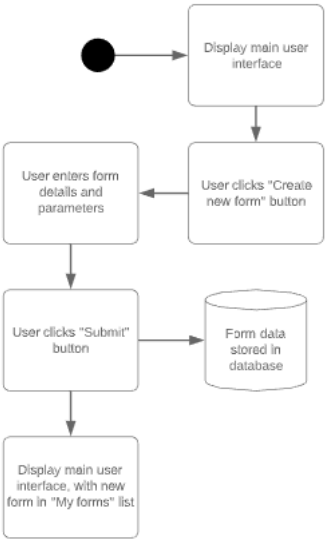

Figure 3.4: Activity Diagram: Form Creation

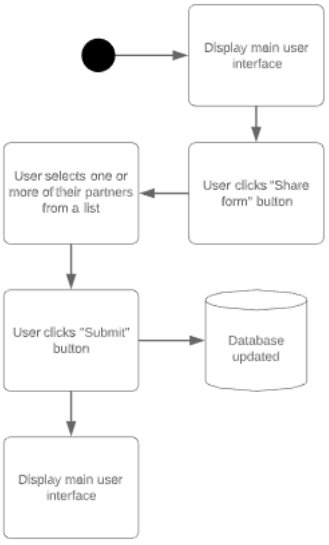

Figure 3.5: Activity Diagram: Form Sharing

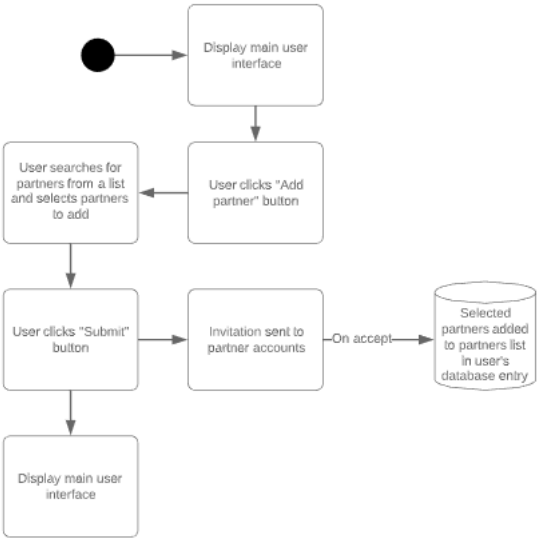

Figure 3.6: Activity Diagram: Partner Invitation

Chapter 4

Conclusions

It works.

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