SECURITY CULTURE DASHBOARD
PROOF OF CONCEPT

UNIVERSITY OF CHICHESTER

1806510

Submitted to the University of Chichester’s Business School as part of the Digital and Technology Solutions Professional (Software Engineer) Degree Apprenticeship.

2022

Abstract

SSE plc has recently undergone a significant transformation in Cyber Security culture, and with increased maturity comes a desire to track and monitor key metrics. The Security Culture Dashboard Proof of Concept was a project delivered for SSE's Cyber Risk and Information Security team, which aimed to provide an artefact that demonstrated how metrics and data generated from internal processes could be manipulated and presented in a clear, concise, and structured manner, eliminating existing manual tasks.

Acknowledgements

I would first like to thank SSE's Security Culture Lead, Mike Whittle, for his continuous support and guidance since early 2021, including during this project. Mike has provided me with invaluable skills, both professionally and personally, which have helped shape my interest in Cyber Security.

Secondly, to my project supervisor and apprenticeship programme lead, Paul Kooner-Evans, thank you for the ongoing support over the last four years.

Finally, to my friends, family, and girlfriend, Aislin, thank you for your support and encouragement throughout the last four years. The apprenticeship journey has undoubtedly been challenging and couldn't have been completed without you.

Security Culture Dashboard Proof of Concept

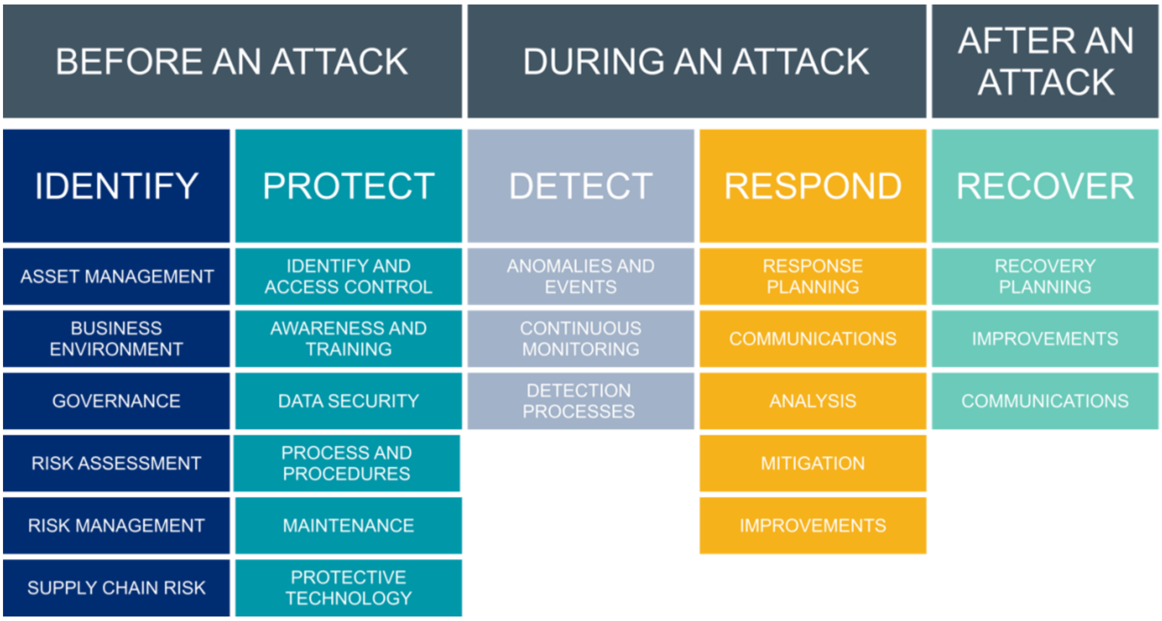
Table of Contents

1 Introduction

1.1 Organisational Background

SSE plc, the client of this project, is a leading generator of renewable electricity in the UK and Ireland and one of the largest electricity network companies in the UK (SSE, 2022). At the time of writing, SSE employs more than 12,000 staff across their seven business units and, in 2021, had an adjusted profit before tax of £1,064.9m (SSE, 2021).

SSE IT is the Information Technology division of SSE that underpins all seven business units by providing core IT services. In SSE's 2020/21 Group Risk Report (SSE, 2021), Cyber Security and Resilience was outlined as SSE's second highest principal risk, second only to politics, regulation, and compliance. The Cyber Risk and Information Security (CRIS) team within SSE IT provides essential cybersecurity functions to address this risk. In addition, the CRIS team directly align their services with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (National Institute of Standards and Technology, 2022), Figure 1.1, to enable long-term Cyber Security and Risk Management.



BEFORE AN ATTACK		DURING AN ATTACK		AFTER AN ATTACK
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
ASSET MANAGEMENT	IDENTIFY AND ACCESS CONTROL	ANOMALIES AND EVENTS	RESPONSE PLANNING	RECOVERY PLANNING
BUSINESS ENVIRONMENT	AWARENESS AND TRAINING	CONTINUOUS MONITORING	COMMUNICATIONS	IMPROVEMENTS
GOVERNANCE	DATA SECURITY	DETECTION PROCESSES	ANALYSIS	COMMUNICATIONS
RISK ASSESSMENT	PROCESS AND PROCEDURES		MITIGATION	
RISK MANAGEMENT	MAINTENANCE		IMPROVEMENTS	
SUPPLY CHAIN RISK	PROTECTIVE TECHNOLOGY			

Figure 1.1 - NIST Cybersecurity Framework

In 2018, the Security Culture programme was set up within the CRIS team to directly tackle the Awareness and Training component of the Protect function, as defined by the NIST Cybersecurity framework. The programme's mission statement is to "Provide SSE colleagues with the awareness, training, education and tools to do our jobs in a safe and secure manner, therefore protecting SSE systems and data from harm."

Over time, the Security Culture programme has developed several metrics through which the cyber resilience of SSE's colleagues is measured. The two fundamental processes that produced these metrics at project initiation were Phishing Resilience and Password Management.

The Security Culture team has manually tracked their key metrics for the past four years, using spreadsheets to collate and analyse data; while this is not inherently wrong, the process is time-consuming and prone to human error. Additionally, statistics are collected and presented to key stakeholders each month in a repeatable fashion. It was therefore identified that this was a prime area for improvement.

1.2 Project Definition and Scope

To address the previously highlighted issues, the Security Culture team wanted to explore their options and understand what was possible when implementing a software solution that met their requirements – this is where the Security Culture Dashboard project came in.

The key aim of the Security Culture Dashboard project (SCD) was to:

> Develop and evaluate a software solution that collates and demonstrates key Security Culture metrics.

Building upon this aim, the following objectives were created:

1. **Delivery of a web dashboard interface** which can be run efficiently on hardware - desktops and laptops - deployed by SSE.
2. **Improved reporting experience** through the automatic creation of charts and reports based on pre-existing data formats.
3. **Delivery of a solution that incorporates researched best practices** for interface design, dashboard design and data visualisation.

As discussed in Appendix A – Project Initiation Document (p.37), the project scope would be limited according to five fundamental points. However, the most important point is that the SCD project would not use confidential data when demonstrating features and benefits. For the solution to be demonstrable both as an internal proof of concept and an academic project, all SSE data used must have a classification of Public or Internal.

2 Lifecycle and Methodology

2.1 Project Lifecycle

There are several appropriate approaches for a systems development project such as this. In his 2019 book, Effective Project Management, Wysocki presents five types of Project Management Lifecycles (PMLCs) by which projects can be operated. These are Linear, Incremental, Iterative, Adaptive and Extreme (Wysocki, 2019, p. 23).

As discussed in Appendix A – Project Initiation Document (pp. 34-36), the five lifecycles were assessed and analysed using Wysocki's five PMLCs matrix, Figure 2.1.

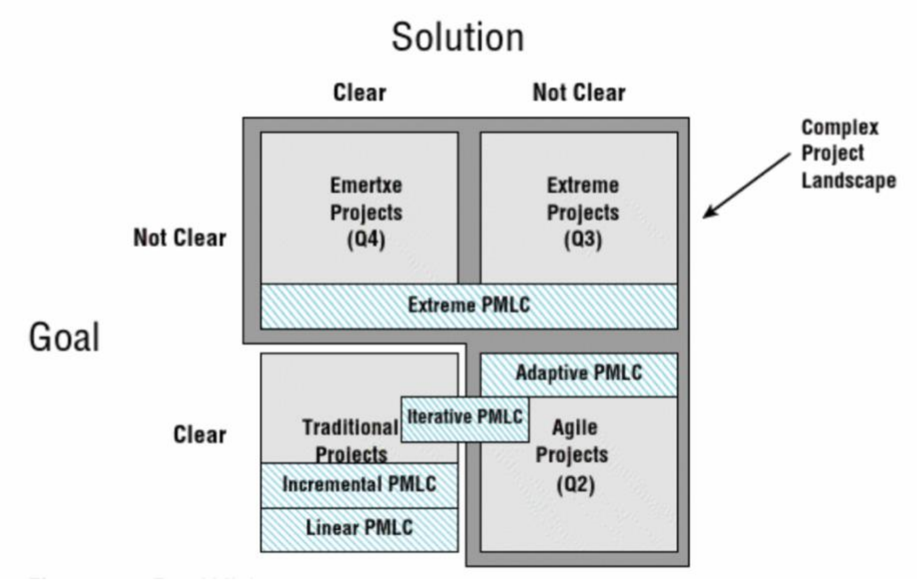


Figure 2.1 - Wysocki's five PMLC matrix (Wysocki, 2019, p. 39)

The aim (goal) of the SCD project was reasonably well defined; however, the solution was more open-ended due to the project being a proof of concept. Aligning these statements with Wysocki's matrix, Figure 2.1, resulted in the Iterative and Incremental PMLCs being considered for the project.

After thoroughly assessing which PMLC would be most appropriate for the SCD project, it was decided that an Iterative approach would be taken due to the creative freedom and learning and development opportunities that the lifecycle provided.

As examples for software development projects, Wysocki presents four models that follow an Iterative approach: Evolutionary Development Waterfall, Scrum, Rational Unified Process (RUP) and Dynamic Systems Development Method (DSDM) (Wysocki, 2019, pp. 48-49). As the project team already had experience operating projects according to Scrum principles, it was decided that this was the methodology of choice. An overview of the Scrum approach to software development can be seen below in Figure 2.2.

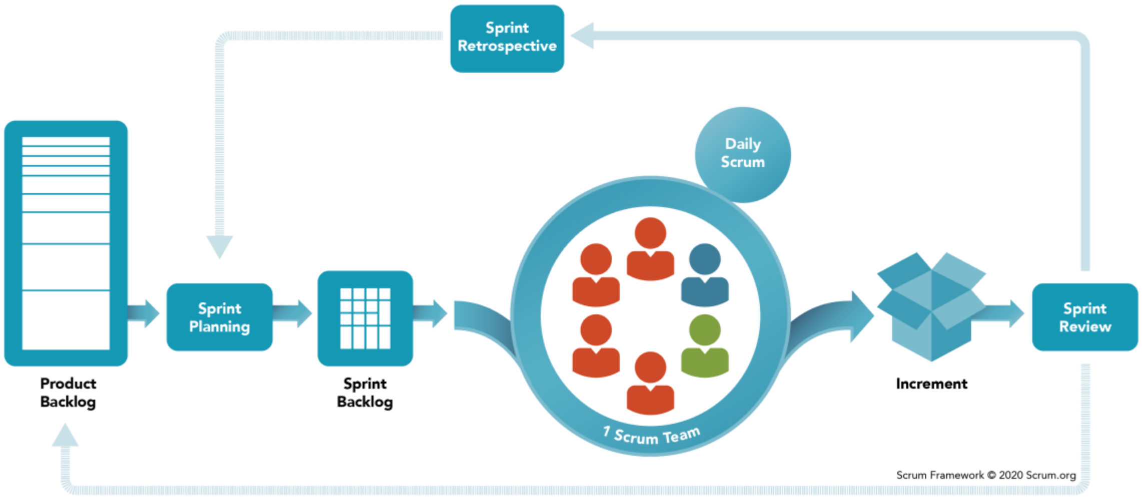


Figure 2.2 - The Scrum Framework (Scrum.org, 2022)

As outlined by Scrum Alliance (2022) and as seen above in Figure 2.2, the three core artefacts for a Scrum systems development project are:

1. A Product Backlog
2. Sprint Backlogs
3. Potentially releasable Product Increments

To ensure consistency of delivery, the project team would use all three Scrum artefacts throughout the project. Additionally, to enable effective high-level project management, several key documents from the Prince2 project management methodology (AXELOS Limited, n.d.) would be adopted, including a Project Initiation Document, Appendix A – Project Initiation Document, a Benefits Case, Appendix B – Initial Benefits Case and a Risk Register, Appendix D – Risk Log.

Additionally, within each sprint, the project team would follow the standard systems development lifecycle (SDLC) outlined below in Figure 2.3.

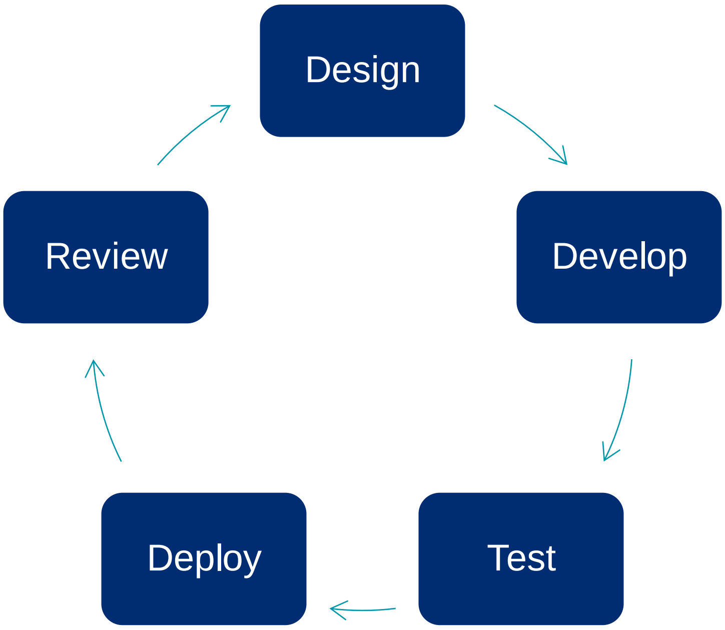


Figure 2.3 - Systems Development Lifecycle

2.2 Research, Analysis and Design Methodology

Before any research could be conducted for the project, ethical approval was sought from the University of Chichester to confirm and validate the research approach, Appendix E – Application for Ethical Approval.

The SCD project primarily used a Qualitative approach to research collection through interviews with primary stakeholders. This was since there would only be one target user persona for the expected system - research for which could be gathered from the project's client. See

Appendix L – Client Interview Questions for the questions proposed to the client at the first project meeting. However, prior to gathering research, a consent form was collected from the client to ensure they knew how their gathered responses would be used, Appendix F – Signed Consent Form.

To aid the formation of the project's aims and objectives, a mixture of closed and open interview questions were presented to the client. As outlined by Susan Farrell (2016), open-ended questions promote answers with sentences, lists and stories, whereas closed-ended questions limit answers, resulting in more direct responses.

The system’s design was at the core of the SCD project, as highlighted in project objectives two and three. As such, a considered approach to design was taken.

2.2.1 User Experience

Understanding the client’s needs and aligning them to the business goals was a central component of the SCD project. In his book Designing for Emotion (2022), Aarron Walter outlines his Hierarchy of User Needs, Figure 2.4, and aligns them directly to the work of Abraham Maslow (Maslow, 1943). This hierarchy has been used to drive decision-making for the SCD’s user interface due to its direct relationship to needs and wants – see

Requirements Formulation for further details.

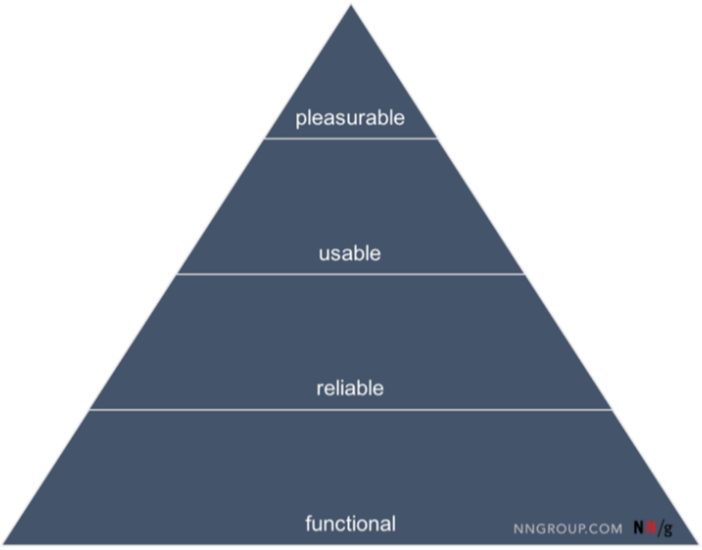


Figure 2.4 - Aaron Walter’s Hierarchy of User Needs (Walter, 2022) (Fessenden, 2017)

Additionally, relating to the key areas of interface design, data visualisation and dashboard design, theory from Google (2022), Tidwell et al. (2020) and Knaflic (2015) has been used extensively to ensure the solution contains current best practices.

2.2.2 Brand Identity

Brand identity is crucial to SSE, with the company having a 178-page guidelines document outlining the specifics for brand usage. By having a solid brand that captures who SSE are and what they do, they believe they can “make SSE a brand people want to buy from, partner with, invest in and work for” (SSE, 2020). The SSE brand guidelines document, Figure 2.5, underpinned all aspects of the SCD project and was an invaluable source for typography, assets, and colour guidelines.

Figure 2.5 - SSE Internal Brand Guidelines (SSE, 2020)

3 Specification of Requirements

3.1 Environmental Analysis

As previously outlined, SSE is a leading generator of renewable electricity in the UK and Ireland and is also a FTSE 100 company as of the project. Understanding the external context within which SSE operates is crucial to the business and this project, as it provides vital inputs to decision making. A PESTLE (Political, Economic, Social, Technological, Legal and Environmental) analysis was conducted for SSE to determine the relevant external factors, Table 3.1.

Political	Economic	Social
• Nationalisation • Brexit • Government backing of clean energy development • Potentially subject to politically motivated cyber attacks	• High commodity price volatility • Domestic price caps • Expansion to different countries/ economies • Protection of Critical National Infrastructure assets	• Fair Tax Mark • Living Wage employer • Significant economic impact • Investment in green technologies • Supporters of a 'Just Transition' • Need to be seen to be 'doing the right thing'
Technological	**Legal**	**Environmental**
• Development of green technologies • Deployment of smart grids/devices • Development of carbon-capture technology	• Health and Safety • Regulatory compliance • GDPR compliance • Business separation	• Transition to green energy sources • Protection of local wildlife populations

Table 3.1 - SSE PESTLE Analysis

As identified in the PESTLE analysis above, SSE has an inherent responsibility to protect the country's Critical National Infrastructure (CNI). This directly relates to the area of Cyber Security as CNI is increasingly becoming internet-connected, which can open it up to a vast array of attacks from anywhere in the world. For example, as recently as 2021, the Colonial Pipeline ransomware attack crippled a section of the

United States' oil pipeline infrastructure, resulting in a pipeline that supplied oil for half of the East Coast becoming unusable for five days (Kerner, 2022). Therefore, this provides significant external context for developing a strong security posture at SSE.

To analyse the internal context within which the SCD project would be developed, a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis was conducted for the Security Culture programme, Table 3.2.

Strengths	Weaknesses
• Solid record of campaign delivery • Clear future strategy • Strong senior stakeholder buy-in • Engaged network of champions	• Legacy/manual processes • Lack of resource • Unable to meet self-imposed expectations • Metrics not fully exploited • Content can be generic and not job-role specific
Opportunities	**Threats**
• Automation of manual processes • Further development of champions group • Enhanced exploitation of metrics for reporting and awareness • The hiring of additional resource • Expansion of the team to cover more areas of the NIST framework • Greater personalisation of content to different target personas	• Lack of budget/investment in the programme • Negative influencing factors such as impacting cyber-attacks or negative senior stakeholder attitudes • Change of direction imposed on the programme • Negative colleague attitudes • Lack of stakeholder support

Table 3.2 – SSE Security Culture programme SWOT

Taking both of the analyses into consideration, several of the key themes relating to the SCD project, including security awareness and culture, interface design and data visualisation, will be explored below in greater detail.

3.2 Security Awareness and Culture

As cyber-criminals increase their capabilities and organisations are exposed to an increasing number of threats, developing a security culture is a common tactic used by Information Security teams to keep their organisations secure. CPNI (Centre for the Protection of National Infrastructure) (2021) suggests that a security culture “refers to the set of values, shared by everyone in the organisation, that determine how people are expected to think about and approach security.”

The Security Awareness Special Interest Group (SASIG), a networking forum for security awareness professionals set up in 2004, had scaled from having only a dozen members when initially founded to several thousand in 2022 (SASIG Events Limited, 2022). This example demonstrates that the security awareness and culture field has expanded significantly over the past 18 years and is only continuing to grow.

As discussed by Spanning Cloud Apps (2022), according to Verizon’s 2021 data breach investigations report, 85% of security breaches involved the human element. Furthermore, Graphus (2021) identify that phishing attacks account for more than 80% of reported security incidents, highlighting the importance of the human element to cyber security. All issues outlined here can be tackled by providing sufficient user training, the effectiveness of which can be increased through targeted campaigns facilitated by measuring colleague activity and reporting on key metrics.

As outlined by Cisco in their 2007 white paper, Measuring and Evaluating an Effective Security Culture, according to a 2006 report published by the Centre for Digital Strategies at the Tuck School of Business at Dartmouth and the Institute of Information Infrastructure Protection, developing composite security metrics that are simple to understand and linked to the business was ranked as the primary imperative for security leaders at Fortune 500 firms.

In summary, this section details the importance of the SSE Security Culture team and highlights the need for sufficient metrics to aid decision-making. Therefore, the SCD project should strive to ensure the deliverable presents simple security culture metrics clearly and concisely, which can be enhanced by applying the best practices highlighted in the following sections.

3.3 Interface Design

The third project objective outlines that best practices must be incorporated into the interface’s design to ensure the solution is complete. Therefore, this section will briefly discuss interface design best practices and their implications for the SCD project.

In their 2020 book, Designing Interfaces: Patterns for Effective Interaction Design, Tidwell et al. dissect interface design into multiple components: designing for people, organising the content, getting around, and the layout of screen elements, among others. Whilst this list is not exhaustive, it has been included to demonstrate that multiple domains within Interface Design should all be considered.

While several of these domains are covered by the SSE Brand Guidelines document (SSE, 2020), in some instances, it was appropriate to override details either where insufficient detail was provided or where the project team determined that another solution would provide a better experience to the end user.

Material Design is an adaptable system produced by Google containing guidelines, components and tools that support best practices of user interface design, with the latest version being Material Design 3 (Google, 2022). As outlined by Fessenden (2021), the usage of design systems allows designs to be created quickly and reused at scale whilst also incorporating current best practices and allowing resources to focus on more complex issues. While there are vast numbers of alternative design systems, as highlighted by McGowan (n.d.) and Slant (2022), Material Design was selected as the design system of choice for the SCD project due to the breadth of guidelines and tools it provides, as well as the extensive developer ecosystem that surrounds it.

3.4 Data Visualisation

Like interface design, including data visualisation best practices was essential to the SCD project. Therefore, relevant literature and sources will be interrogated in this section to determine what this means for the project.

Storytelling with Data: a data visualization guide for business professionals, written by Cole Nussbaumer Knaflic (2015), provides straightforward guidelines for enhancing business data visualisations. Knaflic summarises the complex field of data visualisation into six key lessons:

1. Understand the context
2. Choose an appropriate visual display
3. Eliminate clutter
4. Focus attention where you want it
5. Think like a designer
6. Tell a story

In addition to Knaflic's lessons above, Material Design also provides guidelines for designing data visualisations (Google, 2022), distilling the advice into three principles: Accurate, Helpful and Scalable. To summarise these principles, according to Google, data visualisations should be accurate, clear, and concise, helpful with context and enable exploration, and scale to multiple device sizes without distortion.

While numerous sources present best practices for data visualisation, many repeat the same standard ideas. From the sources that were considered, the general best practices for data visualisation can be summarised as follows:

1. Clearly define the context
2. Choose the right charts for the data
3. Use predictable patterns
4. Keep it simple
5. Use colour wisely – be conscious of accessibility

(Tableau Software, 2022; University at Buffalo, 2022; Predictive Analytics Today, 2022; Lurința, 2021; University of Minnesota, 2021; Painter, Zwar, Carino, & Kermonde, 2021; Knaflic, 2015; Google, 2022)

To demonstrate the application of the five data visualisation principles highlighted above, Figure 3.1 below will now be analysed with detail given to each principle.

When designing the dashboard in Figure 3.1, the context was to present senior stakeholders with high-level charts that effectively summarised the two Security Culture processes. A bar chart was chosen to compare phishing resilience stats between last year and this year; a line was also included to represent SSE's risk appetite level. Comparatively, the part-to-whole doughnut chart was used, as recommended within the SSE brand guidelines document, to summarise the current status of password compliance. All unnecessary visual elements were removed for predictable patterns and keeping it simple, and standard formats for titles, legends and axis were used. Finally, for colour, SSE teal was used to show primary statistics, core SSE blue for secondary statistics and SSE light blue for tertiary statistics and targets. All conventions outlined here are visible throughout the entire project artefact.

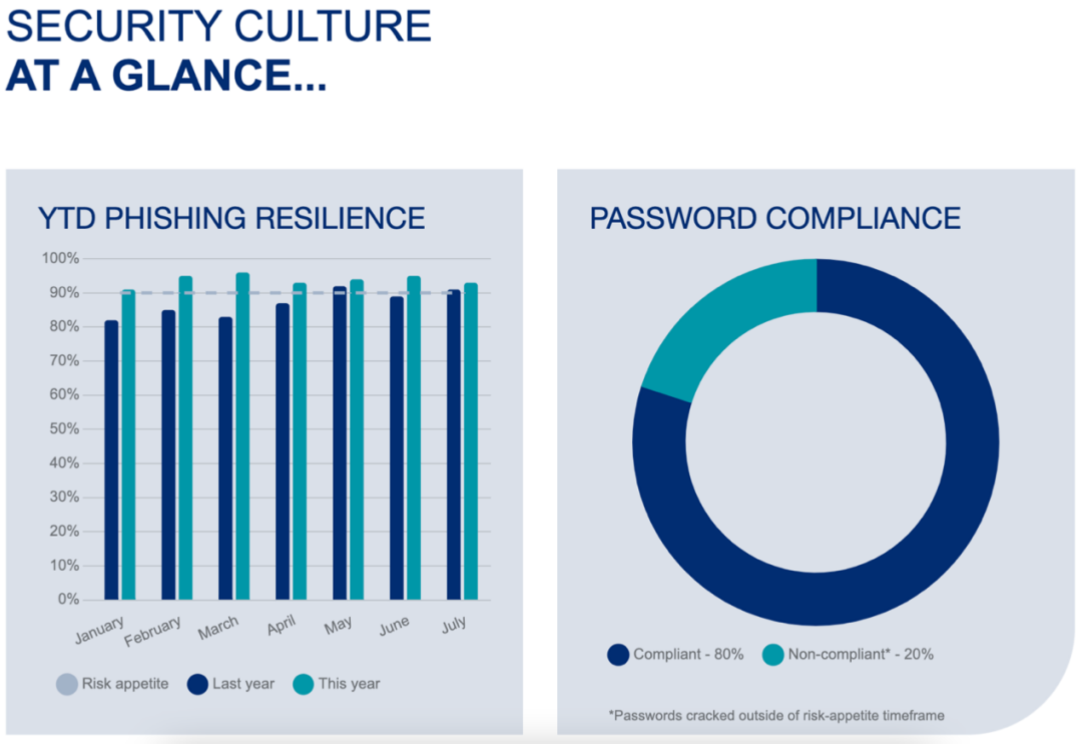
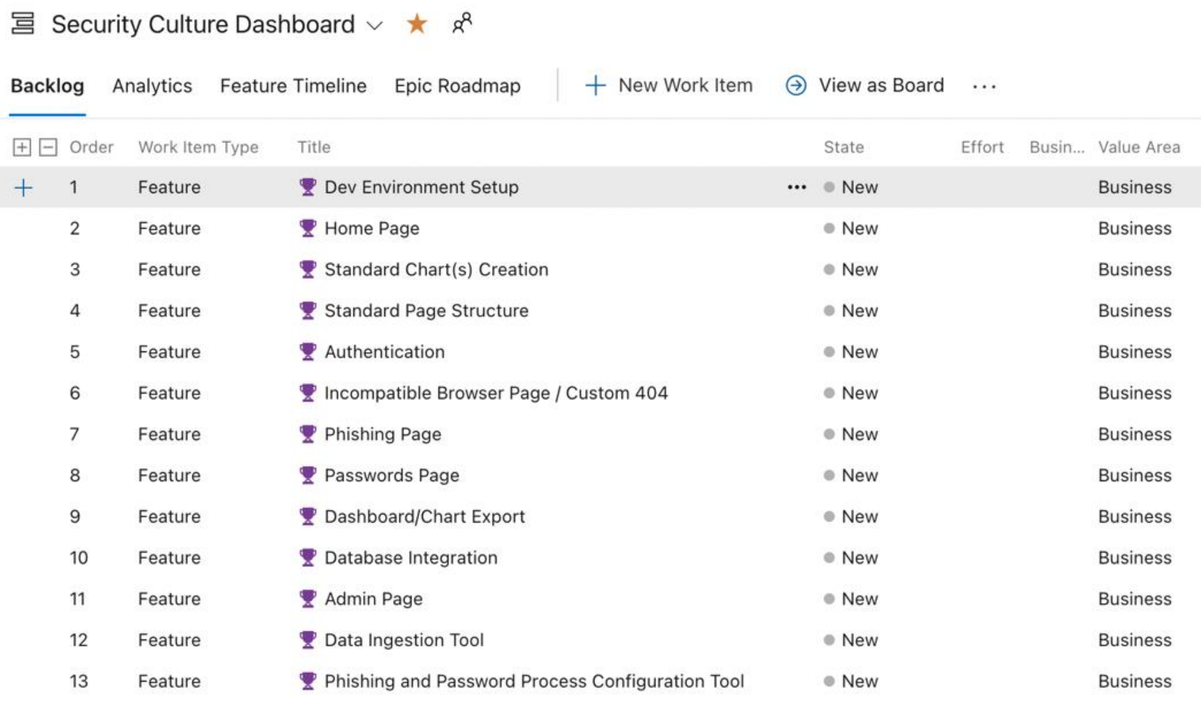


Figure 3.1 - Example SCD data visualisations

3.5 Requirements Formulation

While the SCD project was a proof-of-concept exercise and requirements could flex depending on project findings, several essential requirements were determined with the client during an interview session before the first sprint. Requirements were split into must-haves, could-haves, and won’t-haves in a simplified version of the MOSCOW prioritisation model and user stories were created to articulate each feature’s value to the customer effectively. Appendix G – Detailed System Requirements shows all defined project requirements and associated user stories. As stated in Project Lifecycle, the project adopted an Iterative approach using the Scrum framework. Therefore, the first scrum artefact, a Product Backlog, was created from these requirements, Figure 3.2.



Order	Work Item Type	Title	State	Effort	Busin...	Value Area
1	Feature	Dev Environment Setup	New			Business
2	Feature	Home Page	New			Business
3	Feature	Standard Chart(s) Creation	New			Business
4	Feature	Standard Page Structure	New			Business
5	Feature	Authentication	New			Business
6	Feature	Incompatible Browser Page / Custom 404	New			Business
7	Feature	Phishing Page	New			Business
8	Feature	Passwords Page	New			Business
9	Feature	Dashboard/Chart Export	New			Business
10	Feature	Database Integration	New			Business
11	Feature	Admin Page	New			Business
12	Feature	Data Ingestion Tool	New			Business
13	Feature	Phishing and Password Process Configuration Tool	New			Business

Figure 3.2 - SCD Product Backlog

Throughout development, the must-haves would be prioritised and delivered first (backlog items 1 to 9), with could-haves only being delivered if sufficient time remained (backlog items 10 to 13).

As the implementation details of the solution were initially unclear, a thorough systems specification document was not produced. However, during the project's design phase, time was taken to review relevant system architectures and appropriately upskill the development team to ensure the system could be produced within the strict time constraints imposed on the project. An outline of the project plan can be found in Appendix C – Project Plan.

4 Analysis and Design

During the initial analysis phase of the project, a benefits case was produced for the client, which outlined several options for the solution and highlighted the distinct benefits gained from each option, Appendix B – Initial Benefits Case. It should be noted that the requirements, discussed above, took the two options outlined in the benefits case and scoped the features from option two as must-haves and those from option three as could-haves in a simplified version of the MOSCOW prioritisation model. This enabled the project to deliver as much value to the client as possible in the short time allotted. Additionally, taking the benefits and comparing them with the opportunities presented in the Security Culture programme SWOT, Table 3.2, reveals that the project worked towards exploiting two of the six opportunities and provided a basis for developing a third opportunity in the future. Additionally, the project also worked towards addressing two of the five Security Culture weaknesses.

As highlighted in the project plan, Appendix C – Project Plan, a general design phase occurred before the first project sprint to ensure the project team was clear on the direction of the system and how it could be created. Several system architectures were reviewed, and it was decided that the SCD would be delivered using a full JavaScript technology stack because the project team was already conversant with the language. Additionally, from the system requirements and user stories, Appendix G – Detailed System Requirements, a collection of design artefacts was created. The first design artefact created was a UML case diagram, Figure 4.1, which initially enabled the team to develop their ideas of the system’s interactions. Furthermore, by using a use case diagram, the project could better understand the system from the end user's perspective.

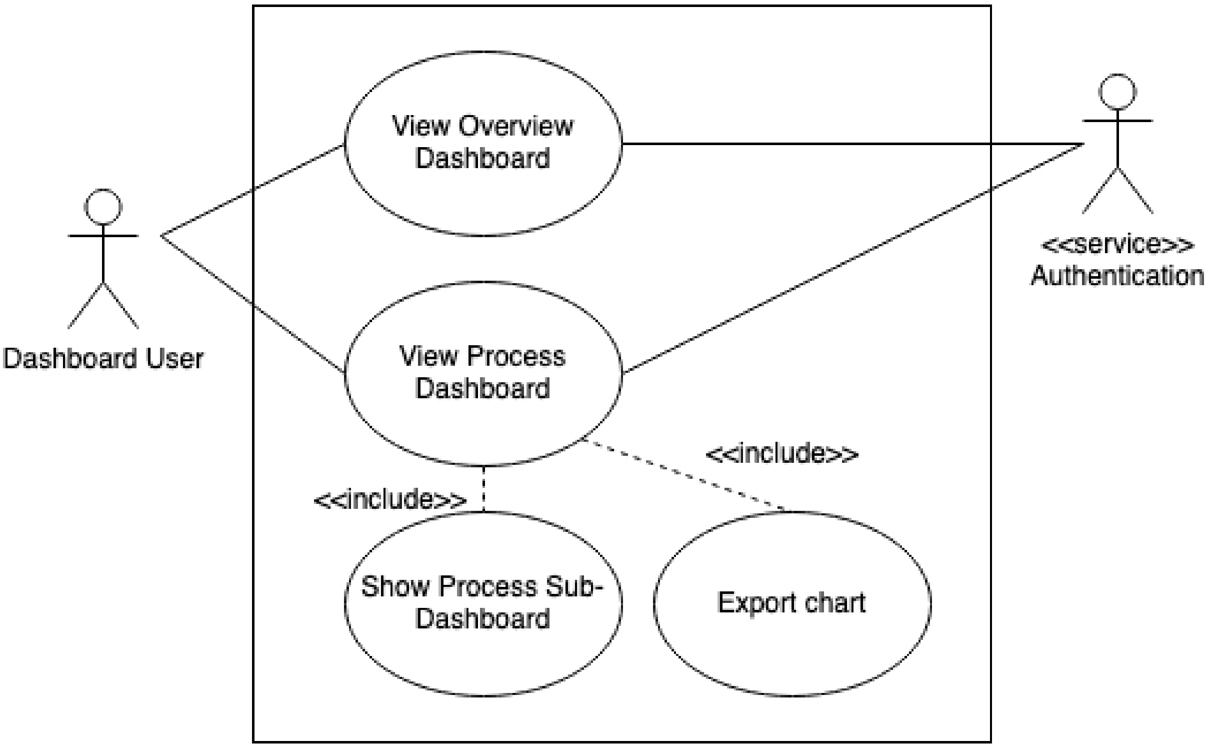


Figure 4.1 - System UML Case Diagram

Additional design artefacts, including an entity relationship diagram, a complete set of system wireframes and system interface and chart prototypes, can be seen in Appendix H – Design Artefacts.

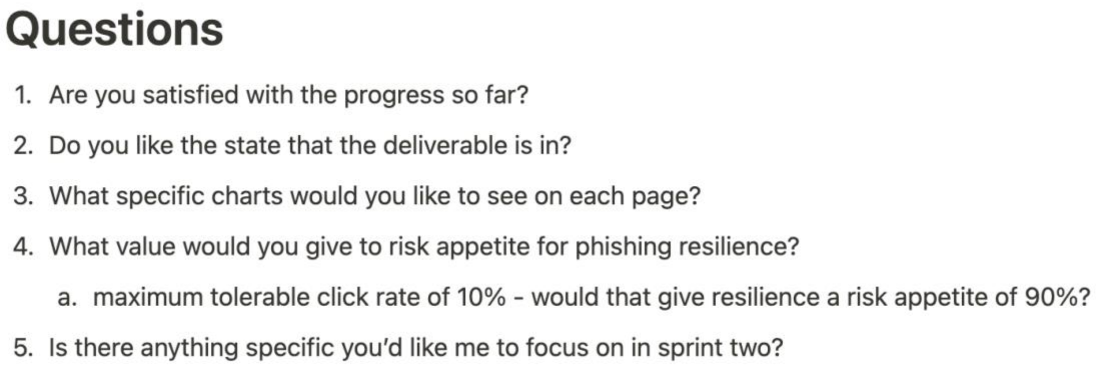
As a final step before progressing to the first development sprint, following the Scrum framework, the first Sprint Backlog was created from the Product Backlog. An overview of the work items (outlined in Figure

3.2 - SCD Product Backlog) delivered as part of each development sprint can be seen below in Table 4.1.

Sprint One	Sprint Two	Sprint Three
1. Dev Environment Setup 2. Authentication 3. Home Page 4. Standard Chart(s) Creation	1. Standard Page Structure 2. Incompatible Browser Page / Custom 404 3. Phishing Page	1. Passwords Page 2. Dashboard/Chart Export 3. Improved quality of sample data

Table 4.1 - Sprint Overview

At the end of each development sprint, a retrospective session was held with the client to ensure they were satisfied with the current state of the deliverable as well as to discuss findings and next steps. Additionally, the sessions were opportunities to present details of the solution to the client to develop their ideas of what they would require from a production system. A screenshot of the questions raised with the client within the first sprint retrospective can be seen below in Figure 4.2.



Questions

1. Are you satisfied with the progress so far?
2. Do you like the state that the deliverable is in?
3. What specific charts would you like to see on each page?
4. What value would you give to risk appetite for phishing resilience?
   a. maximum tolerable click rate of 10% - would that give resilience a risk appetite of 90%?
5. Is there anything specific you'd like me to focus on in sprint two?

Figure 4.2 - Questions presented to the client in sprint retrospective one

Finally, as part of the development cycle within each sprint, Figure 2.3, a range of different tests were performed. Table 4.2 below outlines the different tests performed and provides examples of how the tests were used during the SCD project. Descriptions have been formed based on resources from Atlassian (2022), Hamilton (2022) and Everett and McLeod (2007).

Test	Description	Example
Unit	Testing individual functions and components of the system to ensure they work as expected.	Creating a new chart and verifying that it looks, and functions, as intended.
Integration	At a higher level than unit testing, integration tests verify that functions and components work together and do not produce any erroneous outputs.	Verifying that the chart export feature works with existing charts.
Performance	An evaluation of how efficiently the system operates and whether it is at an acceptable level. Quantified during the SCD project using Google Lighthouse (Google, 2022).	Assessing the system using Google Lighthouse and ensuring the Performance metric is within the acceptable parameters defined in the Project Initiation Document – see Appendix A – Project Initiation Document (p.42) for details.
Acceptance	Formal tests, usually conducted with the client, that ensure the system satisfies the business requirements.	Reviewing progress with the client during each sprint retrospective and determining whether requirements have been delivered upon.

Table 4.2 - SCD Software Testing

5 Conclusions and Recommendations

As part of the project closedown, a final review and acceptance session was held with the client to ensure all requirements and objectives had been delivered. The session was also used to demonstrate the final artefact to the client and answer any questions they may have had about features and functionality. Appendix I – Requirements Delivery Review details the requirements and user stories, whether they were delivered by the project and any relevant comments/feedback from the project team and client. In summary, the project delivered on all requirements scoped as must-haves and none that were scoped as could-haves. Appendix J – System Performance Reports has been attached to quantify the performance metric, containing performance reports produced by Google Lighthouse (Google, 2022).

Overall, the project has delivered on all three objectives it set out to achieve and has provided the SSE Security Culture team with a valuable artefact that can be taken forward and used to inform decision-making when implementing a complete production analytics solution. There are, however, several critical areas that the project recommends the Security Culture team investigate/take further as recommendations. These include:

- Different user types and permission levels
- Native export to email/PowerPoint
- Automatic data ingestion
- System administration and configuration of key values such as targets and risk appetite levels

In hindsight, an Iterative PMLC approach would still appear to be the most appropriate if the project were to be completed again. While the original requirements did not change, the flexibility and learning opportunities provided by the Agile Scrum approach enabled the project team to effectively demonstrate several features and benefits of an analytics solution to the client. However, if the solution's details were defined in greater detail at the beginning of the project, the team acknowledges that an Incremental approach may be a better fit.

Going forward, the project team would like to continue expanding their knowledge and understanding of Agile software development practices as the ability to generate valuable software artefacts in short periods is a highly appealing prospect.

Finally, after the final review session, the client provided the following statement (Appendix K – Client Feedback) highlighting their involvement and experience with the project:

"The end product you have created is fantastic – and this is no accident! Your focused planning, scoping and ability to listen, consume and create a solution from an agreed set of initial objectives is to be commended. You have lead this project well, keeping me informed at all sprint stages and delivering in an agile manner, allowing flexibility and value add.

Such is my enthusiasm and respect for what you've created, I'd love this to be transitioned into a live service for the Security Culture Programme." - Mike Whittle, SSE Security Culture Programme Lead, June 2022.

Reference List

Atlassian. (2022). *The different types of software testing*. Retrieved from Atlassian Software Development: https://www.atlassian.com/continuous-delivery/software-testing/types-of-software-testing

AXELOS Limited. (n.d.). *Prince2*. Retrieved from Axelos: https://www.axelos.com/best-practice-solutions/prince2

Centre for the Protection of National Infrastructure. (2021). *Security Culture*. Retrieved from CPNI: https://www.cpni.gov.uk/security-culture

Everett, G. D., & McLeod, R. (2007). *Software Testing Testing Across the Entire Software Development Life Cycle.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Farrell, S. (2016). *Open-Ended vs. Closed-Ended Questions in User Research*. Retrieved from Nielsen Norman Group: https://www.nngroup.com/articles/open-ended-questions/

Fessenden, T. (2017). *A Theory of User Delight: Why Usability Is the Foundation for Delightful Experiences*. Retrieved from Nielsen Norman Group: https://www.nngroup.com/articles/theory-user-delight/

Fessenden, T. (2021). *Design Systems 101*. Retrieved from Nielsen Norman Group: https://www.nngroup.com/articles/design-systems-101/

Flewelling, P. (2018). The the Agile Developer's Handbook : Get More Value from Your Software Development: Get the Best Out of the Agile Methodology. Packt Publishing, Limited.

Google. (2021). *Lighthouse*. Retrieved from Google Developers: https://developers.google.com/web/tools/lighthouse

Google. (2022). *Data Visualization*. Retrieved from Material Design: https://material.io/design/communication/data-visualization.html

Google. (2022). *Design*. Retrieved from Material Design: https://material.io/design

Google. (2022). *Lighthouse*. Retrieved from Chrome Developers: https://developer.chrome.com/docs/lighthouse/overview/

Google. (2022). *Meet Material Design 3*. Retrieved from Material Design: https://m3.material.io/

Graphus. (2021). *10 Facts About Phishing That You Need to See*. Retrieved from Graphus: https://www.graphus.ai/blog/10-facts-about-phishing-in-2021-that-you-need-to-see/

Hamilton, T. (2022). *What is Software Testing? Definition, Basics & Types in Software Engineering*. Retrieved from Guru99: https://www.guru99.com/software-testing-introduction-importance.html

Kerner, S. M. (2022). *Colonial Pipeline hack explained: Everything you need to know*. Retrieved from WhatIs.com: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Knaflic, C. N. (2015). Storytelling with Data: A Data Visualization Guide for Business Professionals. Hoboken, New Jersey: John Wiley & Sons, Inc.

Luriņa, L. (2021). *5 best practices for data visualization*. Retrieved from Infogram: https://infogram.com/blog/data-visualization-best-practices/

Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*(50), 370-396.

McGowan, S. (n.d.). *5 Alternatives To Material Design*. Retrieved from Usability Geek: https://usabilitygeek.com/alternatives-to-material-design/

National Institute of Standards and Technology. (2022). *NIST Cybersecurity Framework*. Retrieved from NIST: https://www.nist.gov/cyberframework

Painter, E., Zwar, J., Carino, S., & Kermonde, Z. (2021). *BEST PRACTICE DATA VISUALISATION GUIDELINES AND CASE STUDY.* Melbourne: Monash University.

Predictive Analytics Today. (2022). *Top 6 Best Practices in Data Visualization*. Retrieved from PAT Research: https://www.predictiveanalyticstoday.com/top-best-practices-in-data-visualization/

SASIG Events Limited. (2022). *Our Story*. Retrieved from SASIG: Security Awareness Special Interest Group: https://www.thesasig.com/about/our-story/

Scrum Alliance. (2022). *The Three Scrum Artifacts and Their Commitments*. Retrieved from Scrum Alliance: https://resources.scrumalliance.org/Article/scrum-artifacts

Scrum.org. (2022). *What is Scrum?* Retrieved from Scrum.org: https://www.scrum.org/resources/what-is-scrum

Slant. (2022). *What is the best alternative to Material UI?* Retrieved from Slant: https://www.slant.co/options/522/alternatives/~material-ui-alternatives

Spanning Cloud Apps. (2022). *Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year* . Retrieved from Spanning: https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

SSE. (2020). *Brand Guidelines.* Retrieved from SSE: (internal)

SSE. (2021). *Annual Report 2021.* Retrieved from SSE: https://www.sse.com/media/rwhbww02/sse-annual-report-2021.pdf

SSE. (2021). *Group Risk Report 2022/21*. Retrieved from SSE: https://www.sse.com/media/55xfxzoh/group-risk-report-21.pdf

SSE. (2022). *Our Strategy*. Retrieved from SSE: https://www.sse.com/who-we-are/our-strategy/

Tableau Software. (2022). *Tips for creating effective, engaging data visualisations*. Retrieved from Tableau: https://www.tableau.com/en-gb/learn/articles/data-visualization-tips

Tidwell, J., Brewer, C., & Valencia, A. (2020). *Designing Interfaces: Patterns for Effective Interaction Design.* Sebastopol: O'Reilly Media, Inc.

University at Buffalo. (2022). *Search this Guide Data Visualization: Best Practices*. Retrieved from University at Buffalo University Libraries: https://research.lib.buffalo.edu/dataviz/best-practices

University of Minnesota. (2021). *Data Visualization*. Retrieved from University of Minnesota Libraries: https://libguides.umn.edu/c.php?g=921727&p=6643021

Walter, A. (2022). *Designing for Emotion* (Vol. 2). New York: A Book Apart, LLC.

Wysocki, R. K. (2019). *Effective Project Management: Traditional, Agile, Extreme, Hybrid* (Vol. 8). Indianapolis: John Wiley & Sons, Incorporated.

Appendices

Appendix A – Project Initiation Document

PROJECT INITIATION DOCUMENT

(Version created to support DAP605)

Project name Security Culture Dashboard Proof of Concept

Release Draft/**Final**
Date: 30/03/2022

PRINCE2 Based on a reduced version of the PRINCE2 PID documentary requirements

Author:	Adam Blanchard
Owner:	Adam Blanchard
Client:	Mike Whittle
Document Number:	1.0

Document History

Document Location

This document is only valid on the day it was printed.
The source of the document will be found in the Control section of the Project File.

Revision History

Date of next revision:

Revision date	Previous revision date	Summary of Changes	Changes marked

Approvals

This document requires the following approvals.
Signed approval forms are filed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

Purpose

To define the project, to form the basis for its management and the assessment of overall success.

Contents

This publication contains the following topics:

Background

SSE plc (formerly Scottish and Southern Energy plc) is a leading generator of renewable electricity in the UK and Ireland and one of the largest electricity network companies in the UK. SSE's purpose is "To provide energy needed today, while building a better world of energy for tomorrow" (SSE, 2022) and they employ roughly 12,000 employees (SSE, 2021).

To ensure SSE remains secure in the 21st century, the Cyber Risk and Information Security team (CRIS) protects SSE against its second highest principal risk, Cyber Security and Resilience (SSE, 2021). In 2018, a programme called Security Culture was created within CRIS, to specifically tackle the Awareness & Training component of the 'Protect' function within the National Institute of Standards and Technology (NIST) Cybersecurity framework (National Institute of Standards and Technology, 2022).

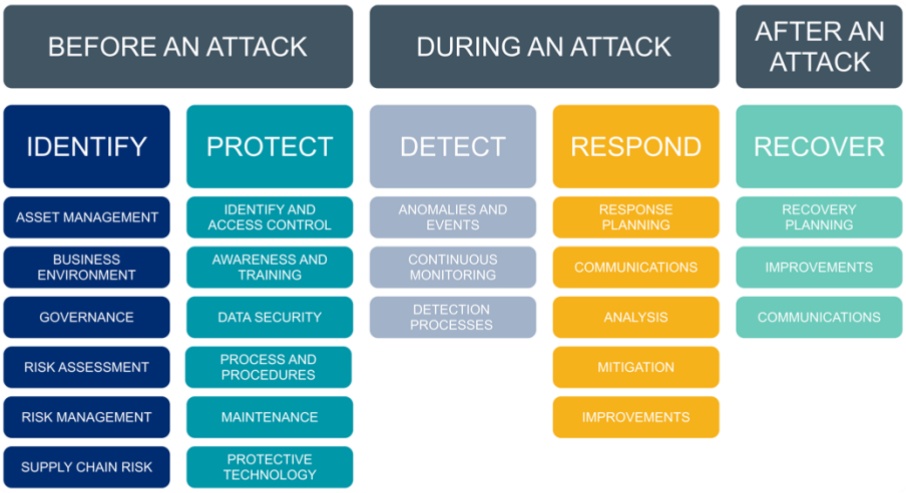


Figure 0.1 - NIST Cybersecurity framework.

Security Culture Dashboard (SCD)

Along with other inputs, the cyber security resilience of SSE's colleagues is measured using metrics from two Security Culture processes: phishing resilience and password management. Currently, metrics from these processes are manually collated each month and are used to produce reports and charts that are presented to a range of stakeholders. As the programme matures, the team is experiencing an increased demand for their services. The time dedicated to producing these reports is therefore becoming more and more valuable over time.

This proof of concept will aim to collate several metrics from the Security Culture processes outlined, and will demonstrate efficient and effective information sharing, which should in turn promote informed decision making by key stakeholders.

Project Definition

Project objectives

Aim

Develop and evaluate a software solution that collates and demonstrates key Security Culture metrics.

Objectives

1. **Delivery of a web dashboard interface** which can be run efficiently on hardware - desktops and laptops - deployed by SSE.
2. **Improved reporting experience** through the automatic creation of charts and reports based on pre-existing data formats.
3. **Delivery of a solution that incorporates researched best practice** for interface design, dashboard design and data visualisation.

Defined method of approach

There are a number of different project management lifecycles (PMLC) that would be appropriate for a software engineering project of this nature. In his 2019 book Effective Project Management, Wysocki outlines five different types of PMLC including Linear, Incremental, Iterative, Adaptive and Extreme (Wysocki, 2019, p. 23). He later goes on to discuss their relationship to each other, and how the five lifecycles fit into the wider context of project management, by overlaying the PMLCs onto the four quadrants of the project landscape, see Figure 0.2 below.

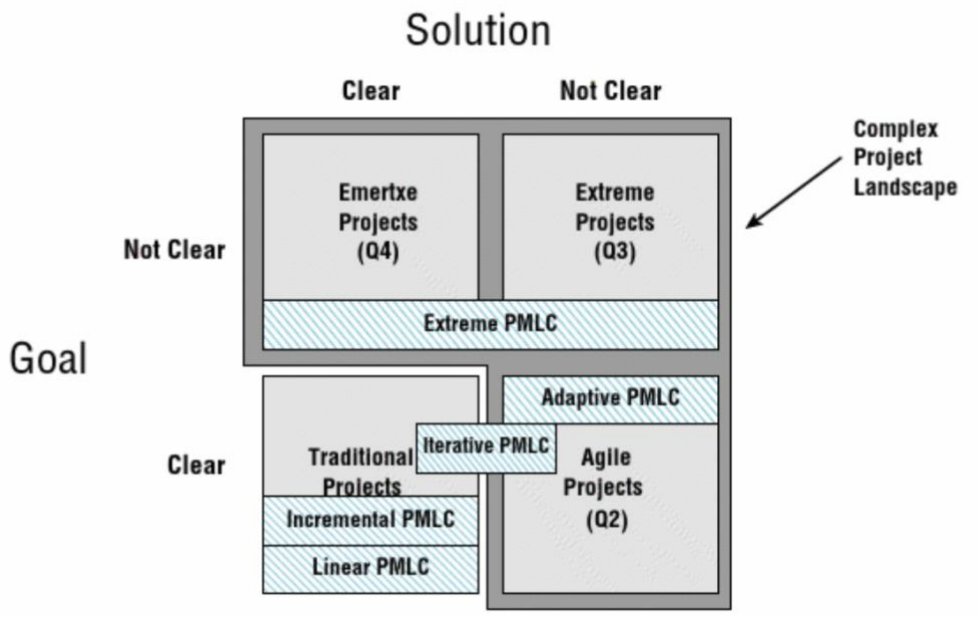


Figure 0.2 - Five PMLC types (Wysocki, 2019, p. 39)

Using the details previously outlined in this report, the project goal is assessed as being reasonably well defined. However, the details of the solution are initially somewhat unclear. Aligning this assessment with Wysocki’s PMLC matrix presented above would suggest that an Iterative PMLC may be appropriate. Should the solution become better defined, it may be more appropriate to use an incremental PMLC. These two PMLCs will be discussed and compared below in order to identify which would be best suited to the SCD project.

An **Iterative** PMLC approach can be summarised by the flow chart seen below in Figure 0.3.

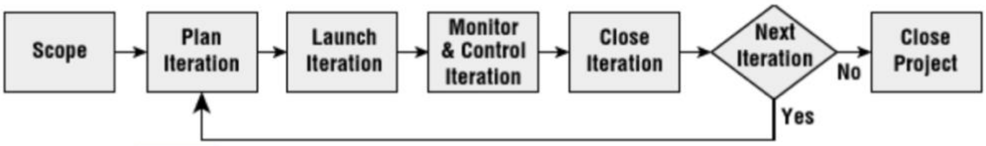


Figure 0.3 - Iterative PMLC Flowchart (Wysocki, 2019, p. 49)

Similarly, an **Incremental** PMLC approach can be summarised by the flow chart seen below in Figure 0.4.

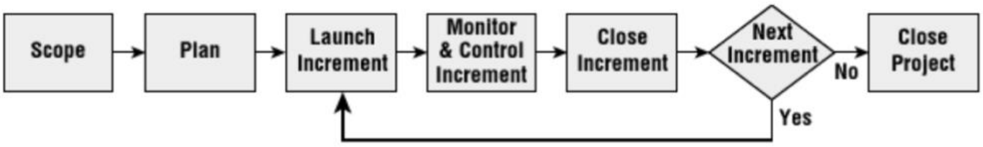


Figure 0.4 - Incremental PMLC Flowchart (Wysocki, 2019, p. 44)

Wysocki suggests that in both Iterative and Incremental PMLCs, change is actively encouraged throughout the course of the project, through frequent engagement with the customer. This is in stark contrast to a traditional PMLC such as Linear, in which change to scope is not expected or encouraged.

While both the Iterative and Incremental PMLCs demonstrate a cyclical process, there are slight variations. When conducting a systems development project according to an Iterative approach, Wysocki suggests that as part of each iteration, the objective is to show the customer an intermediate, incomplete solution and ask them for feedback on changes or additions they would like to see. Additionally, Wysocki further goes on to recommend that Iterative PMLCs "definitely fit the class of projects that provide opportunity to learn and discover", (Wysocki, 2019, p. 49) and that there is an assumption (with an Iterative PMLC) that the client should learn and discover more about the solution from each iteration.

In comparison to the Iterative PMLC, Incremental appears much more rigid in nature. Wysocki outlines that when following an Incremental PMLC, the complete solution should be known at the outset. This solution should then be decomposed into partial solutions which are developed in a sequential fashion. Care should be taken to manage any dependencies amongst partial solutions – this should be addressed through extensive release scheduling. Furthermore, while Wysocki identifies that change is part of an Incremental PMLC, any changes suggested by the client(s) should be managed via a formal change request process - leaving less scope for implementing feedback, when compared to an Iterative approach (Wysocki, 2019, p. 44).

Taking the outlined details into consideration, it appears an Iterative PMLC is more appropriate to the SCD project due to the greater scope for creative freedom demanded by a proof-of-concept project. As examples, Wysocki presents four models that follow an Iterative approach including: Evolutionary Development Waterfall, Scrum, Rational Unified Process (RUP) and Dynamic Systems Development Method (DSDM) (Wysocki, 2019, pp. 48-49).

As the project team is already familiar with the operation of projects according to Scrum principles, this is the methodology that will be adopted - albeit with some slight variations. In the Agile Developer's Handbook, Flewelling identifies that "Scrum recommends a team of no fewer than five" (Flewelling, 2018, p. 41). Flewelling also goes on to discuss the merits of the Kanban methodology and the technique of 'pulling' work through the production process to ensure the work items are delivered at pace.

Taking the consistency and structure provided by Scrum and the flexibility provided by Kanban, the project team will adopt a Scrumban approach to systems development.

The team will make use of tools such as a Product Backlog, Kanban board and Sprint Planning to ensure the project is delivered effectively and progress can be easily demonstrated to key stakeholders. Items on the Product Backlog will be prioritised and delivered through bi-weekly sprints - this duration has been chosen to account for the limited time the project team has available to dedicate to the project each week. The structure of a sprint can be seen represented by **Error! Reference source not found.** below. The following stages will occur within each sprint in order to deliver effective product features: Design, Develop, Test, Deploy, Review.

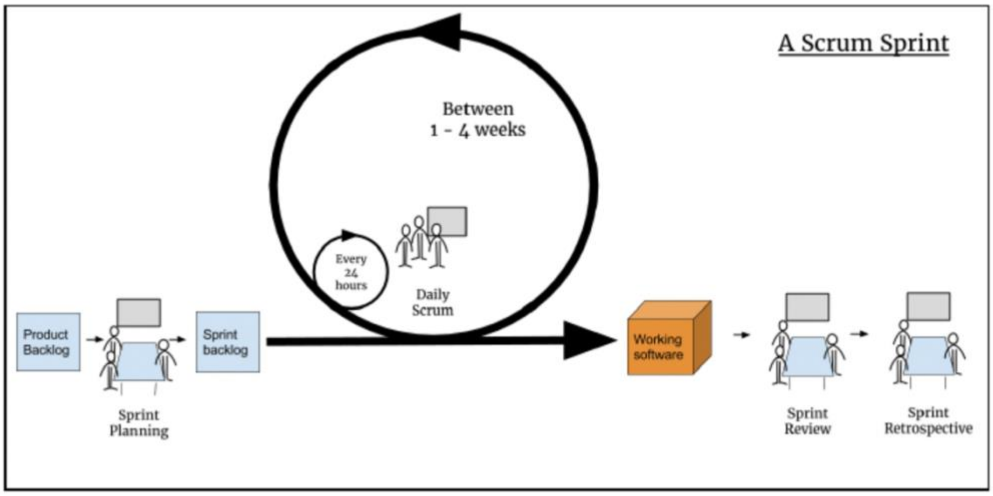


Figure 0.5 - A Scrum Sprint (Wysocki, 2019, p. 42)

Project scope

The SCD project will be delivered as a proof of concept. Therefore, the final deliverable will only demonstrate features and benefits - there will be no consideration for implementation with SSE infrastructure.

The SCD project will only make use of metrics available at the time of project initiation. No further metrics will be adopted by the project during the project lifecycle.

While data structures will be used, **no SSE data** will be used in the project. Resulting in a project that is not classified as Confidential.

The Phishing component of the project will be emphasised as this is the most mature process at SSE today.

To support modern website functionality, only browsers that support the JavaScript standard ECMAScript 6 (ES6) or later will be supported by the project team.

As this is a proof-of-concept project, the project team reserves the right to use any technology architecture they deem appropriate. Standard SSE system architecture will not apply.

Project deliverables

The SCD project will deliver a web application that will demonstrate features and benefits that could be incorporated into a full production system at a later date.

Components of the web application include:

- Data visualisations including graphs and charts
- Supporting context where appropriate
- At least two dashboards summarising each process
- Upload tool for data ingestion

The deliverable should also have the ability to function on SSE device specifications, however this is not a showstopper.

Exclusions

The system delivered is classed as a proof of concept and will therefore only demonstrate features and benefits that could be later developed into a full, production system. No consideration will be given to integration with SSE's systems.

No training will be provided to the customer on usage of the project deliverable.

The final deliverable will be a web application only – no native application(s) will be created.

Constraints

There are several constraints that the SCD project is subject to. These include:

Time

- At the latest, the project must cease all activity by the 12th of June 2022– this provides the team with two weeks of contingency.
- The amount of time committed to the project by the team each week will be capped at 12 hours.
- The client is only available between 08:00 and 17:30, Monday to Friday.

Budget

- There is no budget for the project. As a result, any project or development tooling must be free of charge or open source.

Development standards

- The development team should strive to make use of modern development techniques.
- Any JavaScript written should be constrained to ECMAScript 6 (ES6).

Travel

- Travel required by the project should be minimised as much as possible due to the lack of budget, as defined above.

Assumptions

The project team must have frequent communication with the client as per the communication plan outlined below.

A minimum of three retrospectives should occur in line with the development sprints to ensure the project is progressing as expected.

It is expected that any feedback sought from the client will be gained within five working days of initial communication.

Project Organisation Structure

The project team consists of a single individual who will adopt the multiple roles required by the project. The project has a single client from the SSE Security Culture Programme.

Project Team
Adam Blanchard – Project Manager and Developer

Security Culture Programme
Mike Whittle (Client) – Security Culture Programme Lead

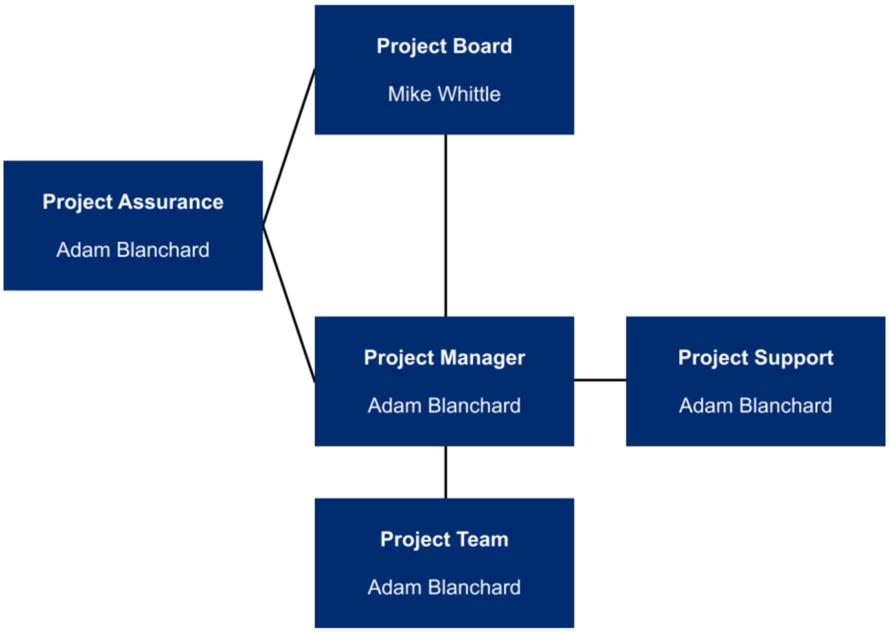


Figure 0.6 - SCD Project Organisation Structure

Communication Plan

In accordance with the Scrumban methodology previously outlined, a sprint retrospective will take place with the client, Mike Whittle, at the end of each sprint to gather feedback.

Additionally, at a higher level, Mike will be engaged at all project milestones including PID completion, development completion and project closedown.

Primarily, Mike will be engaged via Microsoft Teams instant message and email. The project team may also communicate with Mike through a number of Microsoft Teams meetings.

Mike will have access to the project Kanban board and will always have visibility of what product features are work in progress and what remains on the product backlog.

Project Quality Plan

As the SCD project is a proof of concept, there are a number of quality expectations in place which ensure that the project delivers real features and benefits to the client. These quality expectations include:

- Deliverable should demonstrate current best practice in the specific areas of interface design, dashboard design and data visualisation.
- The deliverable should provide context and supporting commentary where appropriate – above and beyond simply displaying ‘raw data’.

Code Standards

- Code produced for the SCD project should make use of modern paradigms where possible and also be efficient in nature.
    - Google Lighthouse (Google, 2021) will be used to measure performance, where performance is assigned a rating of between 0 and 100.
- JavaScript ES6 should be used.
- A repository should be used to store, and version control the project’s source code, to ensure development is a seamless and secure process.

Project Tolerances

The following tolerances are recognised for the SCD project:

Time

- +/- 1 week for target completion dates.

Quality

- Target Google Lighthouse (Google, 2021) performance score of 75/100 +/- 25.

Benefit

- Target of 40% improvement on time taken to produce reports +/- 10%.

Project Controls

The SCD project will be controlled according to the PRINCE2 methodology. Taking into account the phases within Scrum, the project will be delivered through the following stages:

- Project Initiation
- Design
  - Interface and back-end design
  - Architecture review and team upskilling
  - Product Backlog creation
  - Sprint planning
- Development (3x sprints and retrospectives)
- Project Closedown

Project files will be stored within a dedicated Microsoft Teams area, which will be accessible by the project team and the client. It is within this area that the Kanban board will be hosted.

The client (Mike Whittle) will be engaged at all project milestones as well as during each sprint retrospective.

As outlined within Project Definition, requests for change will be captured during each sprint retrospective and incorporated within the deliverable where possible. The prioritised product backlog along with work progress will be tracked via the Kanban board, allowing the team to clearly evidence delivery of key functions.

Risks to the project will be tracked using a risk register/log which can be seen attached.

Appendix B – Initial Benefits Case

INITIAL BENEFITS CASE

Project name	Security Culture Dashboard Proof of Concept
Release	Draft/**Final** Date: 13th March 2022
PRINCE2	Based on a reduced version of the PRINCE2 PID documentary requirements

Author:	Adam Blanchard
Owner:	Adam Blanchard
Client:	Mike Whittle
Document Number:	1.0

Reasons

This document is an evaluation of the several options available to the client with regards to the Security Culture Dashboard project, outlining the advantages and disadvantages of each option.

The findings should assist in the production of a solid benefits case of the chosen solution over the alternative options. Additionally, the details presented will assist with any benefits realisation activity post-project closure.

Options

Taking the project's aims and objectives into consideration, the following options are presented:

1. **Remain the same – do not deliver the Security Culture Dashboard project.**
   The SCD project is not delivered, and no benefits or features from the proof of concept are realised. Reporting is completed in the existing manual way, which continues to require significant amounts of effort monthly.

2. **Delivery of a minimal Security Culture Dashboard**
   The SCD project delivers a dashboard that demonstrates the features and benefits of reporting but does not consider the specific intricacies of storing and managing data. The front-end is delivered, yet any back-end functionality is reduced to an absolute minimum.

3. **Delivery of a 'full-stack' Security Culture Dashboard**
   The SCD project delivers a 'full-stack' application that delivers the front-end outlined in option two and a back-end to the application, which handles data storage and management and server-side functions. This could cover but is not limited to an API used to fetch and update data from a central repository.

Benefits

Option 1
No benefits will be realised from option 1.

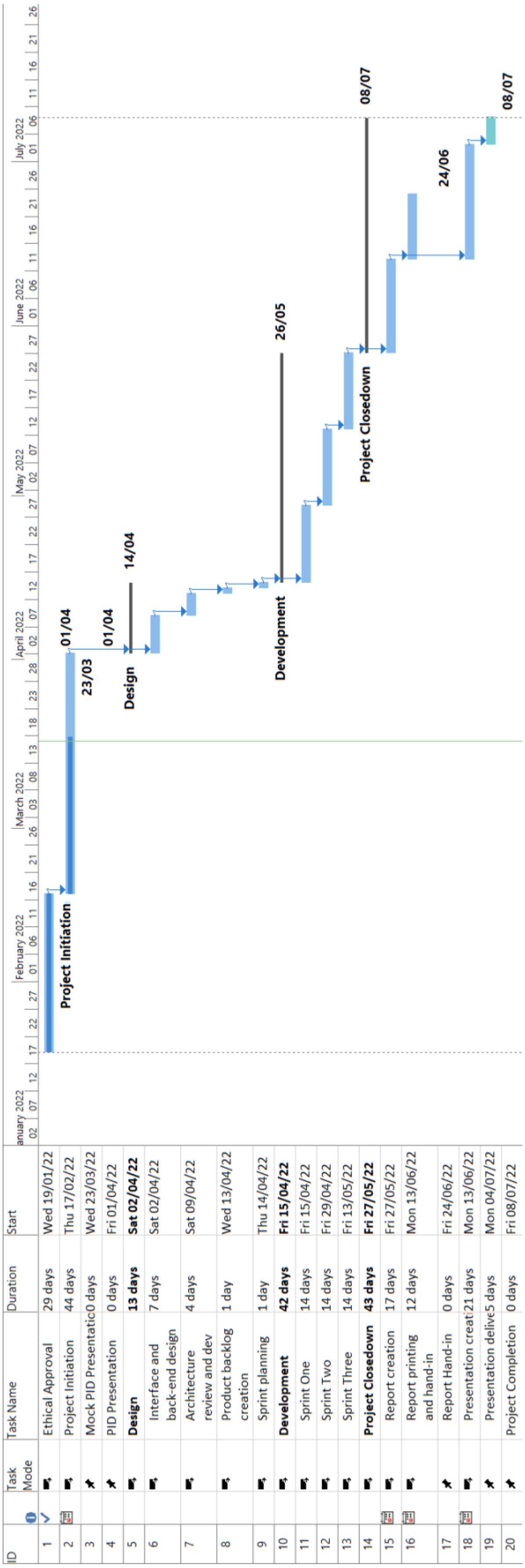
Options 2 and 3
Delivery of either options two or three, outlined above, will demonstrate several key benefits to the client. These include:

- A reduction in effort spent on manual reporting
- An enhancement in the ability to surface insights from data produced from the client's processes
- A demonstration of the features that could be incorporated into a production system
- An example of how to apply current best-practice in the areas of data visualisation and dashboard design
- An artifact that can be demonstrated to the client's stakeholders in order to enhance arguments for delivery of a production analytics solution

Option 3 only
Delivery of option 3 will realise all benefits outlined above, as well as several that are unique to this option - these include:

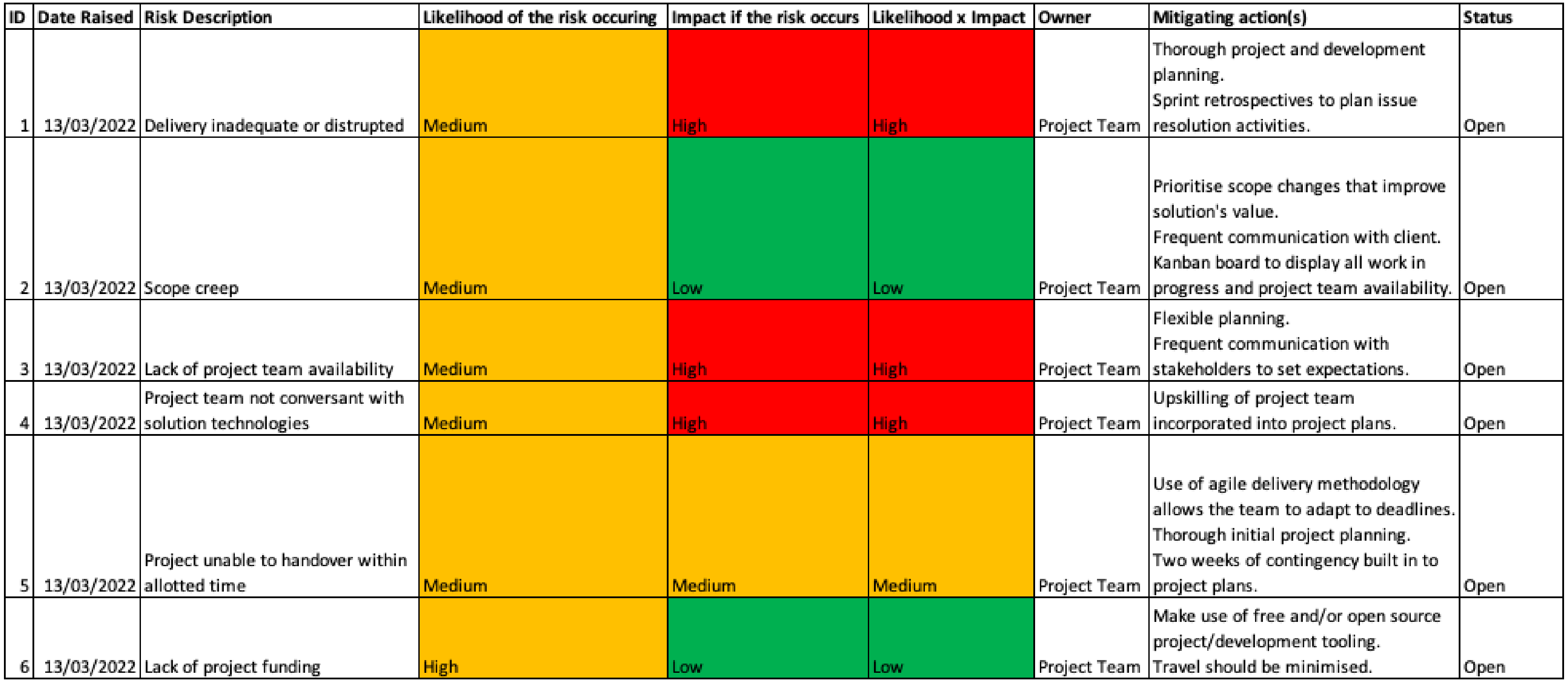
- A demonstration of secure development principles
- An investigation into data architecture and management
- A more 'complete' solution in terms of features and architecture
- A better understanding of the requirements of a production analytics solution
- A more thorough investigation into the 'art of the possible'

Appendix C – Project Plan



ID	Task Mode	Task Name	Duration	Start
1		Ethical Approval	29 days	Wed 19/01/22
2		Project Initiation	44 days	Thu 17/02/22
3		Mock PID Presentatio	0 days	Wed 23/03/22
4		PID Presentation	0 days	Fri 01/04/22
5		**Design**	**13 days**	**Sat 02/04/22**
6		Interface and back-end design	7 days	Sat 02/04/22
7		Architecture review and dev	4 days	Sat 09/04/22
8		Product backlog creation	1 day	Wed 13/04/22
9		Sprint planning	1 day	Thu 14/04/22
10		**Development**	**42 days**	**Fri 15/04/22**
11		Sprint One	14 days	Fri 15/04/22
12		Sprint Two	14 days	Fri 29/04/22
13		Sprint Three	14 days	Fri 13/05/22
14		**Project Closedown**	**43 days**	**Fri 27/05/22**
15		Report creation	17 days	Fri 27/05/22
16		Report printing and hand-in	12 days	Mon 13/06/22
17		Report Hand-in	0 days	Fri 24/06/22
18		Presentation creati	21 days	Mon 13/06/22
19		Presentation delive	5 days	Mon 04/07/22
20		Project Completion	0 days	Fri 08/07/22

Appendix D – Risk Log



ID	Date Raised	Risk Description	Likelihood of the risk occuring	Impact if the risk occurs	Likelihood x Impact	Owner	Mitigating action(s)	Status
1	13/03/2022	Delivery inadequate or distrupted	Medium	High	High	Project Team	Thorough project and development planning. Sprint retrospectives to plan issue resolution activities.	Open
2	13/03/2022	Scope creep	Medium	Low	Low	Project Team	Prioritise scope changes that improve solution's value. Frequent communication with client. Kanban board to display all work in progress and project team availability.	Open
3	13/03/2022	Lack of project team availability	Medium	High	High	Project Team	Flexible planning. Frequent communication with stakeholders to set expectations.	Open
4	13/03/2022	Project team not conversant with solution technologies	Medium	High	High	Project Team	Upskilling of project team incorporated into project plans.	Open
5	13/03/2022	Project unable to handover within allotted time	Medium	Medium	Medium	Project Team	Use of agile delivery methodology allows the team to adapt to deadlines. Thorough initial project planning. Two weeks of contingency built in to project plans.	Open
6	13/03/2022	Lack of project funding	High	Low	Low	Project Team	Make use of free and/or open source project/development tooling. Travel should be minimised.	Open

Appendix E – Application for Ethical Approval

Application for Ethical Approval: For all applications for ethical approval (staff/PGR/Masters/UG)

Section A: Basic Information

A1: Title of study:	**Security Culture Dashboard Proof of Concept**
A2: Name of Applicant: (in collaborative projects, just name the lead applicant)	Adam Blanchard
A3: Position of Applicant (e.g. UG/Masters/PGR student, academic)	UG student
A4: Programme of study: (for UG or taught Masters students only)	Digital and Technology Solutions Professional (Software Engineer)
A5: Department of Applicant:	Business School

A6: Checklist to ensure application is complete. Have you prepared the following documents to accompany your application for ethical approval, please tick the appropriate column for each of the following:

Document	**Yes**	**No**	**N/A**
Confirmation of Ethical Approval of any other organisation (e.g. NHS, MoD, National Offender Management Service)			X
Recruitment information / advertisement (e.g. draft text for email/ poster/social media/letter)			X
Information sheet for participants		X	
Information sheet for carers/guardians			X
Information sheet/letter for gatekeepers e.g. Head teacher, teacher, coach			X
Consent form for participants	X		
Assent form for younger children			X
Documentation relating to the permission of third parties other than the participant, guardian, carer or gatekeeper (e.g. external body whose permission is required)			X
Medical questionnaire / Health screening questionnaire			X
Secondary information sheet for projects involving intentional deceit/withholding information			X
Secondary consent form for projects involving intentional deceit/withholding information			X
Debrief sheet to give to participants after they have participated			X
Statements about completeness of the application	**Yes**	**No**	**N/A**
For research involving under 18s or vulnerable groups, where necessary, a statement has been included on all information sheets that the investigators have passed appropriate ***Disclosure and Barring Service***[1] checks			**X**
I can confirm that the relevant documents listed above make use of document references including date and version number	X		
I can confirm that I have proof read my application for ethical approval and associated documents to minimise typographical and grammatical errors	X		

[1] *Working with under 18's or other vulnerable groups may require a Disclosure and Barring Service Check. Contact HR@chi.ac.uk if you are not sure whether you have an up to date and relevant DBS check or if you require more information. Do note that a DBS check may take several weeks to obtain.*

Declaration of the applicant:

I confirm my responsibility to deliver the research project in accordance with the University of Chichester's policies and procedures, which include the University's '*Financial Regulations*', '*Research Ethics Policy', 'Electronic Information Security Policy'* and *'Privacy Standard'* and, where externally funded, with the terms and conditions of the research funder.

In signing this research ethics application form I am also confirming that:

- The research study must not begin until ethical approval has been granted.
- The form is accurate to the best of my knowledge and belief.
- There is no potential material interest that may, or may appear to, impair the independence and objectivity of researchers conducting this project.
- Subject to the research being approved, I undertake to adhere to the project protocol without deviation (unless by specific and prior agreement) and to comply with any conditions set out in the letter from the University ethics reviewers notifying me of this.
- I undertake to inform the ethics reviewers of significant changes to the protocol (by contacting the clerk to the Research Ethics Committee (research@chi.ac.uk) in the first instance).
- I understand that the project, including research records and data, may be subject to inspection for audit purposes, if required in future, in keeping with the University's Privacy Standard.
- I understand that personal data about me as a researcher in this form will be held by those involved in the ethics review procedure (e.g. the Research Ethics Committee and its officers and/or ethics reviewers) for five years after approval and that this will be managed according to Data Protection Act principles.
- I understand that all conditions apply to any co-applicants and researchers involved in the study, and that it is my responsibility to ensure that they abide by them.
- For the Student Investigator: I understand my responsibilities to work within a set of safety, ethical and other guidelines as agreed in advance with my supervisor and understand that I must comply with the University's regulations and any other applicable code of ethics at all times.

Title of study: Security Culture Dashboard Proof of Concept

Name of applicant: Adam Blanchard

Signature of Applicant: A.Blanchard Date: 16/02/2022

Section B: Authoriser assessment and approval

Where Applicants are students (undergraduate or postgraduate) supervisors should authorise this form; where applicants are staff members their line manager (or nominated signatory) should authorise this form.

B1: Name of Authoriser:	
B2: Position of Authoriser: (e.g. supervisor, line manager)	

AUTHORISER:

Please categorise the application (A, A+ or B) ensure that the application form and all of the required documentation are complete before signing this application.

Authoriser assessment: (tick as appropriate – *see Section 10 of the Research Ethics Policy*)

Category A: Proceed with the research project. ***Undergraduate and Postgraduate Taught Masters applications***: Form and documentation retained at Department level. ***Research Masters, PhD and staff applications***: Form and documentation forwarded to the Research Office *research@chi.ac.uk*	
Category A+: (for studies where information is withheld/there is an element of deceit or similar see Appendix 13) Proceed with the research project. ***Undergraduate and Postgraduate Taught Masters applications***: Form and documentation retained at Department level. ***Research Masters, PhD and staff applications***: Form and documentation forwarded to the Research Office *research@chi.ac.uk*	
Category B: Submit to the Ethical Approval Sub-group for consideration. *research@chi.ac.uk* Proceed only when approval granted by the Chair of the Research Ethics Committee	

Authoriser, please provide a comment on your assessment of the research project and for those projects involving vulnerable groups that you are authorising as Category A please justify this classification in the box below. As a further point, do make appropriate reference to any other codes of practice in your discipline particularly if you think that the proposed research may be in tension with those codes.

For Category A+: the application would be approved by the line manager/supervisor (as with Category A applications) and also by an independent scrutiniser drawn from a pool of experienced researchers within the Institute/Department approved by its Head/Director

Comment:

Authoriser's declaration:

- I have read the Research Ethics Policy and this has informed my judgement as to the category of assessment of this application.
- I understand that the applicant has taken account of the Research Ethics Policy and other relevant University policies in preparing this application.

- For Supervisors: I understand my responsibilities as supervisor, and will ensure, to the best of my abilities, that the student investigator abides by the University's Research Ethics Policy at all times.

Authoriser, please complete this table making it clear which version of the application form you are approving:

Version of the form (e.g. original version/ amended version following REC sub-group comments)	**Signature of authoriser**	**Date**

For Category A+ independent scrutiniser must also sign as authoriser.

For RO use: IF CATEGORY B: Signature of the Chair of the Research Ethics Committee.

Signature: …………………………………………………… Date: …………………………………

Please note that the Research Office will retain all applications for ethical approval for 5 years after the research project has ended as stated in the University's Privacy Standard

.

SECTION C: Ethical Review Questions

C1. Does the study involve human participants?

Yes/~~No~~

Participants in research are taken to include all those involved in the research activity either directly or indirectly and either passively, such as when being observed part of an educational context, or actively, such as when taking part in an interview procedure.

NB: the University does not conduct research on animals. If your proposed project involves animals in any way (including animal tissue) please seek advice from the Research Office before proceeding.

C2. Why should this research study be undertaken?

Brief description of purpose of study/rationale

Purpose of the study is to determine requirements for the development of the Security Culture Dashboard Proof of Concept. Participants are direct stakeholders of the system and therefore their input is essential to ensure the final deliverable meets expectations.

C3a. What are you planning to do?

Provide a description of the methodology for the proposed research, including proposed method and duration of data collection, tasks assigned to participants of the research and the proposed method and duration of data analysis. If the proposed research makes use of pre-established and generally accepted techniques, e.g. established laboratory protocols, validated questionnaires, please refer to this in your answer to this question. (Do not exceed 500 words). If it is helpful for the panel to receive further documentation describing the methodology then please append this to your application and make specific reference to it in box 3a below. For category B applications please include the data collection sheet as an appendix

The research will follow an Interpretivism approach, gathering qualitative requirements and expectations from stakeholders of the project deliverable. It is important that the underlying goals and wants of the stakeholders are captured to ensure the system developed effectively and efficiently meets their goals.

The primary method of data collection will be via interview.

Requirements will be captured during the analysis phase of the project. Additionally, stakeholders will be queried for feedback on the deliverable during the design and development and closedown phases of the project.

C3b. When are you planning to do it?

Please enter the anticipated start and end dates of your study (Consider at which point you will be involving human participants, this would typically be in the data collection/information gathering phase of the project but may be earlier):

Data collection will begin from the 16th February 2022 and will cease with project closure on the 24th June 2022. As previously outlined, stakeholders will be queried for their requirements and expectations of the project deliverable during the analysis phase of the project which is expected to end on the 1st April 2022. Further feedback will be sought after in the subsequent phases of the project.

C3c. Is this research externally funded?

~~Yes~~/**No**

If, the answer yes, please name the research funder(s) here:

C4. Where will the research be undertaken?

Briefly describe the location of the study, provide details of any special facilities to be used and any factors relating to the study site/location that might give rise to additional risk of harm or distress to participants or members of the research team together with measures taken to minimise and manage such risks:

Due to the ongoing Covid-19 pandemic, it is expected that the vast majority of data collection will occur online, with interviews taking place via Microsoft Teams. It is also possible that an interview could take place in-person at the project participants' place of work.

C5. Who are the participants?

Please indicate the number of participants in each of the groups in the table below. If the precise number of participants is not known then please make an estimate. Please enter '0' in the 'Numbers in study' column for those groups that are not included in your study. Please note that the examples provided of different sorts of vulnerability are not an exhaustive list.

Participant	Numbers in study
Adults with no known[2] health or social problems i.e. not in a vulnerable group:	**1**
Children aged 16-17[3] with no known[3] health or social problems:	**0**
Children under 16 years of age with no known[3] health or social problems:	**0**
Adults who would be considered as vulnerable e.g. those in care, with learning difficulties, a disability, homeless, English as a second language, service users of mental health services, with reduced mental capacity[4] Identify reason for being classed as vulnerable group and indicate 'numbers in study' in next column adjacent to each reason (expand the form as necessary): **………………………………………………..** **………………………………………………..**	**0**
Children (aged <18) who would be considered as particularly vulnerable e.g. those in care, with learning difficulties, disability, English as a second language Identify reason for being classed as vulnerable group and indicate 'numbers in study' in next column adjacent to each reason (expand the form as necessary): ……………………………………………….. ………………………………………………..	**0**
Other participants not covered by the categories listed above (please list): ***List other categories here:*** ……………………………………………..	**0**

C6a. Is there something about the context and/or setting which means that the potential risk of harm/distress to participants or research is lower than might be expected?

Answer: Yes/~~No~~

Consider if the study is part of routine activity which involves persons with whom you normally work in a typical work context e.g. Teachers working with children in a classroom setting, researchers in the performing arts working with performers, sports coaches working with athletes/players or research involving students in an academic setting.

Optional: Further information to justify answer to 6a

Primary participant and the applicant work together on a frequent/daily basis.

[2] Known to the researcher

[3] A summary of UK definition of 'Child' : http://www.nspcc.org.uk/Inform/research/briefings/definition_of_a_child_wda59396.html

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224660/Mental_Capacity_Act_code_of_practice.pdf

C6b. Are there any conflicts of interests which need to be considered and addressed?

(For example, does the research involve students whom you teach, colleagues, fellow students, family members? Do the funders, researchers, participants or others involved in the research have any vested interest in achieving a particular outcome? *See section 9 of the Research Ethics Policy (REP)*)

Answer: ~~Yes~~/**No**

If conflicts of interest are envisaged, indicate how they have been addressed:

C7. How will potential participants in the study be identified, approached and recruited?

Please include details of:

- *Basis for selection of participants in the study:* ***e.g. participants must be clinically obese adults; participants must be social workers over the age of 50; participants must have achieved Grade 5 in an appropriate musical instrument***
- *Any criteria for exclusions (e.g.* ***participants declaring a heart problem will be excluded****)*
- *How the selection criteria will be applied* ***e.g. Health questionnaire completed prior to joining the study***

The means by which the participants will be recruited ***(e.g. through an advert, through a school, through a sports club)****, please be specific about the medium of the advertisement/recruitment information* ***(e.g. poster, email, website, social media, word of mouth)*** *and mention any third parties who may be involved in supporting the recruitment.*

Only stakeholders of the project deliverable will be interviewed.

C8. Will any payment, gifts, rewards or inducements be offered to participants to take part in the study? *See section 11 of the REP.*

Answer: ~~Yes~~/**No**

Please provide brief details and a justification:

C9a. Is the process of the study and/or its results likely to produce distress, anxiety or harm in the participants even if this would be what they would normally experience in your work with them?

See section 5 of the REP.

Answer: ~~Yes~~/**No**

If you answered Yes to 9a, please answer 9b below:

C9b. Is the process of the study and/or its results likely to produce distress or anxiety in the participants *__beyond__* what they would normally experience in your work with them?

Answer: Yes/No

If yes this Application must be categorised as 'B'

Please provide details:

C9c. What steps will you take to deal with any distress or anxiety produced?

E.g. have a relevant professional on-hand to support distressed/anxious participants. Careful signposting to counselling or other relevant professional services. Other follow-up support.

C9d. What is the potential for benefit to research participants, if any?

E.g. Participants may gain an increased awareness of some issue or some aspect of themselves.

Participants are stakeholders in the final deliverable. The final artifact developed by the project will demonstrate to stakeholders how the data they already have available to them can be analysed and presented in a way that will facilitate informed decision making.

C10a. Will the study involve withholding information or misleading participants as part of its methodology? *(Please refer to sections 6.2 and 10 of the REP for further guidance)*

Answer: ~~Yes~~/No

Please provide details if this has not already been explained in section 3a:

C10b. Do you envisage that withholding information or misleading participants in this way will lead to any anxiety, distress or harm?

Answer: Yes/No

Please justify your answer to 10b:

It is the University Research Ethics Policy that all projects with the exception of double blind placebo trials (or similar) will be categorise as Category B. Double blind placebo trails (or similar) may be categorised as Category A+.

C11a. Does your proposal raise other ethical issues apart from the potential for distress, anxiety, or harm?

Answer: ~~Yes~~/No

C11b. If your answer to C11a. was 'yes', please briefly describe those ethical issues and how you intend to mitigate them and/or manage them in the proposed study, otherwise jump to C11c.

C11c Does your proposed study give rise to any potential risk of harm or distress to yourself or other members of the research team? OR is there any risk that you could find yourself in a vulnerable position as you carry out your study.

Answer: ~~Yes~~/No

If you answer 'yes' to either of these points please explain briefly what the risks are and what steps you are taking in order to minimise and manage those risks.

For example does your study involve you in 1-1 interviews in a private setting that might suggest precautions need to be taken relating to lone-working (See section 9 of the REP), Have you considered the likelihood of a participant(s) disclosing sensitive information to you about illegal or harmful behaviour and what actions you would take in such circumstances?

C12. Will informed consent of the participants be obtained and if so, how?

Answer: Yes/~~No~~

See section 6 of the REP to help you answer this question. Section 6.3.1 covers research that involves observing behaviour in a public place where gaining informed consent may not be practical or feasible.

When and how will informed consent be obtained? Will it be written or oral consent bearing mind that oral consent will not be considered adequate other than in exceptional circumstances and must be appropriately justified in your application?

NB: Ethical approval should, as a principle, be sought before research participants are approached.

Each participant will be given a consent form to sign, confirming that they agree to be a part of the research.

The consent form provided will be given to participants before an interview.

C13. Is there anyone whose permission should be sought in order to conduct your study? E.g. Head teacher of a school, parents/guardians of child participants.

Answer: ~~Yes~~/**No**

When and how will informed consent be obtained and from whom? Will it be written or oral consent bearing mind that oral consent will not be considered adequate other than in exceptional circumstances and must be appropriately justified in your application? If you are seeking to gain 'loco parentis' consent from a school rather than seeking individual parental consent please describe your reasoning.

C14. Do you need to seek the permission of any other organisations, individuals or groups other than outlined in section 13? E.g. the Research Ethics Committee of partner or participating organisations. Organisations like the NHS and the Prison Service have specific systems for granting ethical approval for research.

Answer: ~~Yes~~/**No**

Please note that all applications must go through the University of Chichester Application for Ethical Approval process and that they must meet the Research Ethics Policy (REP) requirements. Other prior approval will be taken into account but will not in itself be sufficient to gain University Research Ethics Approval. Each application must normally be accompanied by evidence (e.g. formal statement from the appropriate Ethics Committee) confirming approval by the external body (and any concerns/issues identified). In cases where an external body requires prior approval from the University Research Ethics Policy (such as some NHS work) the Research Ethics Committee (REC) may grant in principle approval pending written confirmation of ethical approval by the external body.

Please describe the permission that is required and how you will be seeking that permission: Please attach any relevant documentation e.g. letter, that relates to the seeking of the relevant permissions.

C15. It is normally required that a participant's data is treated confidentiality and stored securely at the outset of, during and after the research study. Will this be the case?

How long will data be stored before being destroyed?

Answer: Yes/~~No~~

If the answer is 'yes' please describe how you will be maintaining the confidentiality of participants' data. If the answer is 'no' please justify the exceptional circumstances that mean that confidentiality will not be guaranteed. See section 7 of the REP.

Please make reference to measures you are taking to ensure security of data from the point of data collection, transfer from notebooks/voice recorders etc., onto secure devices, to the point of analysis, sharing and final storage. If you are planning to store sensitive data on portable devices or media, you should only store such data if there is an immediate need and should remove these data when this immediate need no longer exists. All sensitive data stored on portable devices or media must be strongly encrypted greatly reducing the risk of the data falling into the wrong hands if the device or media is stolen. Actions should be in accordance with the University's Electronic Information Security Policy and Privacy Standard (please also refer to Section 9 of the University of Chichester's Data Protection Guidance for Staff). Signed consent forms should be stored in a locked cabinet for a period of 5 years.

Please provide details:

Participants' data including interview responses and meeting audio will be stored on the applicant's OneDrive which can only be accessed using the applicant's credentials. Data will be retained for 2 years following the end of the project on the 24th June 2022.

C16. It is normally required that the anonymity of participants is maintained and/or that an individual's responses are not linked with their identity. Will this be the case?

Answer: ~~Yes~~/No

If the answer is 'yes' please describe how you will be maintaining the anonymity of participants. If the answer is 'no' please justify the circumstances that mean that anonymity will not be guaranteed. See section 7 of the REP. NB: in group studies it is likely that each individual in the group will be aware that others in the group are participating in the study – they are therefore not anonymous to each other. However, their identity should not normally be associated with their individual responses. In some studies individual participants may not want their identify known to other participants and the study must be designed and undertaken accordingly.

Please provide details:

Any participants will be direct stakeholders of the project deliverable. It is essential that any responses captured can be attributed to the participant, to ensure the deliverable can be accurately assessed against their expectations and goals.

C17. Will participants have a right to comment or veto material you produce about them?

Answer: Yes/~~No~~

Please give details and if your answer is 'no' then please provide a justification.

C18. Does the project involve the use of or generation/creation of audio, audio visual or electronic material (e.g. Dictaphone recording, video recording) directly relating to the participants?

Answer: Yes/~~No~~

If yes, please describe how the collection and storage of this will be managed bearing in mind data protection, confidentiality and anonymity issues (see section 7 of the REP). If you are planning to store sensitive data on portable devices or media, you should only store such data if there is an immediate need and should remove these data when this immediate need no longer exists. All sensitive data stored on portable devices or media must be strongly encrypted greatly reducing the risk of the data falling into the wrong hands if the device or media is stolen

Audio from interviews with participants may be recorded for the purposes of answer recall and requirements validation. Any audio will be from Microsoft Teams meetings recordings and will be stored on the applicant's OneDrive.

C19. How will the participants be debriefed?

It is expected that wherever possible all participants will receive some form of debriefing. This might be a verbal debriefing or a written debriefing depending on the context of the study. Debriefing provides an opportunity to remind participants of the procedures and outcomes of the research, and to provide further assurances on areas such as confidentiality, anonymity, and retention of data. Projects that intentionally withhold information or deceive as part of their methodology must include a written debrief sheet. (Please refer to sections 6.1 and 6.2 of the REP for further guidance)

Participants will be debriefed verbally.

C20a. Might the research entail a higher than normal risk of damage to the reputation of the University, since it will be undertaken under its auspices? *(e.g. research with a country with questionable human rights, research with a tobacco company. See section 9.3 of the REP). If a research partnership has been established with an industry partner please ensure that the University is not linked to claims made by that company regarding benefits of their products unless substantiated evidence of beneficial effects is available.*

Answer: ~~Yes~~/**No**

C20b. If your answer to 20a was yes, please describe the potential risk to the University's reputation and how this risk will be mitigated. If no, please jump to C20c.

C20c. Does the research concern groups or materials that might be construed as extremist, security sensitive or terrorist?

Answer: ~~Yes~~/**No**

If 'Yes' please describe how you will manage the research so that it is not in breach of the Terrorism Act (2006) which outlaws the dissemination of records, statements and other documents that can be interpreted as promoting or endorsing terrorist acts. For example, relevant documents, records, information and data pertaining to the research can be stored on a secure University server. Contact the Head of Research in the first instance if you are unsure as to how to proceed.

If you answered ***Yes*** *to question C20c then please complete the additional pro-forma available from the Research Ethics Moodle:* ***Approval to undertake research concerning groups or materials that might be construed as extremist, security sensitive or terrorist****. Please append the completed form to this application.*

C20d. Does your research fit into any of the following security-sensitive categories? If so, please indicate which:

i. Commissioned by the military: ~~Yes~~/**No**

ii. Commissioned under an EU security call: ~~Yes~~/**No**

iii. Involve the acquisition of security clearances: ~~Yes~~/**No**

If you answered yes to any of the above please provide further information

C21a. Will your results be available in the public arena? (e.g. publication in journals, books, shown or performed in a public space, presented at a conference, internet publication and placing a dissertation in the library) *see section 8 of the REP*.

Answer: Yes/~~No~~

If yes, please provide brief details:

NB: Please note that if participants wish to exercise their right to withdraw or request erasure of their personal data following collection and analysis this may not be possible having regard to permitted exemptions for research under data protection legislation i.e. where it would seriously impair the achievement of the research objectives. Notwithstanding the above, data subjects must still be advised of their rights to object in the information sheet, which can only be overridden if the "research is necessary for a task carried out for reasons of public interest.

The results of the project will be made available in the University of Chichester's library for future students.

C21b. Will your research data be made available in the public arena?

Certain research funding bodies require that research data is made Open Access i.e. freely available to the public. The University has a Research Data Policy that outlines the expectations and requirements for researchers at the University. Contact the Director of Research in the first instance if you are unsure as to how to proceed.

Answer: ~~Yes~~/**No**

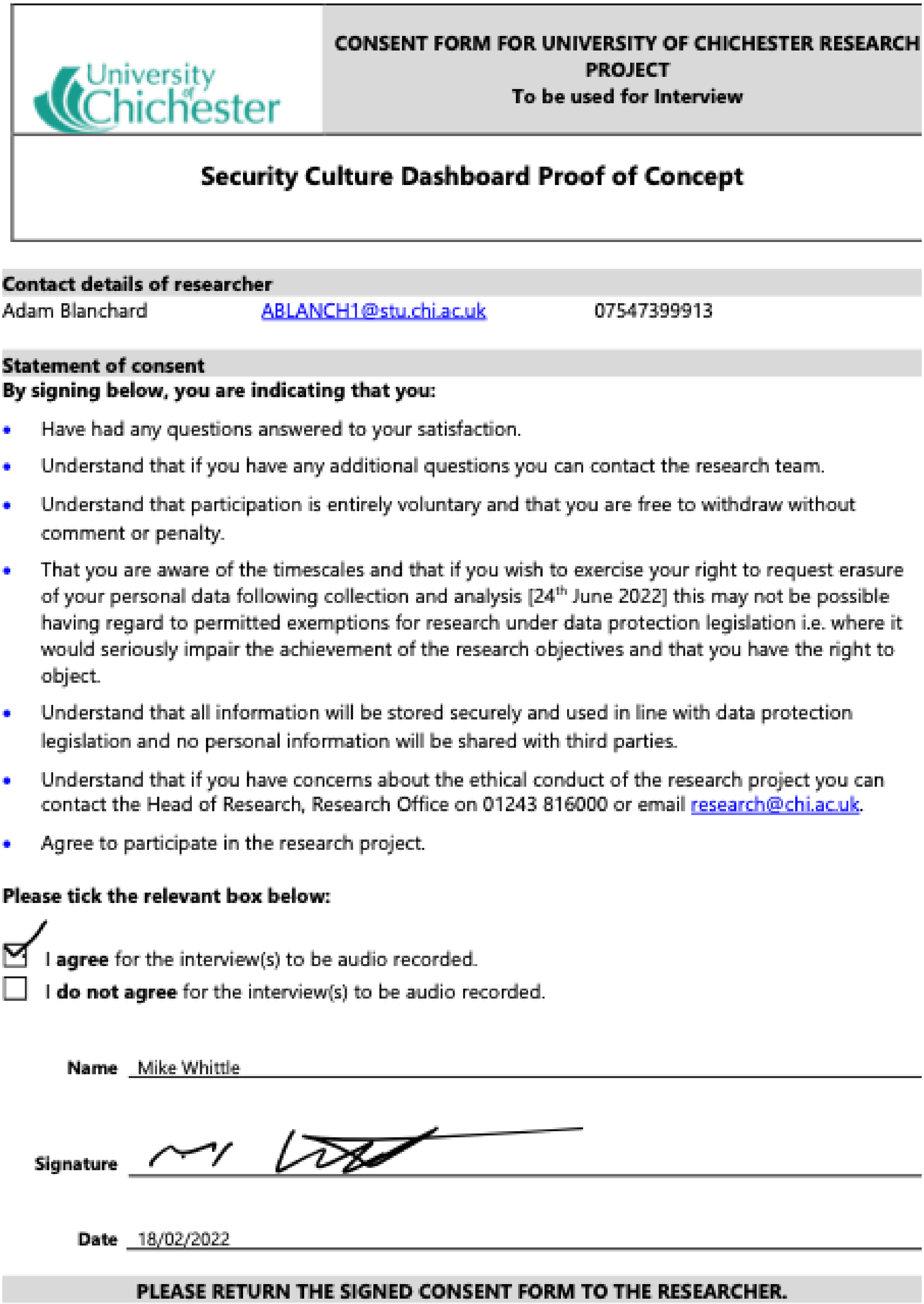
If yes, please provide brief details as to how the data will be prepared for public access including an overview of the meta-data that will accompany published data sets. Please also confirm that your intentions with respect to making data open access are clearly communicated to participants so that they can provide informed consent:

C22. Are there any additional comments or information you consider relevant, or any additional information that you require from the Committee?

N/A

[end of form]

Appendix F – Signed Consent Form



CONSENT FORM FOR UNIVERSITY OF CHICHESTER RESEARCH PROJECT
To be used for Interview

Security Culture Dashboard Proof of Concept

Contact details of researcher

Adam Blanchard ABLANCH1@stu.chi.ac.uk 07547399913

Statement of consent

By signing below, you are indicating that you:

- Have had any questions answered to your satisfaction.
- Understand that if you have any additional questions you can contact the research team.
- Understand that participation is entirely voluntary and that you are free to withdraw without comment or penalty.
- That you are aware of the timescales and that if you wish to exercise your right to request erasure of your personal data following collection and analysis [24th June 2022] this may not be possible having regard to permitted exemptions for research under data protection legislation i.e. where it would seriously impair the achievement of the research objectives and that you have the right to object.
- Understand that all information will be stored securely and used in line with data protection legislation and no personal information will be shared with third parties.
- Understand that if you have concerns about the ethical conduct of the research project you can contact the Head of Research, Research Office on 01243 816000 or email research@chi.ac.uk.
- Agree to participate in the research project.

Please tick the relevant box below:

☑ I **agree** for the interview(s) to be audio recorded.

□ I **do not agree** for the interview(s) to be audio recorded.

Name Mike Whittle

Signature

Date 18/02/2022

PLEASE RETURN THE SIGNED CONSENT FORM TO THE RESEARCHER.

Appendix G – Detailed System Requirements

No.	Functional/ Non-Functional	Type	Requirement	User Story
1	Functional	Must have	Deliver a summary chart for each Security Culture process	As a **dashboard user** I must be able to **view a summarised chart for each of the Security Culture processes**
2	Functional	Must have	Produce a standard set of SSE branded data visualisations	As a **dashboard user** I must be able to **view a standard set of SSE branded data visualisations**
3	Functional	Must have	Consistent page layouts in accordance with SSE branding	As a **dashboard user** I must be able to **view a standard set of pages that share a common look and feel and are compliant with the SSE brand guidelines**
4	Functional	Must have	User authentication	As a **dashboard user** I must be able to **authenticate to the system before accessing metrics and data**

5	Functional	Must have	Error handling	As a **dashboard user** I must be able to **view a custom error page if I use an unsupported browser or encounter an error**
6	Functional	Must have	Phishing Resilience dashboards	As a **dashboard user** I must be able to **view the following three dashboards for the Phishing Resilience process:** • **Executive Summary** • **Department breakdowns** • **Simulation breakdowns**
7	Functional	Must have	Passwords Management dashboards	As a **dashboard user** I must be able to **view the following four dashboards for the Password Management process:** • **Executive summary** • **Account type breakdowns**

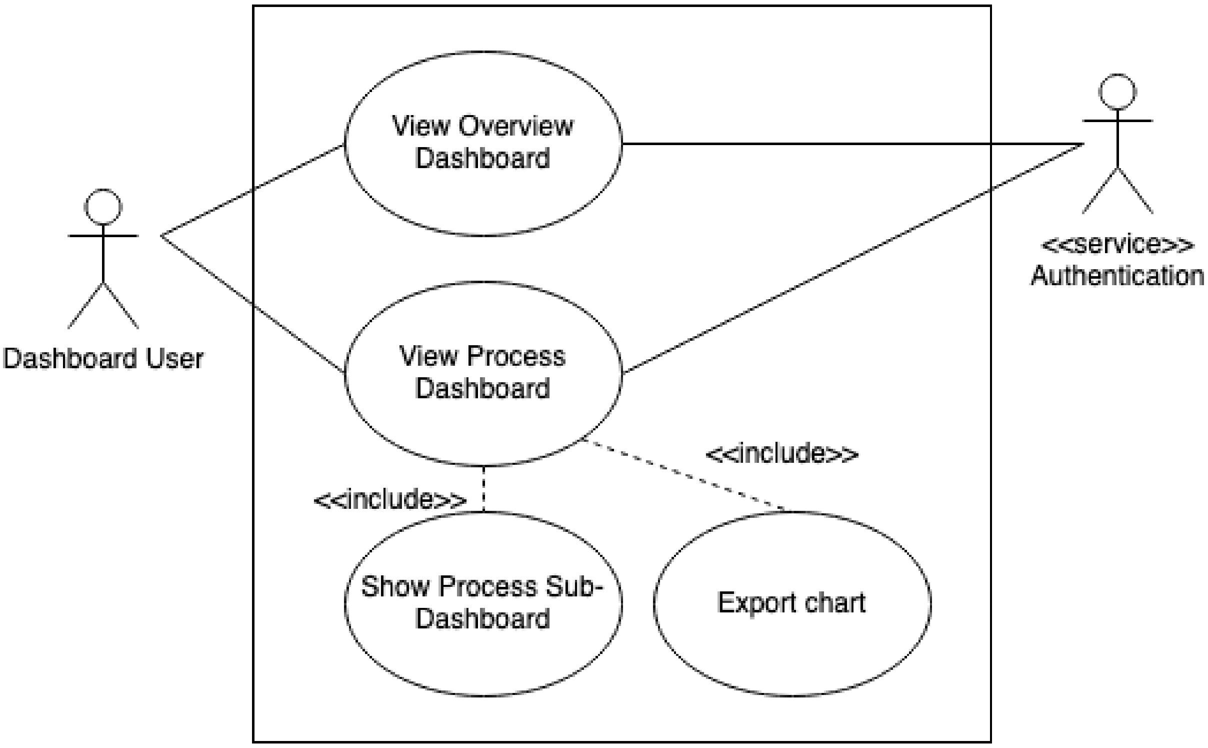
				• **Department breakdowns** • **Quarterly breakdowns**
8	Functional	Must have	Chart export feature	As a **dashboard user** I must be able to **export dashboard charts in a simple and intuitive way**
9	Non-Functional	Must have	System performance	As a **dashboard user** I must be able to **access the system from an SSE standard issue device and have it run efficiently**
10	Non-Functional	Must have	Improvement over existing process	As a **dashboard user** I must be able to **generate reports in a faster manner than the existing manual process**
11	Non-Functional	Must have	Incorporated best practices for interface design, dashboard design and data visualisation	As a **dashboard user** I must be able to **access a system that incorporates best practices in the following areas:** • **Interface design**

				• **Dashboard design** • **Data visualisation**
12	Functional	Could have	Database integration	As a **dashboard user** I could be able to **access Security Culture data stored in a database**
13	Functional	Could have	Admin page	As a **dashboard user** I could be able to **access an admin page to administer system settings and configuration**
14	Functional	Could have	Data ingestion tool	As a **dashboard user** I could be able to **import data directly into the system using standard data formats such as excel**
	Functional	Won't have	Multiple user types	As a **dashboard user** I will not have **the ability to log in as multiple user types**
	Functional	Won't have	Integrations with other systems	As a **dashboard user** I will not be able to **access data directly pulled from other SSE systems**

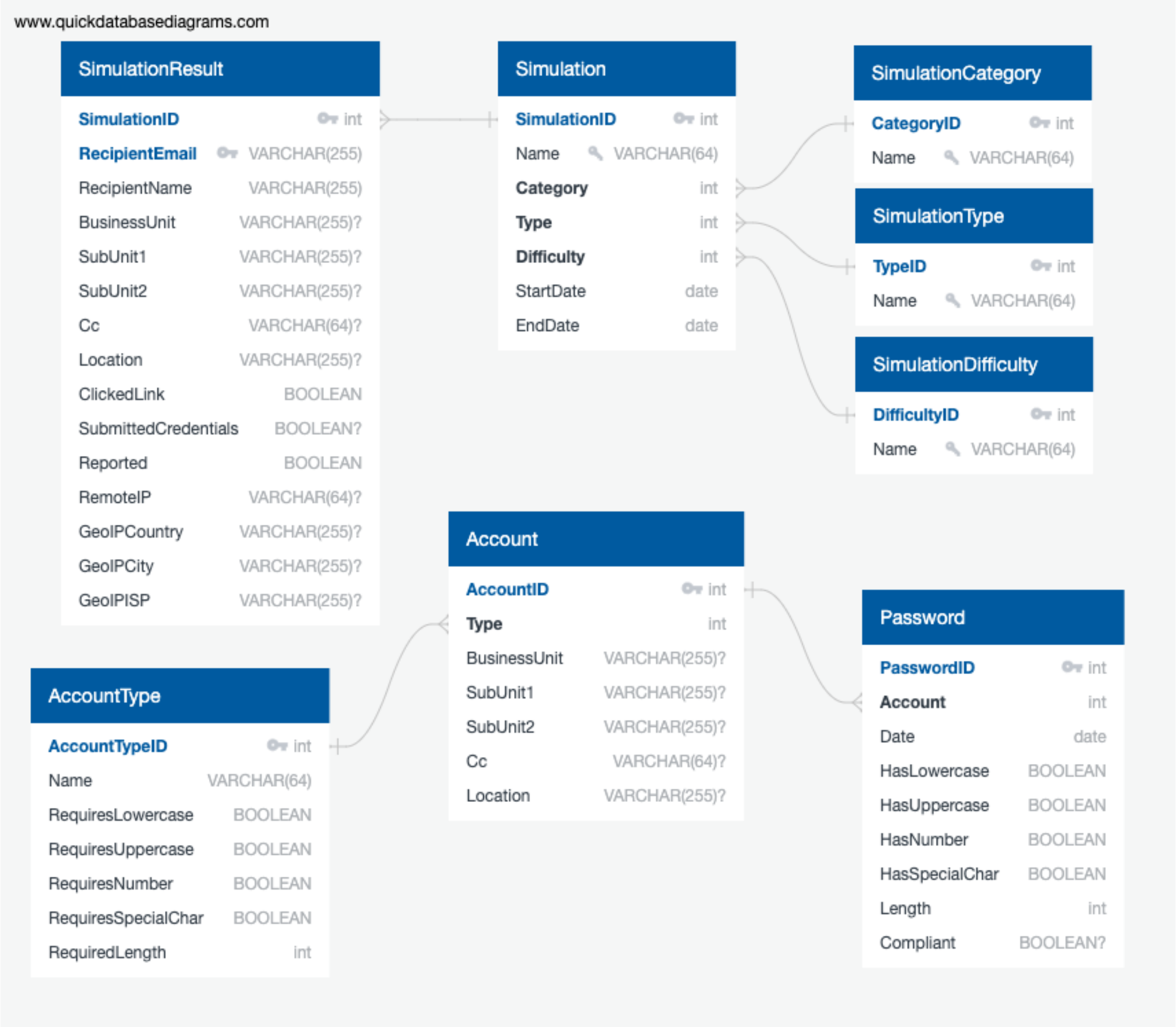
	Non-Functional	Won't have	Real data	As a **dashboard user** I will not be able to **view real SSE statistics**
	Non-Functional	Won't have	SSE system architecture	As a **system administrator** I will not be **constrained to develop using only SSE standard system architectures**

Appendix H – Design Artefacts

UML Case Diagrams



Entity Relationship Diagrams



www.quickdatabasediagrams.com

SimulationResult	
SimulationID	🔑 int
RecipientEmail	🔑 VARCHAR(255)
RecipientName	VARCHAR(255)
BusinessUnit	VARCHAR(255)?
SubUnit1	VARCHAR(255)?
SubUnit2	VARCHAR(255)?
Cc	VARCHAR(64)?
Location	VARCHAR(255)?
ClickedLink	BOOLEAN
SubmittedCredentials	BOOLEAN?
Reported	BOOLEAN
RemoteIP	VARCHAR(64)?
GeoIPCountry	VARCHAR(255)?
GeoIPCity	VARCHAR(255)?
GeoIPISP	VARCHAR(255)?

Simulation	
SimulationID	🔑 int
Name	🔍 VARCHAR(64)
Category	int
Type	int
Difficulty	int
StartDate	date
EndDate	date

SimulationCategory	
CategoryID	🔑 int
Name	🔍 VARCHAR(64)

SimulationType	
TypeID	🔑 int
Name	🔍 VARCHAR(64)

SimulationDifficulty	
DifficultyID	🔑 int
Name	🔍 VARCHAR(64)

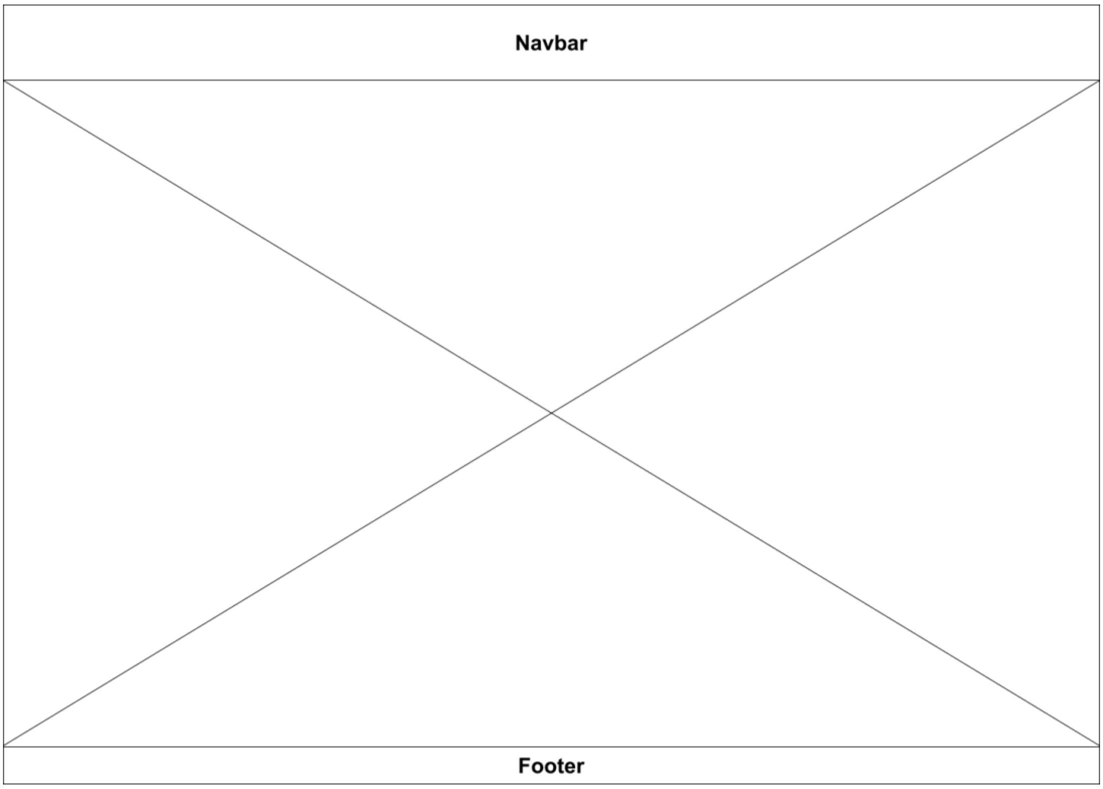
Account	
AccountID	🔑 int
Type	int
BusinessUnit	VARCHAR(255)?
SubUnit1	VARCHAR(255)?
SubUnit2	VARCHAR(255)?
Cc	VARCHAR(64)?
Location	VARCHAR(255)?

AccountType	
AccountTypeID	🔑 int
Name	VARCHAR(64)
RequiresLowercase	BOOLEAN
RequiresUppercase	BOOLEAN
RequiresNumber	BOOLEAN
RequiresSpecialChar	BOOLEAN
RequiredLength	int

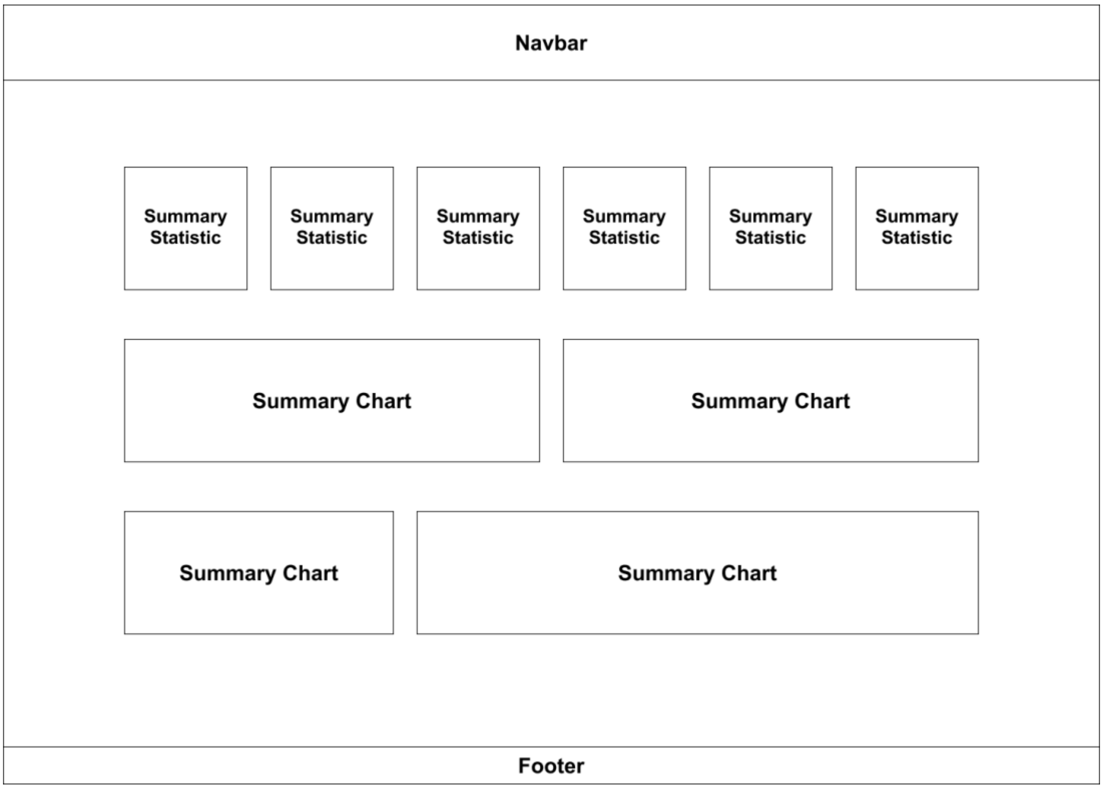
Password	
PasswordID	🔑 int
Account	int
Date	date
HasLowercase	BOOLEAN
HasUppercase	BOOLEAN
HasNumber	BOOLEAN
HasSpecialChar	BOOLEAN
Length	int
Compliant	BOOLEAN?

Interface Wireframes

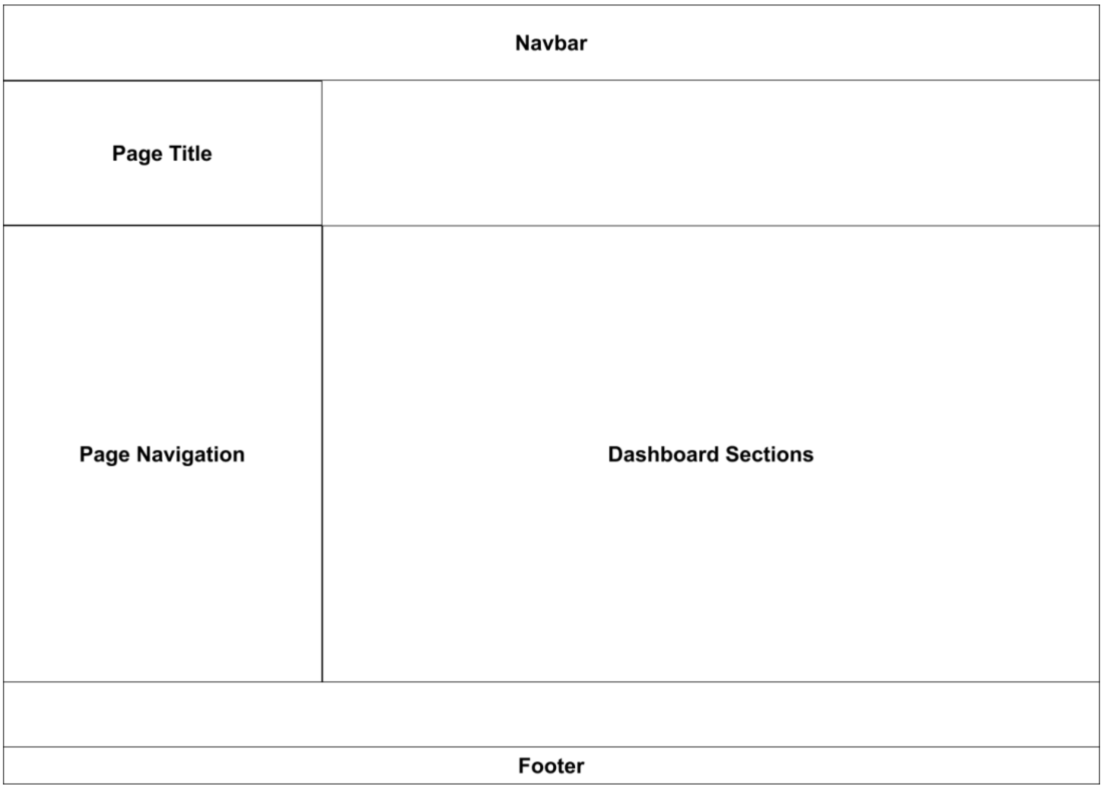
Page Structure



Home Dashboard

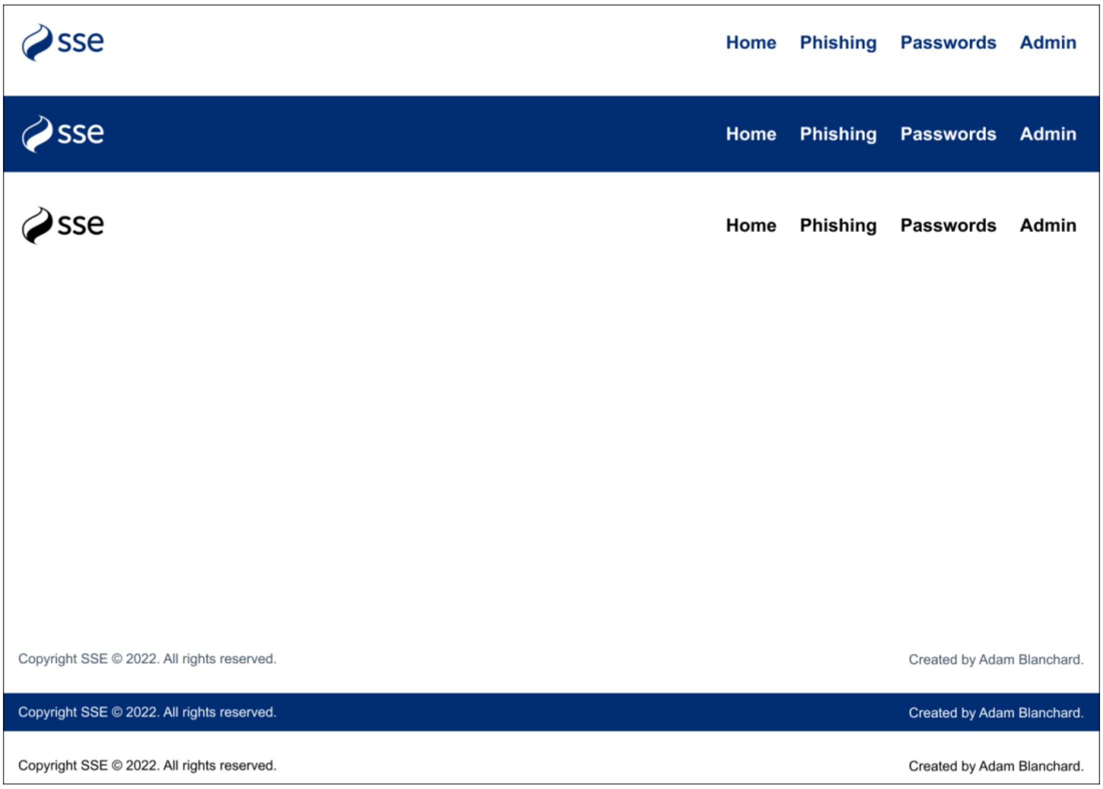


Process Overview Page



System Prototypes

Headers and Footers

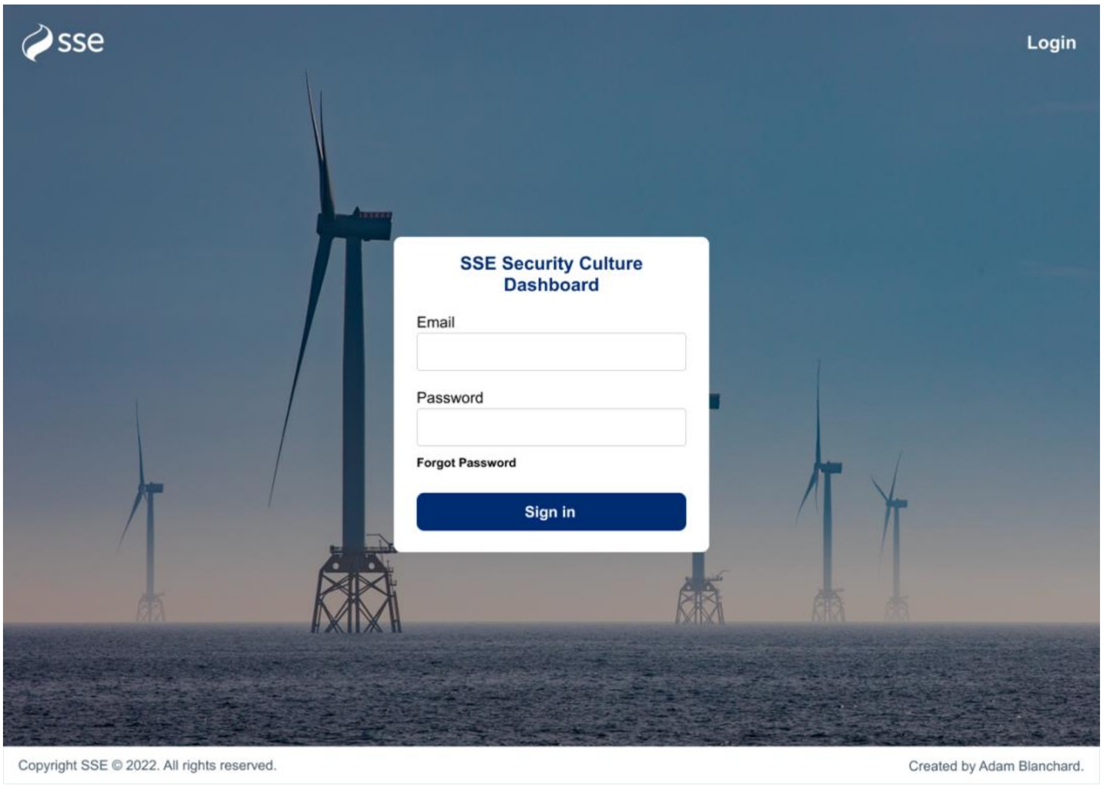


Copyright SSE © 2022. All rights reserved. Created by Adam Blanchard.

Copyright SSE © 2022. All rights reserved. Created by Adam Blanchard.

Copyright SSE © 2022. All rights reserved. Created by Adam Blanchard.

Login Page

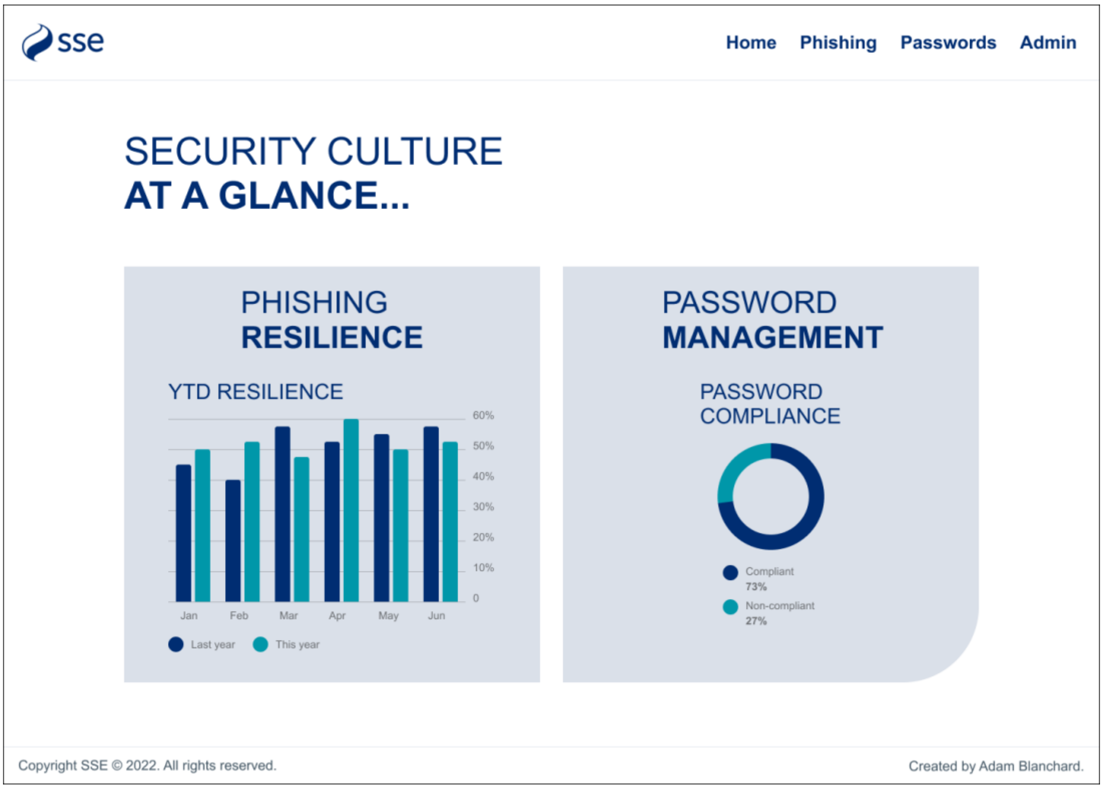


SSE Security Culture Dashboard

Copyright SSE © 2022. All rights reserved.

Created by Adam Blanchard.

Home Page



SECURITY CULTURE
AT A GLANCE...

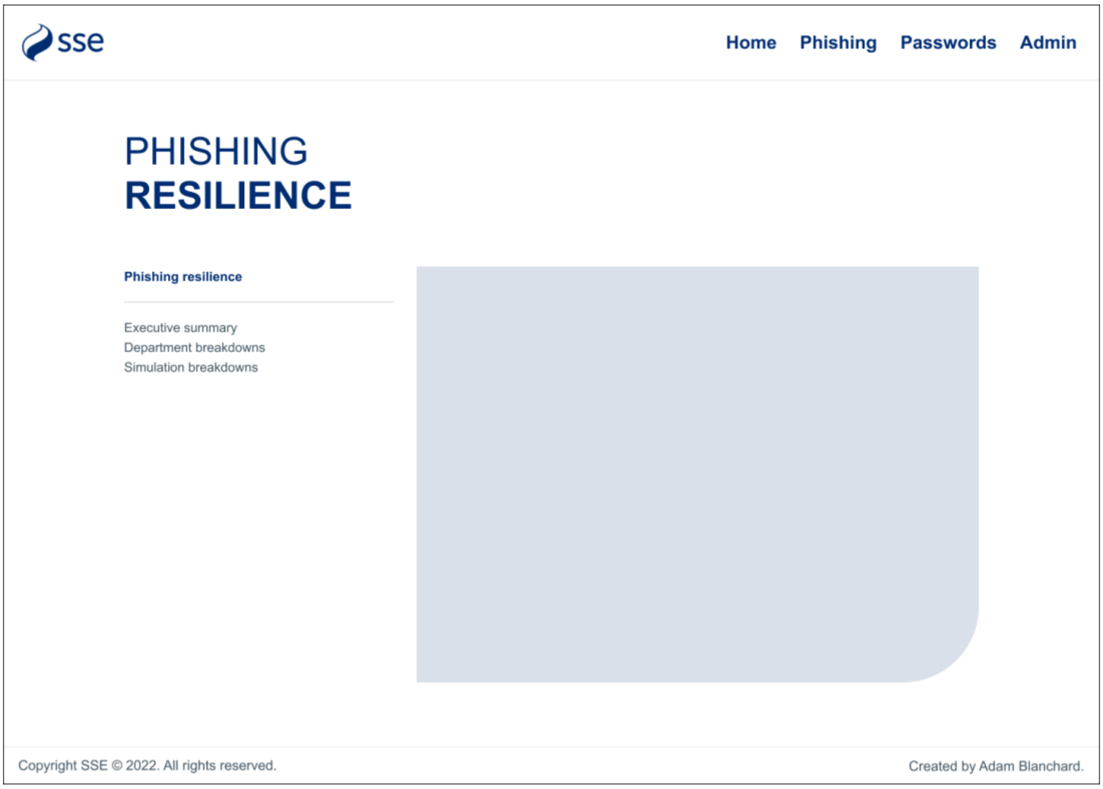
PHISHING
RESILIENCE

PASSWORD
MANAGEMENT

Copyright SSE © 2022. All rights reserved.

Created by Adam Blanchard.

Phishing Page



PHISHING
RESILIENCE

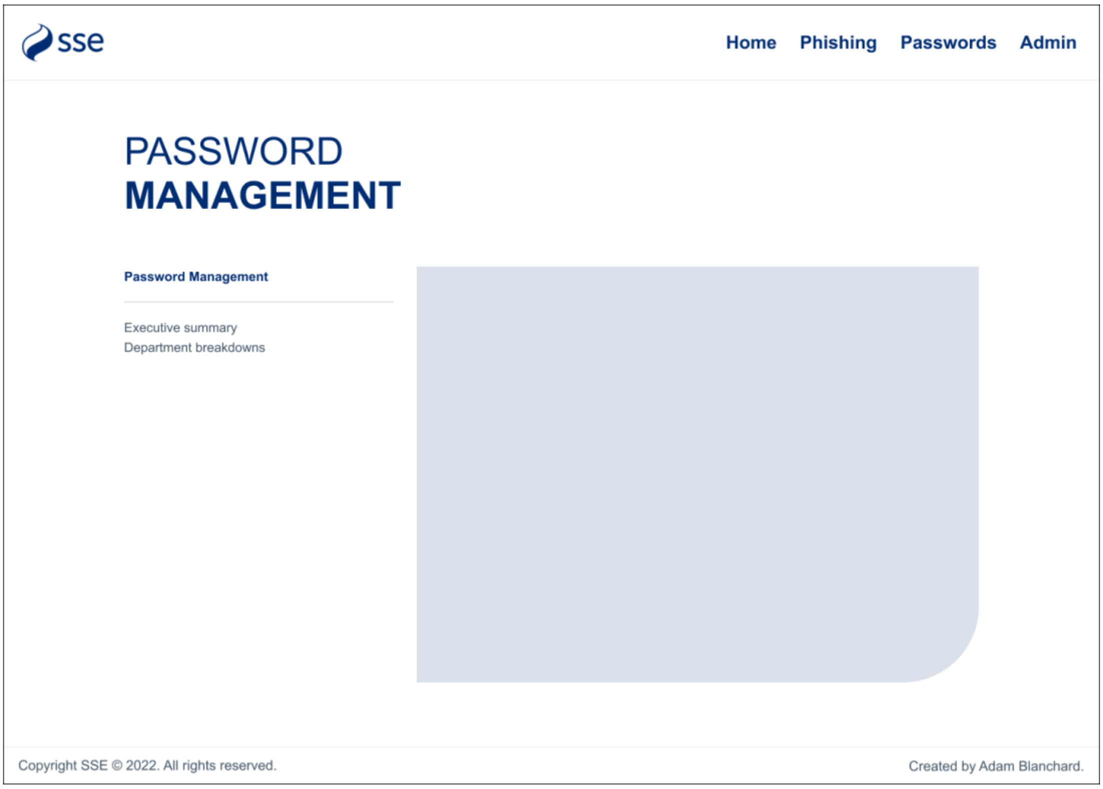
Phishing resilience

Executive summary
Department breakdowns
Simulation breakdowns

Copyright SSE © 2022. All rights reserved.

Created by Adam Blanchard.

Passwords Page



PASSWORD
MANAGEMENT

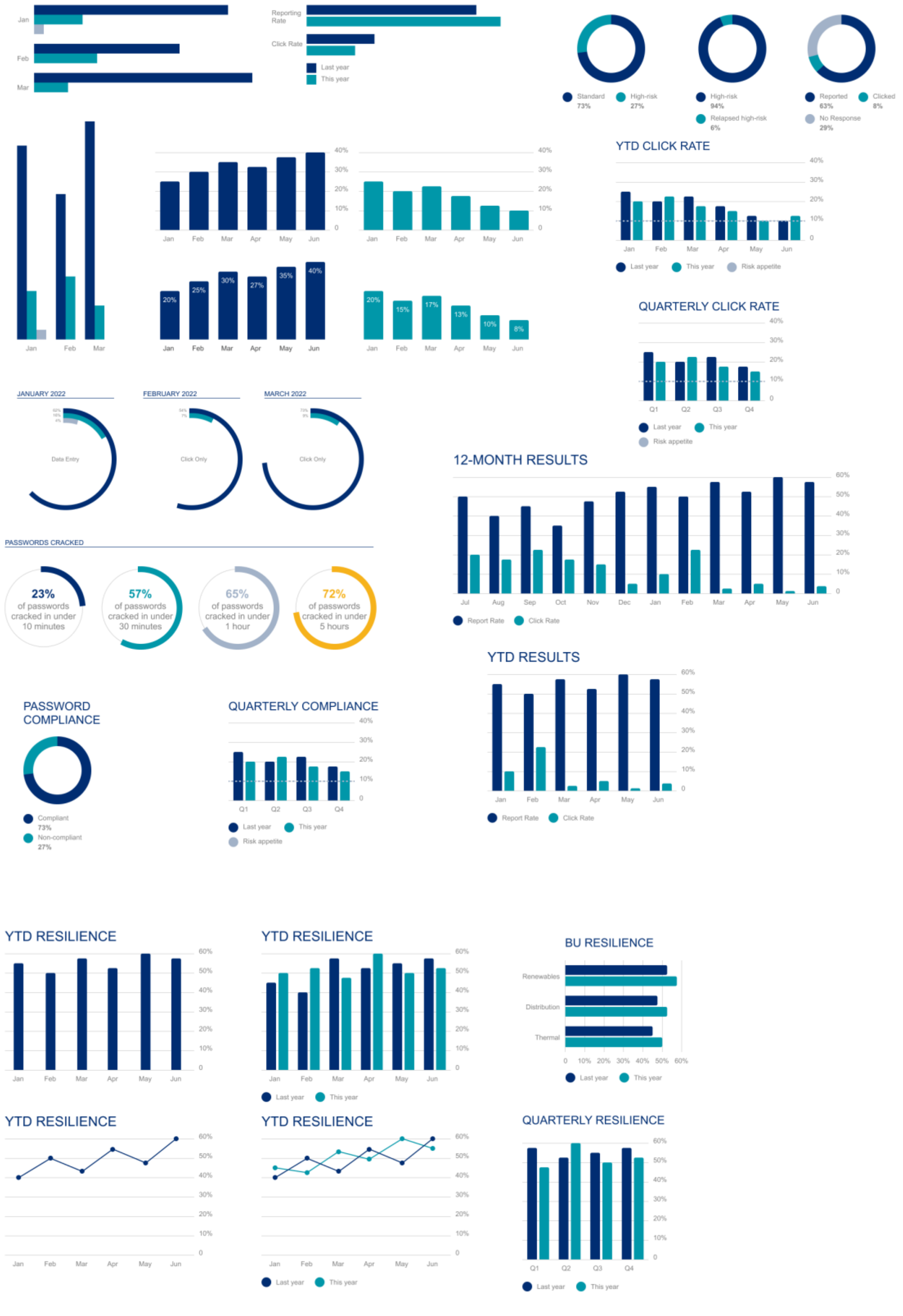
Password Management

Executive summary
Department breakdowns

Copyright SSE © 2022. All rights reserved.

Created by Adam Blanchard.

Charts


Jan
Feb
Mar
Reporting Rate
Click Rate
Last year
This year
Standard 73%
High-risk 27%
High-risk 94%
Relapsed high-risk 6%
Reported 63%
Clicked 8%
No Response 29%
YTD CLICK RATE
Last year
This year
Risk appetite
QUARTERLY CLICK RATE
Q1
Q2
Q3
Q4
20%
25%
30%
27%
35%
40%
20%
15%
17%
13%
10%
8%
JANUARY 2022
FEBRUARY 2022
MARCH 2022
Data Entry
Click Only
Click Only
12-MONTH RESULTS
Report Rate
Click Rate
PASSWORDS CRACKED
23% of passwords cracked in under 10 minutes
57% of passwords cracked in under 30 minutes
65% of passwords cracked in under 1 hour
72% of passwords cracked in under 5 hours
YTD RESULTS
PASSWORD COMPLIANCE
Compliant 73%
Non-compliant 27%
QUARTERLY COMPLIANCE
YTD RESILIENCE
YTD RESILIENCE
BU RESILIENCE
Renewables
Distribution
Thermal
YTD RESILIENCE
YTD RESILIENCE
QUARTERLY RESILIENCE
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
0
10%
20%
30%
40%
50%
60%

Appendix I – Requirements Delivery Review

No.	Requirement	User Story	Delivered?	Comments
1	Deliver a summary chart for each Security Culture process	As a **dashboard user** I must be able to **view a summarised chart for each of the Security Culture processes**	Yes	**Project Team** – Summary charts are presented on the homepage to provide an overview of Security Culture
2	Produce a standard set of SSE branded data visualisations	As a **dashboard user** I must be able to **view a standard set of SSE branded data visualisations**	Yes	**Project Team** – All data visualisations are underpinned by best-practices and SSE brand guidelines. Examples charts can be seen on the /chart page.
3	Consistent page layouts in accordance with SSE branding	As a **dashboard user** I must be able to **view a standard set of pages that share a common look and feel and are compliant with the SSE brand guidelines**	Yes	**Project Team** – All pages use SSE brand guidelines throughout and format inspiration has been taken from the sse.com website.
4	User authentication	As a **dashboard user** I must be able to **authenticate to the system before**	Yes	**Project Team** – Azure SSO is required to access the

		accessing metrics and data		website. Only SSE employees can view the deliverable.
5	Error handling	As a **dashboard user** I must be able to **view a custom error page if I use an unsupported browser or encounter an error**	Yes	**Project Team** – Accessing a page that doesn’t exist, using an unsupported browser or navigating to /404 will present the branded error page.
6	Phishing Resilience dashboards	As a **dashboard user** I must be able to **view the following three dashboards for the Phishing Resilience process:** • **Executive Summary** • **Department breakdowns** • **Simulation breakdowns**	Yes	**Project Team** – All of the outlined dashboards can be viewed on the /phishing page.
7	Passwords Management dashboards	As a **dashboard user** I must be able to **view the following four dashboards for the**	Yes	**Project Team** – All of the outlined dashboards can be viewed on the

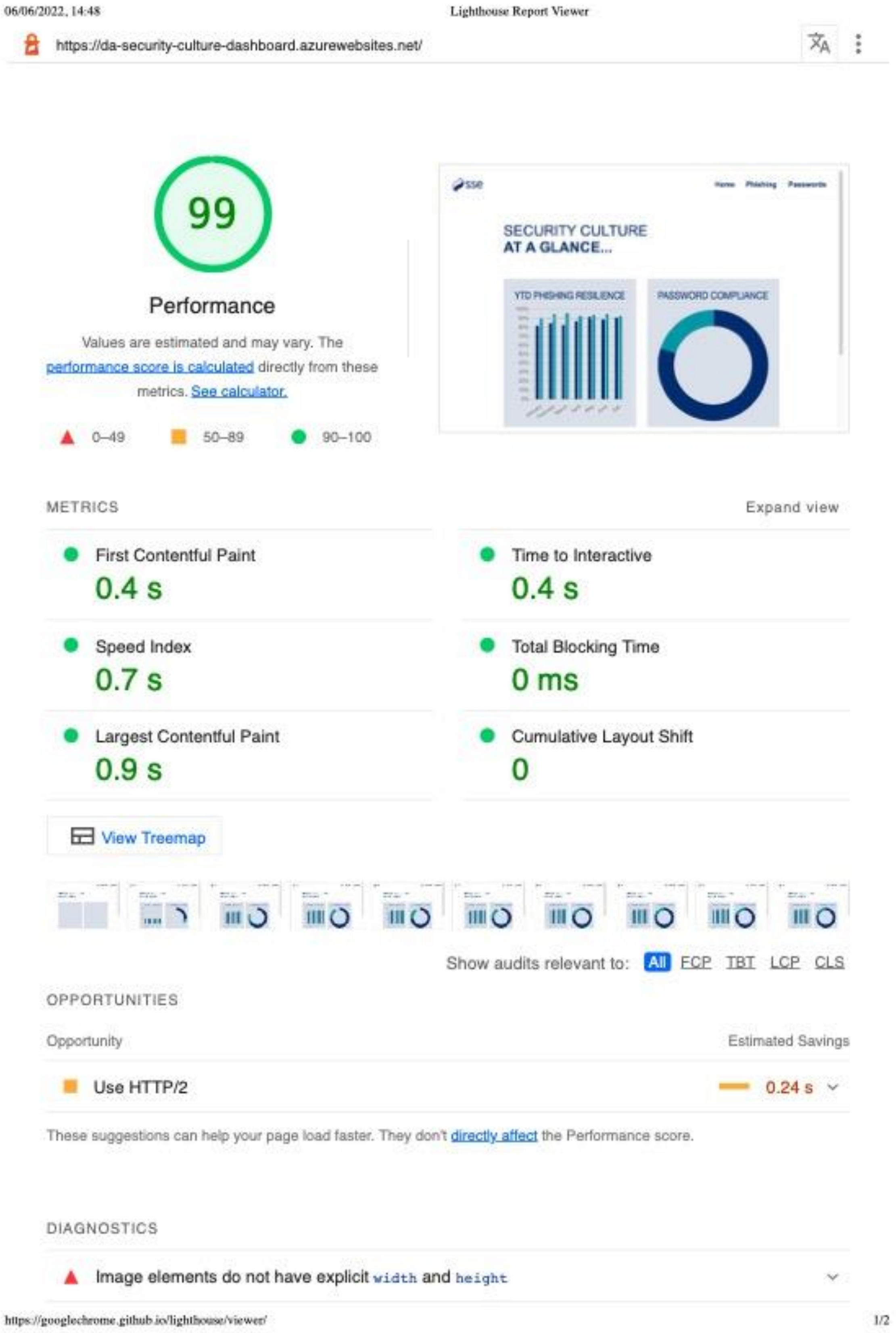
		Password Management process: • **Executive summary** • **Account type breakdowns** • **Department breakdowns** • **Quarterly breakdowns**		/passwords page.
8	Chart export feature	As a **dashboard user** I must be able to **export dashboard charts in a simple and intuitive way**	Yes	**Project Team** – The chart export button can be found on all dashboards, excluding the Security Culture at a glance dashboard.
9	System performance	As a **dashboard user** I must be able to **access the system from an SSE standard issue device and have it run efficiently**	Yes	**Project team** – Final Google Lighthouse performance score of 99/100 for all pages. See Appendix J – System Performance Reports for details.

10	Improvement over existing process	As a **dashboard user** I must be able to **generate reports in a faster manner than the existing manual process**	Yes	**Project Team –** Need confirmation from client on this.
11	Incorporated best practices for interface design, dashboard design and data visualisation	As a **dashboard user** I must be able to **access a system that incorporates best practices in the following areas:** • **Interface design** • **Dashboard design** • **Data visualisation**	Yes	**Project Team –** Best practices outlined within the project report have been incorporated at all stages of development. Google's Material Design has underpinned all elements of the deliverable.
12	Database integration	As a **dashboard user** I could be able to **access Security Culture data stored in a database**	No	**Project Team –** Requirement scoped as a could have. Insufficient time to deliver.
13	Admin page	As a **dashboard user** I could be able to **access an admin page to administer system settings and configuration**	No	**Project Team –** See requirement 12 comment.

14	Data ingestion tool	As a **dashboard user** I could be able to **import data directly into the system using standard data formats such as excel**	No	**Project Team –** See requirement 12 comment.

Appendix J – System Performance Reports

Homepage



06/06/2022, 14:48 Lighthouse Report Viewer

https://da-security-culture-dashboard.azurewebsites.net/

99

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

METRICS Expand view

● First Contentful Paint
0.4 s

● Time to Interactive
0.4 s

● Speed Index
0.7 s

● Total Blocking Time
0 ms

● Largest Contentful Paint
0.9 s

● Cumulative Layout Shift
0

View Treemap

Show audits relevant to: All FCP TBT LCP CLS

OPPORTUNITIES

Opportunity	Estimated Savings
■ Use HTTP/2	0.24 s

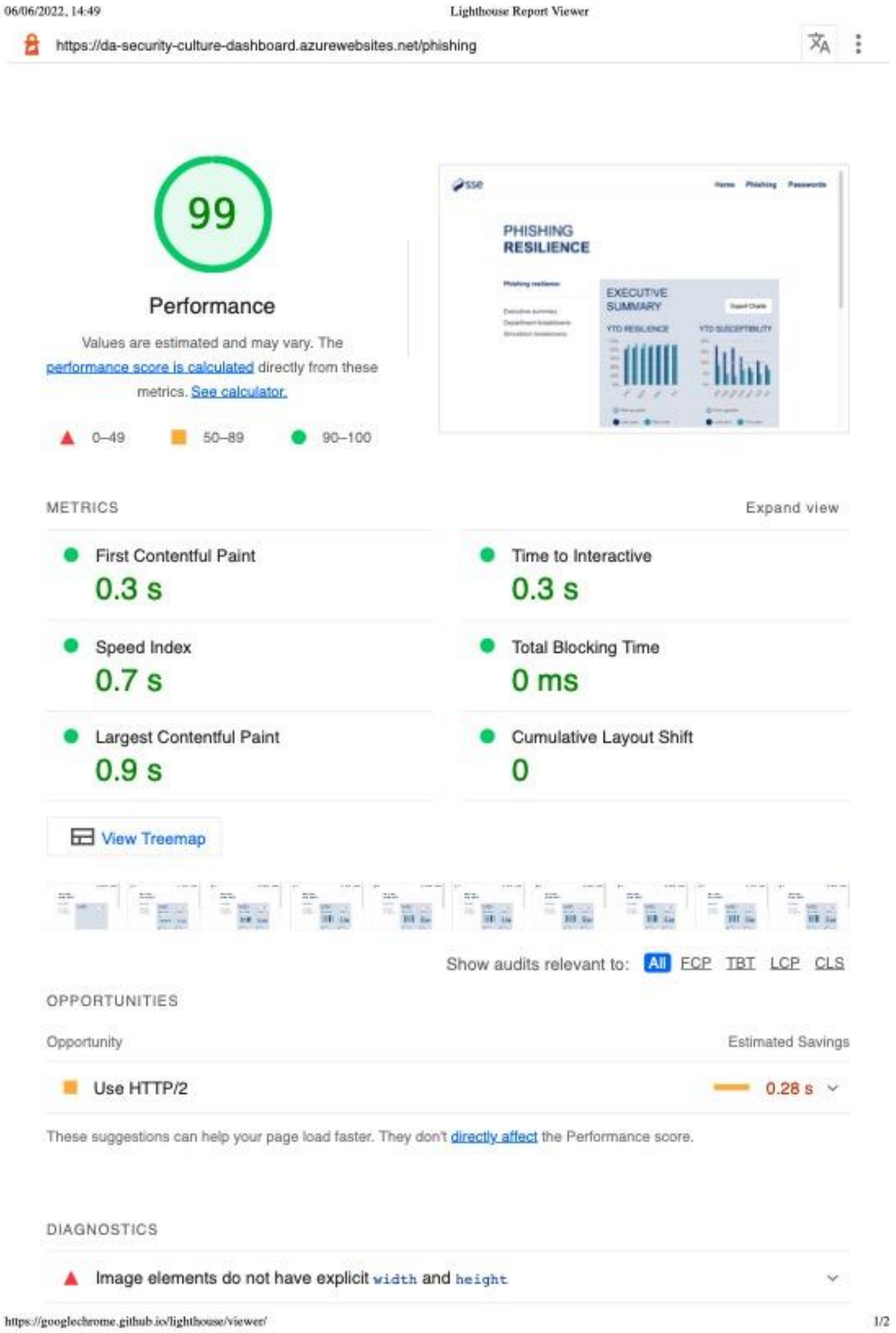
These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

▲ Image elements do not have explicit `width` and `height`

https://googlechrome.github.io/lighthouse/viewer/ 1/2

Phishing Resilience Page



06/06/2022, 14:49 Lighthouse Report Viewer

https://da-security-culture-dashboard.azurewebsites.net/phishing

99

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

METRICS Expand view

● First Contentful Paint 0.3 s	● Time to Interactive 0.3 s
● Speed Index 0.7 s	● Total Blocking Time 0 ms
● Largest Contentful Paint 0.9 s	● Cumulative Layout Shift 0

View Treemap

Show audits relevant to: All FCP TBT LCP CLS

OPPORTUNITIES

Opportunity	Estimated Savings
■ Use HTTP/2	0.28 s

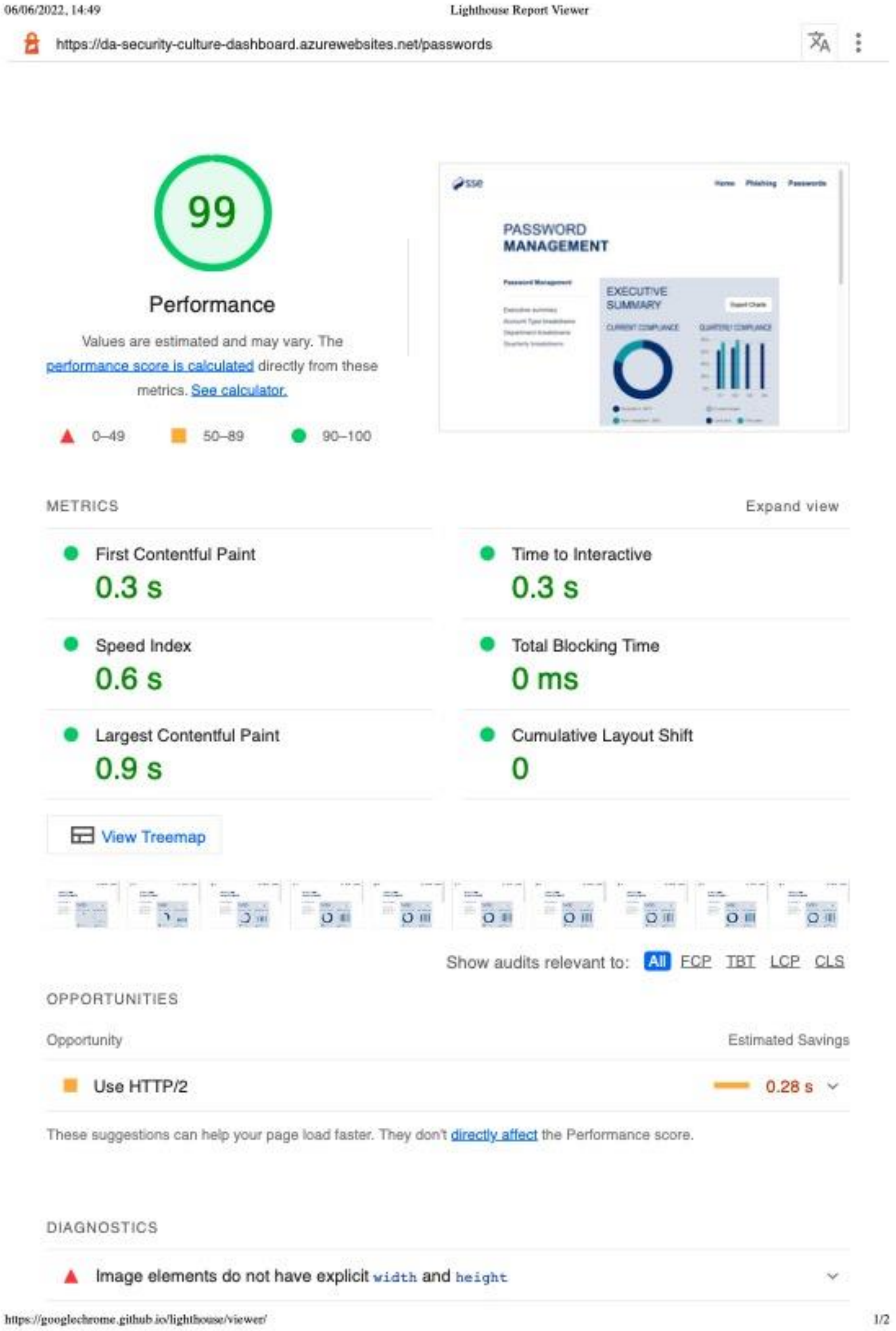
These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

▲ Image elements do not have explicit `width` and `height`

https://googlechrome.github.io/lighthouse/viewer/ 1/2

Password Management Page



06/06/2022, 14:49 Lighthouse Report Viewer

https://da-security-culture-dashboard.azurewebsites.net/passwords

99

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

METRICS Expand view

● First Contentful Paint 0.3 s	● Time to Interactive 0.3 s
● Speed Index 0.6 s	● Total Blocking Time 0 ms
● Largest Contentful Paint 0.9 s	● Cumulative Layout Shift 0

View Treemap

Show audits relevant to: All FCP TBT LCP CLS

OPPORTUNITIES

Opportunity	Estimated Savings
■ Use HTTP/2	0.28 s

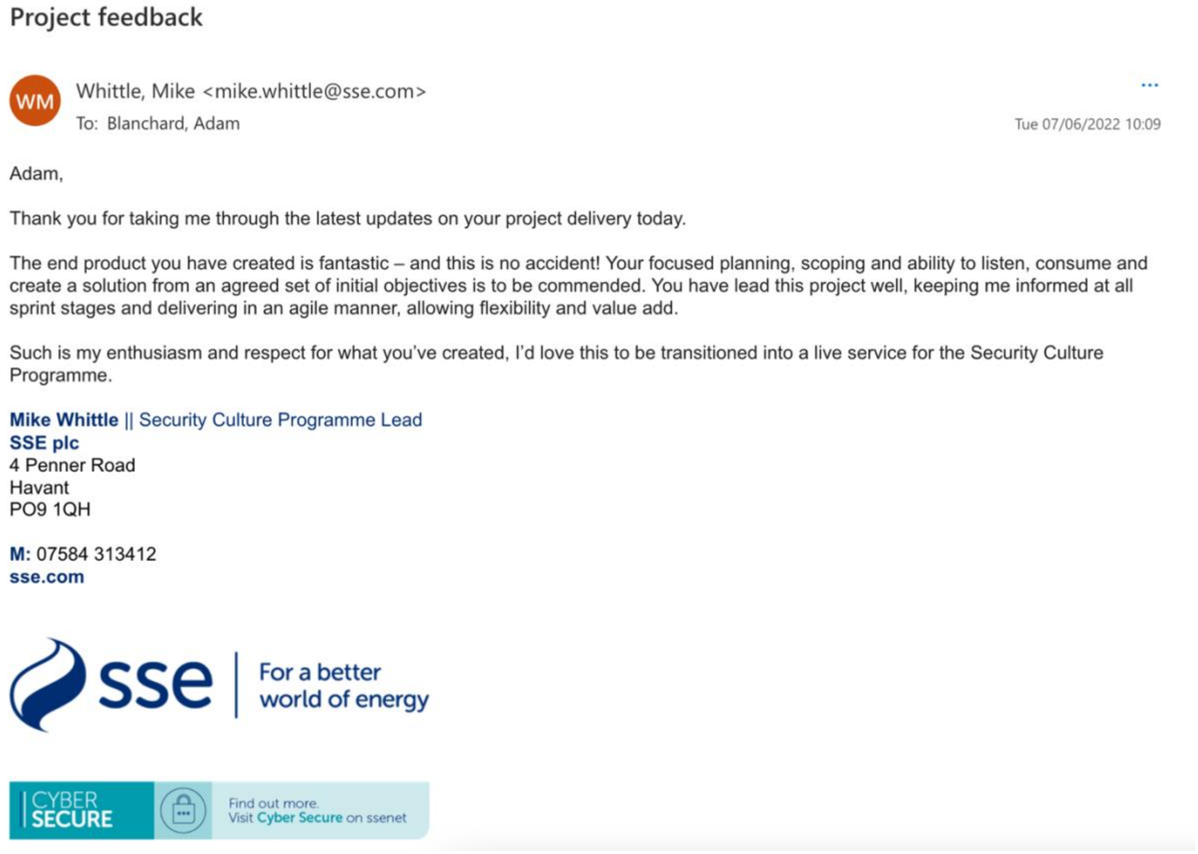
These suggestions can help your page load faster. They don't directly affect the Performance score.

DIAGNOSTICS

▲ Image elements do not have explicit `width` and `height`

https://googlechrome.github.io/lighthouse/viewer/ 1/2

Appendix K – Client Feedback



Project feedback

WM Whittle, Mike <mike.whittle@sse.com>

To: Blanchard, Adam

Tue 07/06/2022 10:09

Adam,

Thank you for taking me through the latest updates on your project delivery today.

The end product you have created is fantastic – and this is no accident! Your focused planning, scoping and ability to listen, consume and create a solution from an agreed set of initial objectives is to be commended. You have lead this project well, keeping me informed at all sprint stages and delivering in an agile manner, allowing flexibility and value add.

Such is my enthusiasm and respect for what you've created, I'd love this to be transitioned into a live service for the Security Culture Programme.

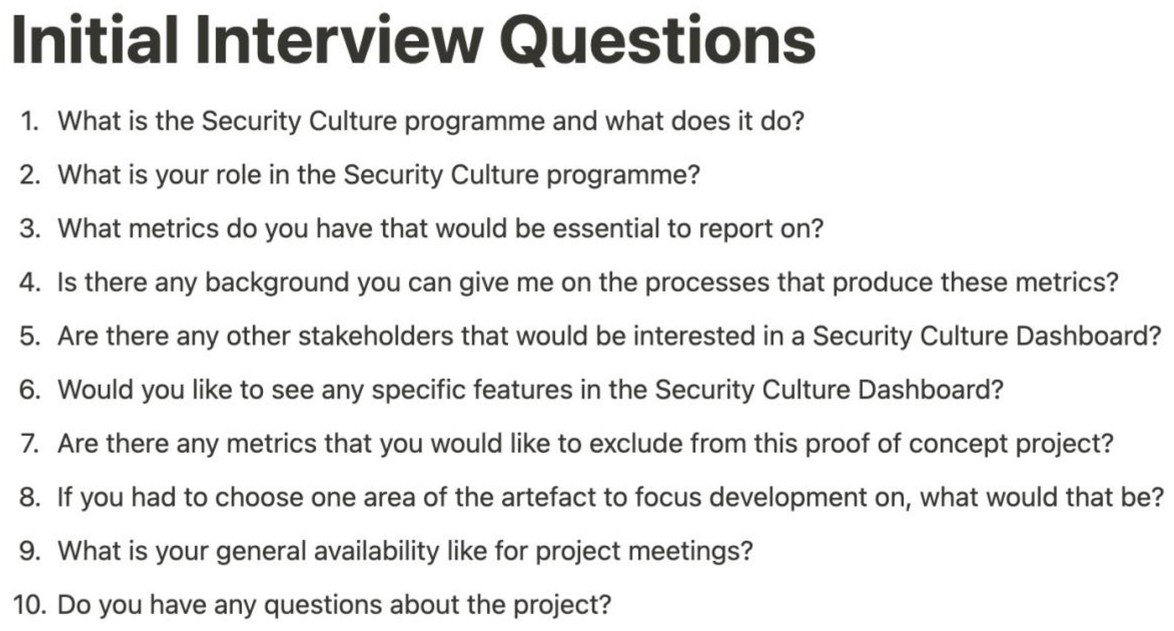
Mike Whittle || Security Culture Programme Lead
SSE plc
4 Penner Road
Havant
PO9 1QH

M: 07584 313412
sse.com

sse | For a better world of energy

CYBER SECURE Find out more. Visit Cyber Secure on ssenet

Appendix L – Client Interview Questions



Initial Interview Questions

1. What is the Security Culture programme and what does it do?
2. What is your role in the Security Culture programme?
3. What metrics do you have that would be essential to report on?
4. Is there any background you can give me on the processes that produce these metrics?
5. Are there any other stakeholders that would be interested in a Security Culture Dashboard?
6. Would you like to see any specific features in the Security Culture Dashboard?
7. Are there any metrics that you would like to exclude from this proof of concept project?
8. If you had to choose one area of the artefact to focus development on, what would that be?
9. What is your general availability like for project meetings?
10. Do you have any questions about the project?