The Life and Times of Miscreants, Attackers, Abusers, Misusers and Evil Folk:
An Action Research Study Focussing on Agile Methods to Manage Information Security Risk.

By: ***Alex Harding***

Supervisor: ***Katie Taylor***

A project report submitted in partial fulfilment of the

Degree of Master of Science - Agile Leadership

Table of Contents

Table of Figures 8

Table of Tables 11

Acknowledgements 13

Abstract 14

1 Introduction 15

2 Background 17

2.1 Information Security / Cyber Security 17

Risk 20

Hacking 21

Ethical Hacking & Penetration Testing 22

Miscreants 22

Methods for Approaching Information Security. 22

2.2 Agility 23

Facilitated Workshops 24

Rich Picture 24

Stakeholders 25

Personas 26

Attacker Personas 27

Use Cases & Use Case Diagrams 27

Abuse Cases 27

User Stories & Epics 28

Abuser Stories / Security Stories 29

3 Literature Review 30

3.1 Objectives 30

3.2 Related Work 30

3.3 Search Strategy 31

3.4 Search Criteria 32

3.5 Key Themes 33

Are Agile Methods Insufficient for Capturing Non Functional Requirements? 33

Pairing or Nesting User Stories and Abuser Stories 33

Threats 34

User Story Constraints 34

Security Backlog 35

Penetration Testing 35

3.6 Discussion 35

4 Research Objectives 37

RQ1. Are Abuse Cases and Abuser Stories effective means of documenting Information Security Risk in a Software Project. 37

RQ2. Can Specific Agile Approaches succeed in aiding the prioritisation and treatment of Information Security Risk. 37

5 Context 38

5.1 Personal Context 38

5.2 Organisational Context *38*

5.3 Theoretical Context *38*

6 Method **39**

6.1 Research Design *39*

Participants 39

Permissions 40

6.2 Research Methodology *40*

Why Action Research? 40

Validity 41

Monitoring of Actions and Learning 41

6.3 Research Ethics *41*

Ethics Statement 41

Research Stakeholders 43

7 Sector Survey **44**

7.1 Objectives *44*

7.2 Survey Methodology *44*

7.3 Results *45*

7.4 Survey Discussion *52*

7.5 Survey Conclusions *54*

8 Action Research - Data Gathering **55**

8.1 Prior to Improvements *55*

8.2 Outset & Post Cycle Team Surveys 55

9 Action Research - Cycles 57

9.1 Prior to Cycles 57

9.2 Initial Cycle 58

Planning 58

Rich Picture 58

Attacker Personas 59

Post Cycle Review & Retrospective 61

9.3 Second Cycle 64

Planning 64

Abuse Case Diagram 65

Abuser Stories 67

Post Cycle Review & Retrospective 70

Cycle 2 – Post Script 72

9.4 Final Cycle 73

Planning 73

Risk Assessment 74

Prioritising Mitigations 84

Post Cycle Review & Retrospective 84

10 Findings After Three Cycles 86

11 Discussion 88

12 Critical Evaluation 91

Assumptions & Experience 91

Value of Research & Findings 93

Project Management & Completion 93

13 Conclusion 95

RQ1. Are Abuse Cases and Abuser Stories effective means of documenting Information Security Risk in a Software Project. 95

RQ2. Can Specific Agile Approaches succeed in aiding the prioritisation and treatment of Information Security Risk. 95

References 96

Appendices 106

Appendix 1 – Email to JISC CMIS and UK Security Groups 106

Appendix 2 – Survey Questions 107

Appendix 3 – Email to Mike Cohn 111

Appendix 4 – Participation Statement 112

Appendix 5 – Team Survey 113

Appendix 6 – Facilitated Workshop Agendas 115

Appendix 6.1 – First Cycle, Rich Picture of High Level Threats Workshop 115

Appendix 6.2 – First Cycle, Attacker Persona Workshop 115

Appendix 6.3 – Second Cycle, Abuse Case Workshop 116

Appendix 6.4 – Second Cycle, User Story Workshop 116

Appendix 6.4 – Third Cycle, Risk Day 117

Appendix 7 - Project Management 118

Appendix 8 – Data.....119

Table of Figures

Figure 1 - The CIA and DAD Information Security Triads 17

Figure 2 - Ten Steps to Cyber Security 18

Figure 3 - Five Key Mitigations of Cyber Essentials 19

Figure 4 - Risk Measurement Calculation. 20

Figure 5 - Example of a Rich Picture from [55] 25

Figure 6 - Example of a Persona Map from [61] 26

Figure 7 - Example Attacker Persona Adapted from [64]. 27

Figure 8 – Cohn/Connextra User Story Format. 28

Figure 9 – Root Definition Format. 28

Figure 10 - Graph Depicting Growth of Published Papers Over Time. 32

Figure 11 - Resourcing 46

Figure 12 - Cyber Security Certifications 47

Figure 13 - Information Security Policies 47

Figure 14 – Information Security Risk Assessments 48

Figure 15 – Importance of Cyber Security. 48

Figure 16 – Cyber Security Risks. 49

Figure 17 – Usage of Agile Methods & Techniques. 50

Figure 18 – Agile Maturity. 51

Figure 19 – Willingness to Utilise Agile Methods for Information Security Risk Documentation. 51

Figure 20 - Calculated Agility Scores vs Willingness to Use Agile Methods for Information Security Risk 52

Figure 21 - Likert Style Questions from the Team Survey 56

Figure 22 – Plot of Median Responses to Pre Project Questions 57

Figure 23 - Initial Threats Rich Picture 59

Figure 24 - Miscreant Types 60

Figure 25 - Attacker Persona (Paper) 60

Figure 26 - Attacker Persona (Electronic) 61

Figure 27 - Plot of Median Responses to Post Cycle 1 Questions 63

Figure 28 - Abuse Cases and Mis-Actors added to a Use Case Diagram 66

Figure 29 - Abuser Stories in the Jira Project 69

Figure 30 - Abuser Stories on the Project Kanban Board 69

Figure 31 - Post Cycle 2 Scores 70

Figure 32 - Additional Abuser Story 72

Figure 33 - Risk Measurement Calculation. 74

Figure 34 - Impact & Likelihood Scores 74

Figure 35 - Risk Impact / Severity Matrix 75

Figure 36 - MoSCoW Prioritisation for Risk 76

Figure 37 - Asset & Service Priorities in Jira 78

Figure 38 - Service Record from Jira Showing Priorities and Linked Assets 78

Figure 39 - Service Portfolio with Priorities Added.....79

Figure 40 - Selection of Physical Assets with Priorities Added 79

Figure 41 - Sample of Threats stored in Jira 80

Figure 42 – Sample of Risks stored in Jira.....82

Figure 43 - Sample Risks defined in Jira.....83

Figure 44 - Sample Mitigation from Jira.....84

Figure 45 - Post Cycle 3 Scores 84

Table of Tables

Table 1 – Microsoft's STRIDE Model. 21

Table 2 – Volume of Search Results returned by Google Scholar for varying terms. 31

Table 3 - Comparison of Risk Calculations 34

Table 4 – Ranking of Threats (JISC vs Government vs Survey Respondents). 53

Table 5 - Incident Statistics (Inc Info. Sec.) 55

Table 6 - Issues, Questions and Value for the First Cycle 58

Table 7 - Cycle 1 WWW & EBI. 62

Table 8 - Outcomes of the First Cycle 64

Table 9 - Issues, Questions and Value for the Second Cycle 65

Table 10 - Epics in the RunshawPay Project 67

Table 11 - Abuser Stories 68

Table 12 - WWW & EBI From Cycle 2 70

Table 13 - Outcomes of the Second Cycle 71

Table 14 - Issues, Questions and Value for the Third Cycle 73

Table 15 - Risk Treatment Options 77

Table 16 - RACI Model for Information Security Risk Management/Assessment 77

Table 17 - Post Cycle 3 WWW & EBI 85

Table 18 - Graph Depicting Growth in Scores over the Cycles. 86

Table 19 - Overall Median Scores (Per Cycle) 86

Table 20 - Terms with Emotive Entries Struck-through.....89

Table 21 - Post Project WWW & EBI.....91

Acknowledgements

Guidance and support from a number of parties has been instrumental in the completion of this research project. Throughout the course of my Masters level studies, my supervisor Katie Taylor has provided a wealth of advice, guidance and most of all a critical, inquisitive eye. Katie constantly encourages the group to question approaches, and experiment with new ideas.

"An Agile Way to an Agile MSc" features in the header of the VLE page for the course and that has certainly been a major force in the production of this research and my wider studies.

Thanks must also go to my workplace colleagues, my ever dedicated IT Services team and the College's Senior Management Team. Their support and encouragement has been of paramount importance.

I would also like to thank the wider Further Education IT community for their participation in the survey phase of the project, specifically those respondents from the JISC CMIS and Security groups.

Abstract

The Information Security landscape is ever changing, and faced with new threats, new legislation and decreasing finances it's imperative that we consider new and novel methods to analyse and document these risks.

This Action Research project report explores the deployment of a number of Agile Techniques and Methods, experimenting with adaptations to current practice in order to reduce the burden of traditional approaches to Information Security.

A background analysis of the current literature related to these methods takes place, which is also supplemented with a survey, considering the attitudes towards Information Security and Agility across the Further Education Sector.

A phased approach to improvements is adopted, splitting the experimentation into three distinct Action Research Cycles. Feedback has been gathered at each stage, both observationally and via the use of Surveys.

A number of conclusions are drawn, revealing that these Methods and Techniques have fulfilled the requirements set out in the initial research questions. The success of the project can also be attributed to the Agile approaches used to manage the project.

1 Introduction

College and University networks have become the source of a number of high profile virus and denial-of-service attacks in recent years [1]. A recent publication revealed that 100% of Colleges and Universities were susceptible to data exfiltration via the use of Phishing campaigns [2]. This is set against a recent report showing that less than half of all education senior managers see Cyber Security as a high priority, allocating only an average of £1,810 in the 2016/2017 financial year to cyber security projects [3].

During 2014 the UK Government mandated, that contractors must have achieved Cyber Essentials[4] certification in order to bid for some Central Government contracts . Specifically, those involving the handling of personal information [5]. Certification is encouraged in all other contract areas. The Scottish Government have also set out an action plan [6] and expect Public Sector Bodies, including FE & HE institutions to prepare for Cyber Essentials accreditation by March 2018, and to further extend the reach by June 2018. As of March 2019, 51% of Institutions had achieved this [7].

Compounding the intentions of the Government, May 25th 2018, saw the countdown towards enforcement of the EU's new Data Protection legislation, the General Data Protection Legislation (GDPR) come to an end [8]. Information security falls firmly within the GDPR's realms of Integrity and Confidentiality. GDPR Article 25 states that approved certification mechanisms may be used as an element to demonstrate compliance with the requirements of Data Protection by Design and by Default [8].

As of March 2019, the Information Commissioners Office are yet to prosecute any organisation under the provisions of the GDPR and recent cases still relate to DPA1998 Enforcement [9]. The changes to policies & processes following the new legislation, resulted in the number of businesses identifying a cyber security attack in the last 12 months (to March 2019) fell to 32% from 43% the previous year [10].

A recent survey carried out by JISC found that within FE only 35% of organisations have a strategic Cyber Security lead [11]. Furthermore only 29% of FE colleges are working toward Cyber Essentials certification with a small fraction 4% having already achieved certification [11]. Data published by the Information Commissioners Office reports that the Education

Sector has saw a 40% increase in the number of reported Information Security incidents in the latter part of 2017 [12].

The College has now achieved the minimum standards imposed by the Cyber Essentials [4] framework, however at the outset of this project, no methodical Information Security Risk Assessment has been carried out and nor did an Information Security Management System exist.

This Action Research report documents a number of the processes implemented, the progress and lessons learnt during the implementation of a formal Information Security Management System as per the ISO27000 series [13] International Standard at a UK Further Education Institution. The Study focusses particularly on the use of Agile tools and techniques to analyse, document and treat Information Security Risk both within the colleges Systems Development function, and in the wider IT Services group.

The Action Research study is supported by a survey across the Further Education Sector, considering attitudes towards Cyber Security and Agility.

The following section sets out a number of key concepts that feature in the study and additionally further supporting information.

2 Background

The Action Research study intends to deploy a number of Agile methods and tools in order to improve the way the College's IT Services function approaches the analysis and documentation of Information Security Risk. With that in mind, it is first appropriate to consider the wider aspects of Information Security and Agility, and look at possible avenues for application.

2.1 Information Security / Cyber Security

Information Security is the *art* of protecting Information and Information Systems from unauthorised access, use, disclosure, disruption, modification, or destruction [14]. Information Security revolves around the protection of Confidentiality, Integrity and Availability known as the CIA triad [15]. These facets are sometimes expressed in their negative forms as Disclosure, Alteration and Denial the DAD triad [15]. Internationally, a number of attempts at standardising Information Security Practice exist [4], [13], [16].

Traditional	**Negative Variant**
Confidentiality	Disclosure
Integrity	Alteration
Availability	Denial

Figure 1 - The CIA and DAD Information Security Triads

Ten Steps to Cyber Security

Launched by the UK Government in 2012, and later redefined in 2016 [17] the Ten Steps to Cyber Security [16] recommends the implementation of a number of Risk Management controls, in order to prevent a wide range of common attacks [18].

1. Information Risk Management Regime
2. Secure Configuration
3. Network Security
4. Managing User Privileges
5. User Education and Awareness
6. Incident Management
7. Malware Prevention
8. Monitoring
9. Removable Media Controls
10. Home and Mobile Working

Figure 2 - Ten Steps to Cyber Security

Two thirds of FTSE 350 companies, now use the Ten Steps [19]. Following the success of the Ten Steps scheme, the Government in conjunction with the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI) developed the Cyber Essentials framework [20].

Cyber Essentials

Cyber Essentials certification is said to be a simple, cost-effective, set of basic cyber security controls for organisations of all sizes [4].

> *"Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme"*
>
> UK Government [21]

The scheme exists in order to provide a mechanism to implement the 'Ten Steps of Cyber Security' [16][18]. Specifically it focuses on five '*essential*' mitigations and intends to be compatible with other established standards (e.g. ISO27001) [20].

1. Boundary Firewalls & Gateways
2. Secure Configuration
3. Access Control
4. Malware Protection
5. Patch Management

Figure 3 - Five Key Mitigations of Cyber Essentials

Each control is subdivided into a number of technical controls, with controls varying in terms of depth and required expertise [20].

A recent study [18], found that the Cyber Essentials controls were effective, and mitigated (or aided the mitigation) of 200 vulnerabilities, found by the US Department of Homeland security. Cyber Essentials is tested by a reviewed self-assessment questionnaire, and a remote vulnerability scan of all external facing services [22].

Cyber Essentials Plus

Cyber Essentials Plus certification, requires the exact same controls as Cyber Essentials, however it extends the validation to include on site assessments, internal vulnerability scans, and a review of physical security [22].

ISO27000 Series

Dating back to 1998 as BS7799, the ISO27000 series of International Standards has existed since 2005 [23]. The best known of these is ISO27001. ISO27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization [13]. The standard is made up of 114 controls in 14 groups and 35 control objectives [24].

Often referred to as costly and time consuming [23], studies suggest that integration of ISO27001 processes with ITIL service management approaches can lower the total cost of maintaining appropriate security levels, and aid in managing and mitigating risk [25][26].

Approximately 20% of education institutions have implemented ISO 27001 [3].

A major element of any Information Security Management system, is a comprehensive Risk Assessment and Risk Management process, for that to take place we must gain a deeper understanding of Risk itself, and the risks posed to our organisations.

Risk

A risk is defined by the ISO as the effect of uncertainty on objectives [13]. The ISO also define Information Security Risk as the potential that a given threat, may exploit vulnerabilities of an asset and thereby cause harm to an organisation [13].

Risk is measured in terms of the likelihood of an event and its consequences or impact [13]. A Risk exists where there is a likelihood of a threat; that someone or something could exploit a vulnerability within our organisation, or in a system we may utilise.

Risk= Likelihood * Impact

Figure 4 - Risk Measurement Calculation.

Threats

A threat is the potential cause of an unwanted event, which may result in harm to a system or organisation [13]

A variety of papers and standards propose methods for categorisation of these Information Security Threats [27], [28]. One such method is Microsoft's STRIDE [29] which attempts to categorise the various threats into a number of types.

Category	Description
Spoofing	Posing as somebody or something else.
Tampering	Modification of data or code.
Repudiation	These threats relate to the inability to track the (malicious) actions of a user.
Information Disclosure	Information is exposed to individuals who are not supposed to have access to it.
Denial of Service	Attacks which deny or degrade service for valid users.
Elevation of Privilege	Where a user (or non user) gains increased levels of access to a system.

Table 1 – Microsoft's STRIDE Model.

What can be seen from this model is there is a lack of attention to Environmental, Organisational and Physical Threats. This model could be applied to a software solution, but not necessarily to an Information System nor organization as a whole.

Vulnerabilities

A vulnerability is a weakness or gap in a system or process that may be exploited [13]. In essence a risk exists when there is a threat of the vulnerability being exploited.

When that vulnerability exists in a software system, or some form of network hardware that may give rise to maybe the most *revered* of threats, that of Hacking.

Hacking

Carried out by those referred to as Black Hat [30] or Grey Hat [31] hackers, Hacking is the illegal or unauthorised access of a computer system [32]. Hackers, alone or in groups pose a variety of threats to an organisation. At one end of the scale they may cause minor breaches of confidentiality, however there is also the chance that their intentions or beliefs may result in more widespread damage, destruction of information and even extended outages.

One such example in the Education sector targeted the parents of students attending a private school . In the first step of that attack, hackers were able to acquire a database of parents information, and this then was used to transmit the well-crafted Phishing email.

In certain sectors, the threat posed by hacking goes beyond simple lone wolf attacks, and can be perpetrated by so-called Hacktivist groups [33] or state sponsored groups. In this flavour, attacks can be instigated on the basis of political belief, or to gain advantage for the nation state sponsoring their activities.

Ethical Hacking & Penetration Testing

If we take the concept of Hacking, and flip it by 180 degrees we come to the idea of Ethical Hacking [34], or White Hat Hacking [35] and our opportunity to potentially see into the minds of, and think like our Miscreant Stakeholders.

A recent Information Security seminar I attended was delivered by none other than Ryan Ackroyd aka "Kayla" [36], formerly of the Hacktivist [37] group LulzSec [33]. Ryan's move from Black Hat to White Hat is uncommon in the industry [38], [39] and is set against a move of approximately 10% from White to Black [39].

Ethical Hacking may take place as part of officially sanctioned Penetration Testing, whereby an organisations network is scanned and attack attempts are mounted by a third party under the terms of a contract or official engagement.

Miscreants

Miscreants [29] we can consider, as the collective term for those who may wish to cause damage, or rather effect one or more elements of the Information Security Triad, e.g. compromising the Confidentiality, Integrity or Availability of a system. We can consider that Black Hat and Grey Hat hackers are both Miscreant actors in a given system. Additionally other types of actor may fall into this category.

Methods for Approaching Information Security.

With a focus on efficiency, and relative speed a number of organisations have turned to Agile methodologies for identifying and analysing Information Security Risk and in turn prioritising mitigations.

2.2 Agility

The turn of the century saw a movement emerge, culminating in the publication of the Agile Manifesto [40]; a set of four values and twelve principles that underpin a new suite of methods and tools intended to improve the software development community. They encourage practitioners to embrace change, hold both the needs of the customer and interactions with them as the highest priorities and to value working software over process and documentation.

Prior to this surge in preference towards Agile methods, formal methods that we can consider to be waterfall [41] approaches were the de-facto standard. These methods became less popular given they were based upon rigid, sequential processes [42]. We may also see them referred to as Plan-Driven methods, due to the use of tools such as Gantt charts to model the flow of work at the outset.

Some state that Agile is now the mainstream method for software development worldwide [43], with 97% of respondents to a recent Agile survey reporting use across their organisation [43], [44].

Following the manifesto, a number of new and existing methods were enveloped by the Agile umbrella, far from an exhaustive list we see methodologies such as Scrum [45], XP [46], and the recently retitled Agile Project Framework [47] (was DSDM). Key throughout the application of these practices, is the concept that these methods are here to be adapted. Borrowing ITIL's mantra of "Adopt and Adapt" [48], then there is also room for amalgamated methods, the AgilePF Framework for Scrum is one such example [49].

Furthermore, of the most interest in the way of Adopting and Adapting, is the idea that organisations can take elements of these methods, to solve problems in a piecemeal fashion, however this is an approach that has faced some criticism [50].

In recent times, we have also seen Agile escape the arena of software/IT and begin to change the way we think about leadership; business change, culture and processes as whole [51], [52].

Given that we place customers at the heart of everything we do, there is a need to engage with our customers, stakeholders and even the team in an engaging focussed way. Facilitated Workshops [53] are one such way of approaching these interactions.

Facilitated Workshops

One particular example of an Agile tool that pre-dated the Manifesto is the Facilitated Workshop, a key component of the DSDM/AgilePF approach. A component however that was co-opted based on previous methodologies (JAD/Participatory Design) [47].

In the Facilitated Workshop model, an often neutral party guides the participants through a process with an end goal in sight. The use of this model aims to bring about greater levels of buy-in, boosted team spirit and a faster road to a consensus [47], [53].

In addition to the facilitator, the model defines a number of roles, such as the Workshop Owner who sets the high level objectives, the participants who are selected in order to add value and the optional role of observers who may be auditing or monitoring the process and its outcomes.

If we consider that a Facilitated Workshop's key intention is to encourage engagement and collaboration, then there should be an Agile way in which we can document what is discussed. One such method is that of the Rich Picture [54].

Rich Picture

Soft Systems Methodology [54] is now respected as a collection of tools which can be deployed in an Agile environment [55]. Within that set of tools, is the Rich Picture, a visual representation valuable in that it provides a richness of understanding relating to the problem at hand [54].

Figure 5 - Example of a Rich Picture from [55] .

A Rich Picture has no rules [55] however it may feature drawn representations of People, Problems, Conflicts [56] and the such like in order to provide a holistic overview. In the above example, we see a Rich Picture that depicts the current situation for a small hotel, along with their desires for improvement and elements of their culture. The views of relevant Stakeholders are often represented in the Rich Picture, and their needs should be paramount in any Agile project.

Stakeholders

"Stakeholders encompass everybody inside or outside the project who are involved in or affected by it."

(AGILE BUSINESS CONSORTIUM, 2015) [47]

Stakeholders we can consider are at the very core of any Agile project, and we can reference the Agile Manifesto, valuing Individuals and Interactions, along with Customer Collaboration [40]. We can categorise Stakeholders in a number of ways. In one such method, we see: Primary Stakeholders, the end users of a system; Secondary Stakeholders, who provide input and who interrogate the output; Tertiary Stakeholders, who are affected by the success or

failure of a system; and lastly Facilitating Stakeholders, those who are involved in the project [57].

In ITSM practice, stakeholders are often identified and mapped using tools such as a Sponsor Map [48]. A sponsor map identifies a number of Individuals or Groups: The Authorising Sponsor, the person who has final and overall control of the project; Reinforcing Sponsors who's input is vital to the success of the project, and the success of any related Business Change [48]; and finally those Impacted by the project.

We may need to take the idea of our Stakeholders further, and begin to look deeper at their needs, motivations and skillsets. Personas [58] are one tool that may fit the bill.

Personas

A Persona [58] taken from the world of User Experience (UX) or Participatory Design [59], is a way in which we can document a typical user. Rather than a mere name or job title, the Persona brings life to this user giving it a biography, a background and identifying key information. By utilising the Persona we are able to become absorbed and identify the particular users' needs [60], often empathising as if we were that user [59].

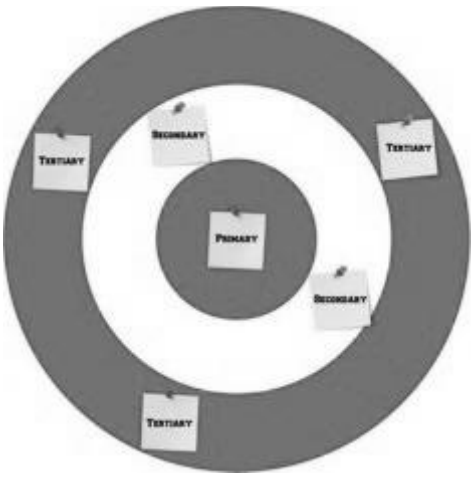


Figure 6 - Example of a Persona Map from [61]

As with other modelling techniques, Categorisation [58] and Mapping [61] may take place. Personas can be categorised in a number of ways for example Primary, Secondary and Tertiary

[60]. Tools such as Persona Maps [61] can be utilised in order to fit personas into these categories.

Attacker Personas

Attacker Personas [62], [63] represent a development extending traditional user Personas to cover typical forms of negative user. In line with the templated format of a Persona, templates for Attacker Personas have been defined [64].

Name			
Age			
Location			
Quote			
Motives			
Activities			
Ratings		Skills	/5
		Equipment	/5
		Funds	/5
		Criminal Intent	/5
		Damage Caused	/5
Profile			

Figure 7 - Example Attacker Persona Adapted from [64].

Use Cases & Use Case Diagrams

Use Cases are short descriptions of tasks or functions which a user can carry out in a given system [65]. A pictorial representation of the Use Cases takes the form of a Use Case Diagram, Ambler describes this as a diagram which provides an overview of the usage requirements of a system [65].

Abuse Cases

Converse to the function of a Use Case, Abuse Cases [66] (aka Misuse Cases [67]) document negative interactions that may target a system [68], and are cited as being easily understood by users, customers and developers [66]. They have been criticised in some instances and

advice is provided that the Abuse Case model should not replace more formal security engineering processes [66].

User Stories & Epics

Popularised by the work of Cohn [69], User Stories have taken hold as the de-facto method of requirements capture in the sphere of Agile [70]–[72]. The vast majority of story authors reporting that they use a standard template [70]. Of the slight variations in template, the most commonly used [70] is the format defined by Cohn/Connextra [69].

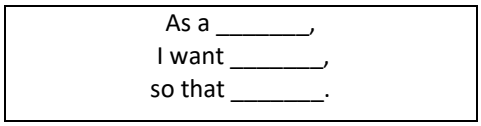


Figure 8 – Cohn/Connextra User Story Format.

In some instances, early on in the lifecycle of a project, the requirements may be defined at a higher level utilising Epics [69], which again follow the above format but potentially represent a wider scope.

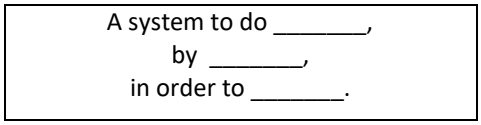


Figure 9 – Root Definition Format.

.

These Epics may show a resemblance to the format of a Root Definition, an element of Soft Systems Methodology [54].

[73] sets out the case that in addition to collaboration with a customer, that in the realms of security, User Stories may also be defined from Standards and Policies. Other proponents also cover options for new User Story variants, Abuser Stories [74] and Security Stories[75]

Abuser Stories / Security Stories

> *"Abuser stories identify how attackers may abuse the system and jeopardize stakeholders' assets."*
>
> (PEETERS, 2005) **[74]**

The term "Abuser Stories" coined by Peeters [74] in 2005, and recognised by the Open Web Application Security Project (OWASP) [76] as "Evil User Stories" cemented the need for a way to express the negative interactions that may occur to a given system [77], [78].

Security Stories [75] widen this concept and cover what the system should do to prevent the outcome of the Abuser Story.

3 Literature Review

3.1 Objectives

As of late 2018, papers referring to Abuser Stories or alternate variants made up less than 1/50th (n=90, f=1.81%) of papers relating to User Stories and their application.

The objectives of this Literature Review were:

1. To seek out, and explore the literature surrounding Security practices within Agile projects, specifically those papers documenting the use of Abuser Stories.
2. To research key Themes, and Ideas which may assist in the experimental phase of this study.

These objectives align with the research questions posed in section 1.3.

3.2 Related Work

At the time of writing, no literature reviews dedicated to Abuser Stories or other varying forms of title identifying a User Story which purports to identify a negative scenario have been completed.

No reviews of the literature solely concerning the practice of User Stories could be located.

Reviews concerning the broader topic of Agile Requirements Engineering have been completed.

Early studies by Paetsch et al (2003) [79] and Bjanrsaon et al. (2011) [80] are referred to by Lyanat et al. [81] in their 2014 published review of Agile Requirements Engineering. This was followed by a similar study by Schön et al. [82] in 2016 where User Stories featured in over half of the literature they identified.

In a second 2016 review, Heck & Zaidman [83] identify a number of papers referring to User Stories and their refinement, often focussing on quality aspects.

A systematic review of Security in Agile Requirements Engineering has taken place. Villamizar [84], finds a number of Authors discussing utilsiing Abuser Stories as a tool to document security requirements amongst many other techniques.

3.3 Search Strategy

During the initial scoping of this project, it was identified that Abuser Stories are often referred to by a number of names, and as such the literature identified was scoured to source as many of these alternate terms as possible. These can be seen in Table 2. During the initial search, the term Security Story was also apparent in a number of papers [85], [86]. Unlike the other title variations, the Security Story describes what an attacker should be unable to achieve. This is further explored below.

Search Term	**Number of Results (Google Scholar)**					
	2000-2005	**2006-2010**	**2011-2015**	**2016-2019**	**Total**	**%**
User Stories / User Story	270	788	2,140	1,680	**4,878**	
Negative User Stories / Negative User Story	0	2	5	5	**12**	**10.43%**
Abuser Stories / Abuser Story	1	10	8	4	**23**	**20.00%**
Attacker Stories / Attacker Story	0	0	2	0	**2**	**1.74%**
Evil User Stories / Evil User Story	0	0	6	5	**11**	**9.57%**
*Security Stories / Security Story **	*0*	*6*	*21*	*15*	***42***	**36.52%**
Misuse Stories / Misuse Story	0	4	9	11	**24**	**20.87%**
Misuser Stories / Misuser Story	0	0	0	1	**1**	**0.87%**
					115	**100.00%**

Table 2 – Volume of Search Results returned by Google Scholar for varying terms.

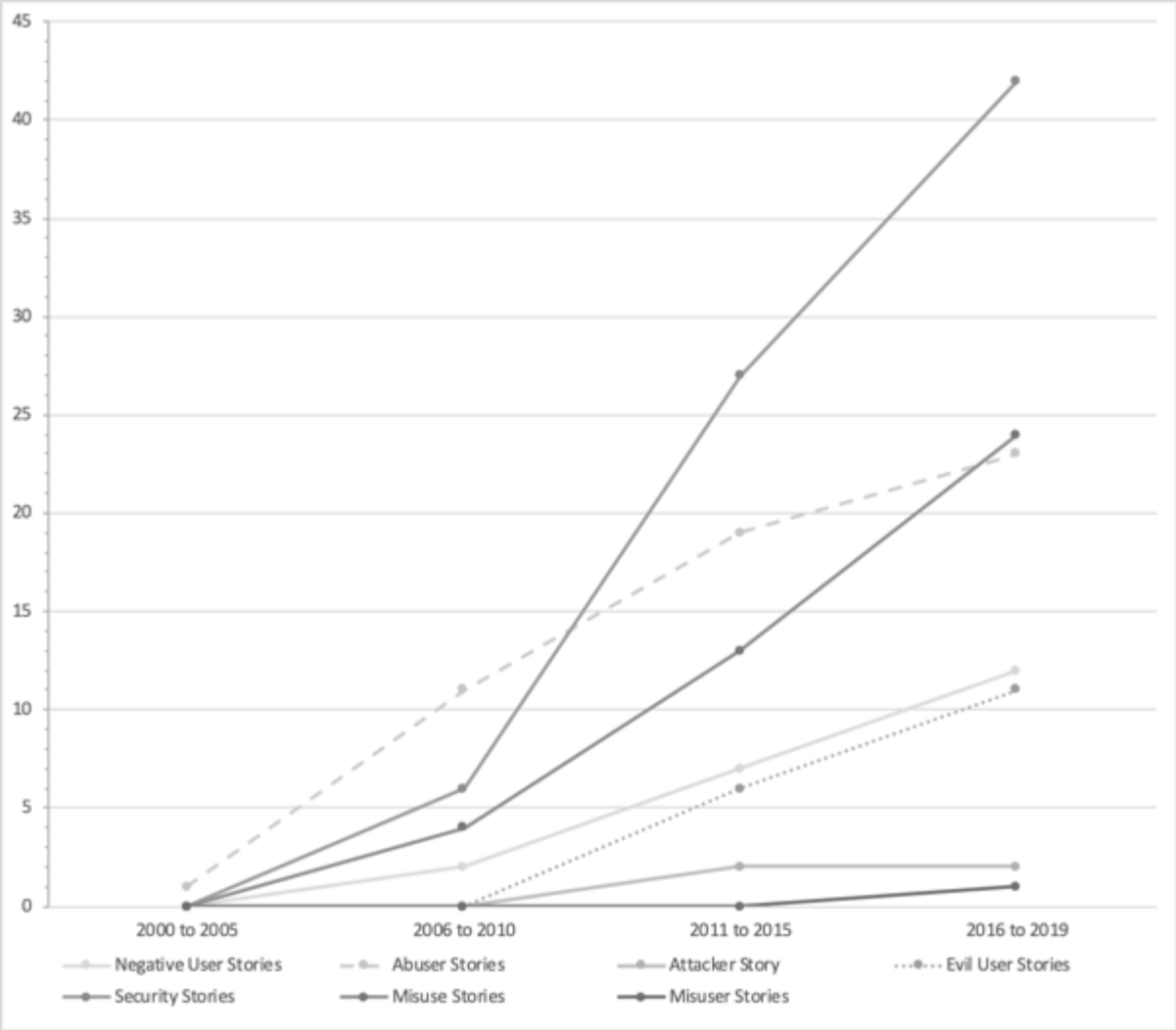


Figure 10 - Graph Depicting Growth of Published Papers Over Time.

3.4 Search Criteria

The following inclusion and exclusion criteria were utilised in order to define the scope of literature relevant to this review.

- Papers written in English.
- Dated January 2000 to December 2018.
- No full books.
- Title or body contains one of the search terms above.

The final number of papers returned not including those solely discussing User Stories was Ninety.

3.5 Key Themes

Are Agile Methods Insufficient for Capturing Non Functional Requirements?

A number of sources criticise existing Agile Methods for lacking in means to analyse Non Functional Requirements (NFR), and within that specifically Information Security Risk [85], [87]. NORMAP [87] introduces a new way to model NFR, firstly via a new mechanism for recording a User Story and utilising new types of Use Case.

A second group propose extending the planning phase of XP [67] in order to identify Assets, and formulate Abuser Stories. Those stories are then Risk Assessed and counter stories referred to as Security-related User Stories are defined. Where a User Story cannot counter the Abuser Story then the recommendation is to implement a mitigation by mandating a relevant coding standard.

An extension of the Scrum framework is similarly highlighted by [86], their proposal includes the addition of a Security Owner to guide the team to produce more secure increments. This type of role is seen in the area of Risk Management [88]. The Security Owner's role revolves around the maintenance of a Security Backlog. Misuse Stories are created to represent the threat being posed and again as with [85], Security Stories are proposed to mitigate these risks.

Use cases feature across these proposals, often in the form of Misuse cases [86], [89] or Loose Cases [85]. In a similar vein, User Stories feature either as Abuse [85], [86] or Misuse Stories [86]. Security Stories [85], [86] are utilised to counter these NFR type stories and provide a unit of work which can be worked towards a Definition of Done [45].

Pairing or Nesting User Stories and Abuser Stories

The root of an Abuser Story is none other than that of a User Story. Mapping out the Assets involved in functional stories allows the Agile Team to consider any attack vectors and

formulate Abuser Stories. This can be seen in the lightweight, multi-layered model defined by [90]. This model sees User Stories analysed and Assets collated in a similar fashion to [85].

Thinking like an attacker is discussed by [91] but they counter the idea of pairing in preference to tracking the Abuser Stories based upon their Cost (value).

Threats

Discussion surrounding the analysis and modelling of Threats is common across the literature [92], [93], [94].

A new formula for calculating risk, that deviates from the standard [Risk=Impact*Probability] mechanism [13] features in [92]. Entitled DREAD and originally created at Microsoft [95], this calculation takes into account the Damage Potential, Reproducibility, Exploitability, Affected Users and the Discoverability of a vulnerability. The original calculation sees the five areas rated from 1 to 10, they are summed and then divided by five to give a mean result.

Model	**Detail**
Traditional	Risk = Impact * Probability
DREAD	Risk = $\frac{(\text{Damage} + \text{Reproducibility} + \text{Exploitability} + \text{Affected Users} + \text{Discoverability})}{5}$

Table 3 - Comparison of Risk Calculations

In [93], a four stage process for threat analysis is defined, following this process leads to a list of identified Threats, Assets, Controls and Scenarios. Once defined, these artefacts are realised as Abuser Stories and added to the backlog. This model extends the Abuser Story to include various security controls within the acceptance criteria. Thus mitigating the impact of the Abuser Story can be assured if the acceptance criteria are met.

User Story Constraints

Contradicting the work of those preferring Abuser Stories, [96] considers adding Constraints on every Story. These constraints are declared in order to describe what cannot occur in a given Story.

Security Backlog

One author takes the story concept a stage further, and proposes a potential, separate Backlog of stories, a so called Security Backlog [42]. Security items are linked to traditional stories as we saw with [85], [90]. The reasoning here is that they should reflect threats against features implemented by those stories. Items on the backlog are to be prioritised by Risk, and the proposal goes further to suggest that the customers should be consulted to elicit the consequences of particular security stories.

When a prioritised Backlog item is selected for development, the security implications and thus linked security items from the Security Backlog should be selected in parallel. The model proposed sees the Security Stories used again to extend the User Story, and formulate acceptance criteria.

Penetration Testing

Across a number of the papers [42], [93], [96]–[99], there is a repeated concept, that of Penetration Testing. One paper defines these tests as a simulated attack against a system that can be used to identify weaknesses and strengths [93]. Often, Penetration Testing is carried out as a form of External Assurance [97].

Early and regular testing is one preference expressed [96], justified in line with the Agile desire to fail fast in that issues will be identified early. Others propose that these tests are carried out when a system is nearing completion [98], though this is reminiscent of waterfall type approaches. Alternate solutions involve carrying out the Penetration Testing as a parallel exercise to testing against the individual Security Stories [99].

3.6 Discussion

In an Agile environment, where ‘just good enough is good enough’ [100], is it therefore acceptable that approaches to ensure security in our projects again need only be good enough? A recent retrospective on Agile compounds our question, asking ‘how do agile methods ensure that security requirements are continually met?’ [43].

Some argue that with Agile, security is not absolute, and that even systematic traditional approaches do not ensure completeness [96]. Across the literature, the apparent view is that as of yet no one approach to Security within an Agile project outshines the others.

Previous reviews of the literature suggest that what is required is further empirical evaluation of the various approaches [84]. Research appears to be focussed presently on modifying existing Agile methods to introduce new artefacts [84].

The argument also that as Agile methods encourage rapid development, without a heavy documentation burden that this can lead to the production of less secure software is seen [86]. Contradicting these, previous work and experimentation directs us toward a number of solid avenues to explore in the areas of Threat Analysis, Abuse Cases and Abuser Stories.

Given the respective low volume of literature, in comparison to papers on wider topics such as Information Security and Agility, the decision was taken to supplement this review with an initial posture survey. This approach is covered in more detail throughout the following sections.

4 Research Objectives

The review of relevant literature was completed in order to direct the enquiry and strengthen the findings from the study. Following this, two key research questions were identified:

RQ1. Are Abuse Cases and Abuser Stories effective means of documenting Information Security Risk in a Software Project.

RQ2. Can Specific Agile Approaches succeed in aiding the prioritisation and treatment of Information Security Risk.

These research questions have been explored utilising a combination of a survey, and a number of Action Research [101]–[103] cycles, exploring the use of a number of Agile tools and techniques in order to analyse and document Information Security Risk as well as to prioritise Risk Treatment. Action Research follows an iterative Plan, Act, Observe, Reflect cycle [103].

5 Context

5.1 Personal Context

Action Research leads reflective practitioners to propose, and experiment with solutions to problems in their current practice [103]. An exploration of Agile tools and techniques in order to lighten the burden of Information Security, and specifically Threat Identification and Risk Assessments is a prime area of interest.

5.2 Organisational Context

Key on the agenda for organisations across all sectors, and specifically within Further Education is the topic of Information Security [11]. A recent external Penetration Test carried out by JISC[104] highlighted a number of areas of improvement that the College could make.

The College has also set out its commitment to prioritise Information Security [105], including the maintenance of a minimum standard of Certification (Cyber Essentials).

Within the IT Services function, preference toward the use of lightweight processes and tools such as ITIL and Agile lead this Action Research study to be a worthwhile investigation.

5.3 Theoretical Context

The literature presented a number of opportunities to explore Agile methods for documenting Information Security threats and risk in software projects. However as the literature was sparse in comparison to more broader discussion of Agility and Information Security, a background survey also took place.

6 Method

6.1 Research Design

Timescale

The study took place Between November 2018 and March 2019, this included a background survey to identify key trends in Information Security, and the sector's willingness to explore Agile methods to reduce the analysis and documentation burden. The action research phase included three linked Plan, Act, Observe, Reflect cycles to experiment with and explore a practical application of some of the techniques identified during the literature review.

Participants

Action Research Participants were selected from the IT Services function of the College, involving colleagues from all three IT Teams:

- **IT Systems.**
  Responsible for the development and maintenance of a large volume of in-house Information Systems, core databases and third party solutions.
- **IT Infrastructure.**
  Manage and maintain the College's IT infrastructure, including virtualized server platform, storage area network, end-user PCs, classroom AV and campus networking.
- **Service Desk.**
  The first point of contact for Staff, Students, Parents and Third Parties in relation to any IT, Facilities or MI queries along with the initial triage of Data Protection queries and campus Security requests (CCTV).

Each of the teams has a core responsibility to ensure the Confidentiality, Integrity and Availability of all IT solutions and equipment.

Resources

Throughout the three cycles a number of techniques created artefacts that were stored and developed utilising two electronic tools Atlassian Jira [106] (Project/Story Management) and

Atlassian Confluence [106] (Document Management). Though these artefacts could be represented and worked on paper, these electronic methods aligned with the team's current workflow and preferences.

The main exception to this rule was the use of a whiteboard and markers to create the Rich Picture, this is cited [107] as the preferred method due to the ease of modification and lack of formal structure versus a computerised drawing.

Permissions

The study required the participation of a number of colleagues, their permission was sought at the outset, and reconfirmed during each cycle. A number of items within the College's overarching Information Security Risk Assessment (created in conjunction with this study) are of a commercially sensitive nature, those items featured in this study do so after agreement with the College's Senior Leadership Team.

6.2 Research Methodology

Why Action Research?

Action Research is cited as a suitably rigorous method for carrying out studies within Information Systems [102] and for research into Agile methods and techniques [108], [109]. With its roots in Educational Research [103], Action Research is carried out by practitioners measuring the outcome of changes to their practice rather than observation as with a Case Study [102].

This study involves the deployment of a number of new techniques, and requires that the team are observed and that actions and outcomes are documented. Potentially these changes will occur incrementally and Plan, Act, Observe, Reflect cycle [103], supports this akin to an iterative Agile approach. It is also reminiscent of the ISO27000 series Plan, Do, Check, Act cycle.

Validity

Though sometimes criticised [101] as lacking in rigour, Action Research when combined with sufficient control is to be considered an Empirical Research method [101]. Adherence to the Plan, Do, Check, Act cycle allows for repeatability and Scientific Rigour [103].

Monitoring of Actions and Learning

A variety of approaches to monitor the actions of the various participants, and my own learning are to be used. These range from simple observations, surveys and to the monitoring of Incident tickets as the project moves forward. Notes will be kept concerning progress, and possible future improvements.

6.3 Research Ethics

In line with the findings of a recent report [110] considering ethics in Information Security projects, the outline of the proceeding Ethics Statement follows that of the Menlo Report [111]. In line with this report, relevant Research Stakeholders have also been identified.

Ethics Statement

Respect for Persons

A variety of types of data will be recorded throughout the study, this will vary from data of commercial value or sensitivity, through to personally identifiable information (PII). The principles of informed consent, will be adhered to.

The study requires the participation of a number of colleagues within the College, and they will be furnished with a short summary of the reasons for their participation (Appendix 4 – Participation Statement). Colleagues should be in a position to consent to participate, and will be free to withdraw from the study at any stage.

An initial survey to identify the overall posture of the Further Education Sector as far as Information Security and Agility will take place. This survey shall be anonymous in order that

respondents do not compromise their organisation should they disclose an exploitable vulnerability or a weakness in management and leadership.

Beneficence

This study aims to be of benefit to the Further Education community, along with practitioners and researchers of both Agility and Information Security. That withstanding, given the nature of Information Security there remains a minimal risk that harm may be inadvertently caused to participating colleagues and organisations. This could be in the form of commercial or financial harm should a vulnerability disclosed and documented in this study be exploited.

To that end, this report features only discussion of common vulnerabilities and in all cases only generalised descriptions.

Before the inclusion of corporate/commercial information, permission from the College's Senior Leadership team was be sought.

Fairness

All participants, whether those from the initial wider survey or direct participants during the project will have access to completed analysis and outputs.

Respect for Law & Public Interest

The principles of Data Protection, and compliance with current Data Protection legislation shall be adhered to at all times.

This research study aims to be of high quality and will be documented in order that its findings can be reproduced. Risks will be considered and mitigated at all stages.

At no stage will the study require the breaching of any third party network or system, however detailed threats and vulnerabilities documented may be exploited by those of a criminal nature.

Research Stakeholders

Primary Stakeholders

In terms of this research study, the Primary Stakeholders are the end-users of IT Systems within the College. This includes Staff, Students, Parents (& Guardians) and the Governing Body.

Secondary Stakeholders

Secondary Stakeholders take the form of a number of suppliers to and partners of the College:

- Internet Provider – JISC Ltd
- Student Records System Supplier – Unit 4
- HR System Supplier – Jane HR
- Finance System Supplier – Advanced
- Education and Skills Funding Agency
- Ofsted
- Department for Education
- Association of Colleges
- Other Further Education Providers

Key Stakeholders

Key to the project were a number of internal colleagues within the IT Services function, alongside members of the Senior Leadership Team.

A number of negative stakeholder groups such as external malicious actors, the authors of malware and current staff/students with maligned intent are also included within this category.

7 Sector Survey

In order to support the action research study, a preliminary survey was created and shared amongst IT professionals within the Further Education sector.

7.1 Objectives

The intention of the survey was to assess the level of preparedness and the attitudes towards Information Security, and Agility of Further Education organisations. The format and questions aligned with that of previous works [11]. In particular the survey focussed on the following areas:

- What level of staffing is provided to oversee or carry out the organisation's Information Security function.
- Which types of compliance or certification does the organisation believe is necessary and appropriate for the sector.
- How does the organisation rate the importance of a number of standard Cyber Security practices.
- To what extent does the organisation believe a number of common Cyber Security Risks may impact them.
- Does the organisation have experience with the use of Agile Techniques and Methods and would the organisation consider utilising these tools or methods when considering their Information Security Risk Assessments.

7.2 Survey Methodology

Participants

As with previous work [112] the potential respondents are members of the JISC College Management Information Systems group and additionally the JISC Security group. Both groups receive approximately 20 topics or topic responses each day and the members are IT/IS professionals within the Further Education sector (JISC CMIS) and Cyber Security Professionals across education (JISC Security).

Design

Response Capture

The survey was emailed to all members of both groups (Appendix 1 – Email to JISC CMIS and UK Security Groups), the email contained a link to a Google Form which facilitated the data capture into a spreadsheet format.

Questioning

Five major sections form the survey, the first of those is used as a sanity check that respondents are reporting to be from a Further Education organisation. The second section looks at Staffing and Policies within the organisation. This section aims to identify the structures and certifications present to support the organisations Information Security aims.

Understanding the importance of Cyber Security and the organisations approach is the focus of the third section. Likert [113] style questions (e.g. 1 Not Important to 5 Vitally Important) are utilised in this and two following sections The fourth section then assesses the level of a number of common Cyber Security Risks to the organisation.

The fifth and final section queries the organisations utilisation of Agile Methods & Techniques and their maturity level. The organisations willingness to employ Agile approaches is probed with a final, simple Yes/No question.

The questions utilised can be found in Appendix 2.

7.3 Results

Responses

Overall 27 responses were received, of this number four reported representing organisations outside of the Further Education sector: A single training provider, and three Higher Education Institutions. These four records were duly rejected, and removed from the analysed data.

The 23 remaining responses represent just over $1/8^{th}$ of the General Further Education Colleges in England (n=23, f=13.07%) [114]. This may mean that the sample and results are not representative of the full population [115].

Staffing and Certification

Over 80% of respondents report that their institution does not have a dedicated Cyber Security resource (n=19,f=82.61%). Worryingly over a third have no identified resource at all (n=8,f=34.78%). **Figure 6** further highlights the distribution of roles across respondents.

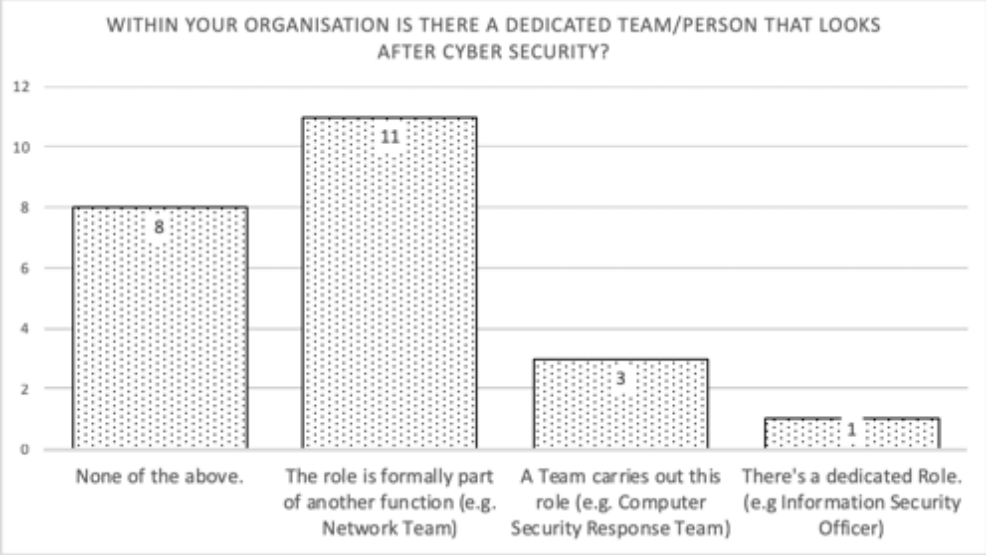


Figure 11 - Resourcing

Nearly 40% of respondents had no plans to complete any of the three major Cyber Security certifications (n=9,f=39.13%). The most popular of all of the schemes was Cyber Essentials with over 60% Considering or having Achieved certification against the standard (n=14,f=60.87%). Conversely full ISO27001 certification is out of scope for over three-quarters of organisations (n=18,f=78.26%). **Figure 7** provides further data regarding plans.

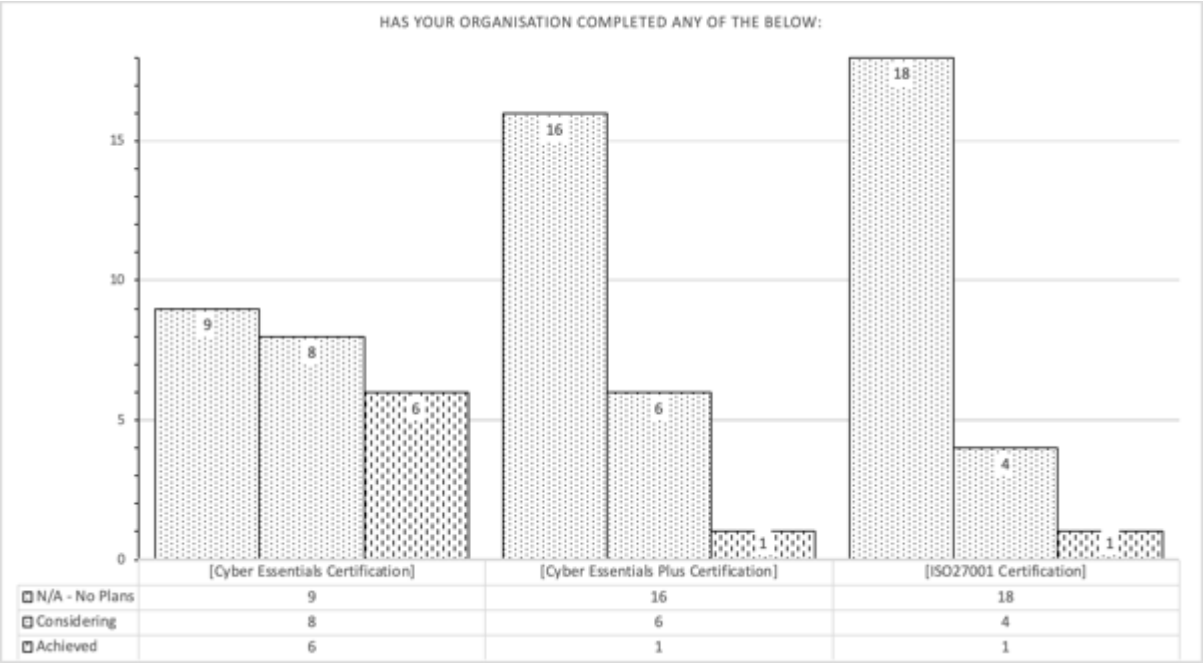


Figure 12 - Cyber Security Certifications

Policies & Risks Assessment

Nearly two thirds of respondents reported that their organisation has developed a specific Information Security policy (n=15,f=65.22%) **(Figure 8).**

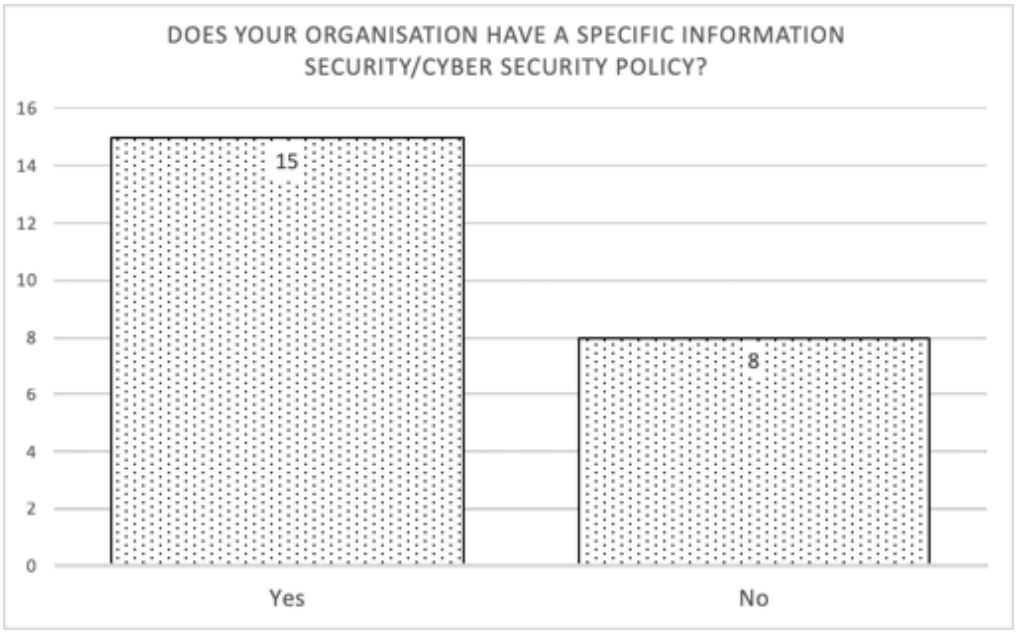


Figure 13 - Information Security Policies

However only slightly over one third (n=8,f=34.78%) (**Figure 9**) of organisations had carried out an Information Security Risk Assessment.

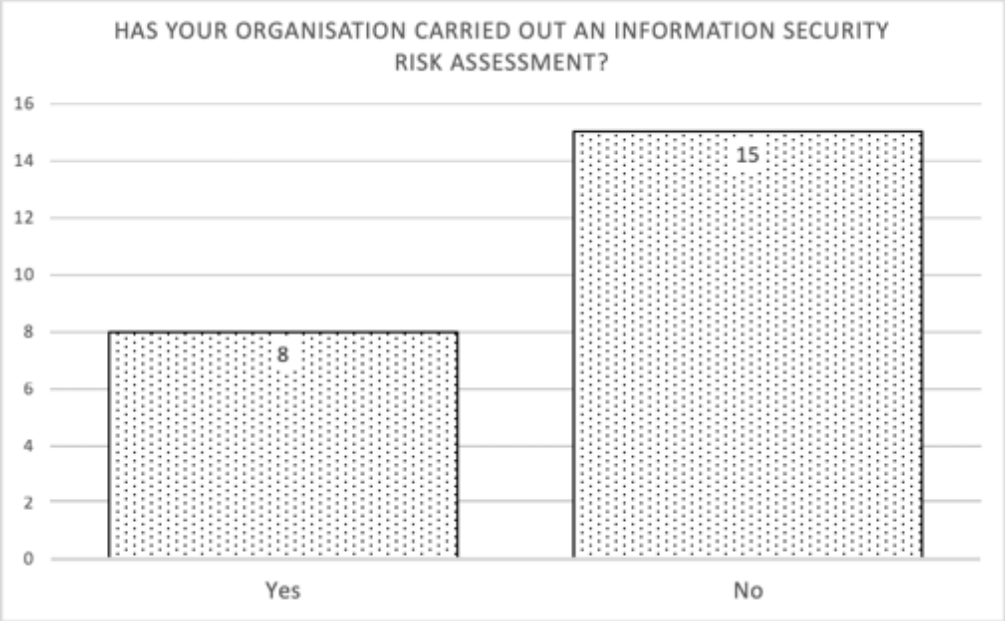
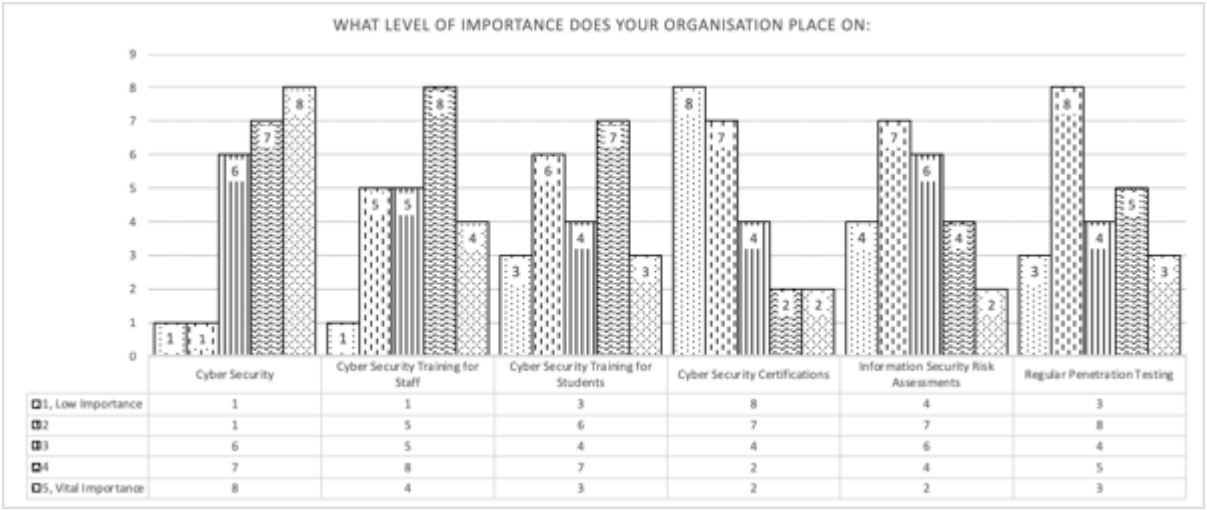


Figure 14 – Information Security Risk Assessments

Importance of Cyber Security

The majority of respondents (n=15,f=65.22%) reported placing a High (4) or Vital (5) level of importance on Cyber Security as a whole, the average being a High level of Importance (Mdn=4,n=7,f=30.43%).

Figure 10 highlights further the Importance of various Cyber Security Techniques and Mitigations.



	Cyber Security	Cyber Security Training for Staff	Cyber Security Training for Students	Cyber Security Certifications	Information Security Risk Assessments	Regular Penetration Testing
1, Low Importance	1	1	3	8	4	3
2	1	5	6	7	7	8
3	6	5	4	4	6	4
4	7	8	7	2	4	5
5, Vital Importance	8	4	3	2	2	3

Figure 15 – Importance of Cyber Security.

Over half of all respondents (n=12,f=52.17%) prioritised Cyber Security Training for staff (Mdn=4,n=8,f=34.78%). Slightly less than half (n=10,f=43.48%) place a High or Vital level of Importance on Cyber Security Training for Students (Mdn=3,n=4,f=17.39%).

Less than a fifth (n=4,f=17.39%) of respondents reported placing a High or Vital level of importance on Cyber Security Certifications (Mdn=2,n=7,f=30.43%). Similarly only a quarter (n=6,f=26.09%) place a High or Vital level of Importance upon completing Information Security Risk Assessments (Mdn=3,n=6,f=26.09%).

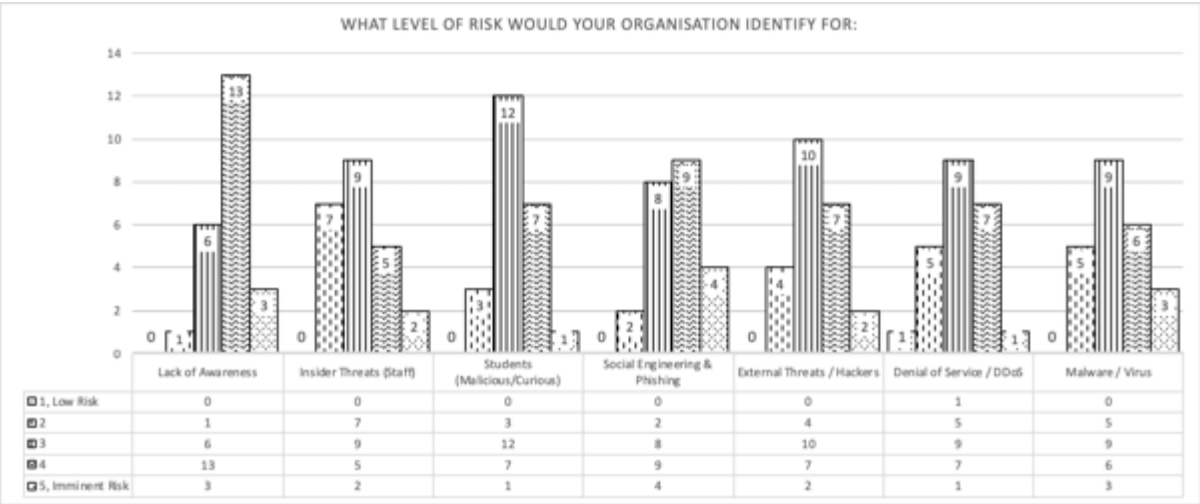
Regular Penetration Testing is given a High or Vital level of importance from just over one third of respondents (n=8,f=34.78%), (Mdn=3,n=4,f=17.39%).

Risks

Figure 11 displays the results of questioning regarding the Risk the organisation considers a number of common Cyber Security Threats.

A Lack of Awareness features as a High (4) or Imminent (5) Risk for the highest number, over two thirds of organisations (n=16,f=69.57%), (Mdn=4,n=13,f=56.52%).

The threat from Phishing and Social Engineering attempts ranked second with over half of all respondents (n=13,f=56.52%) considering this a High or Imminent Risk (Mdn=4,n=9,f=39.13%).



	Lack of Awareness	Insider Threats (Staff)	Students (Malicious/Curious)	Social Engineering & Phishing	External Threats / Hackers	Denial of Service / DDoS	Malware / Virus
1, Low Risk	0	0	0	0	0	1	0
2	1	7	3	2	4	5	5
3	6	9	12	8	10	9	9
4	13	5	7	9	7	7	6
5, Imminent Risk	3	2	1	4	2	1	3

Figure 16 – Cyber Security Risks.

The threat of an External Hacker is only considered a High or Imminent Risk for less than 40% of all organisations (n=9,f=39.13%) (Mdn=3,n=10,f=43.48%). Similar figures are reported for Denial of Service type threats (n=8,f=34.78%) (Mdn=3,n=9,f=39.13%) based upon them being High or Imminent Risks.

Malware or Viruses were only considered a High or Imminent risk by approximately 40% of respondents (n=9,f=39.13%) (Mdn=3,n=9,f=39.13%).

Insider threats in the guise of Staff (n=7,f=30.43%),(Mdn=3,n=9,f=39.13%) and Students (n=8,f=34.78%), (Mdn=3,n=12,f=52.17%) are considered as less likely to be High or Imminent Risks.

Agility

Less than 20% of organisations (n=4,f=17.39%). report utilising Agile Methods & Techniques with a High (4 or 5) rating (Mdn=2,n=4,f=17.39%). **Figure 12** shows the spread of values for this question.

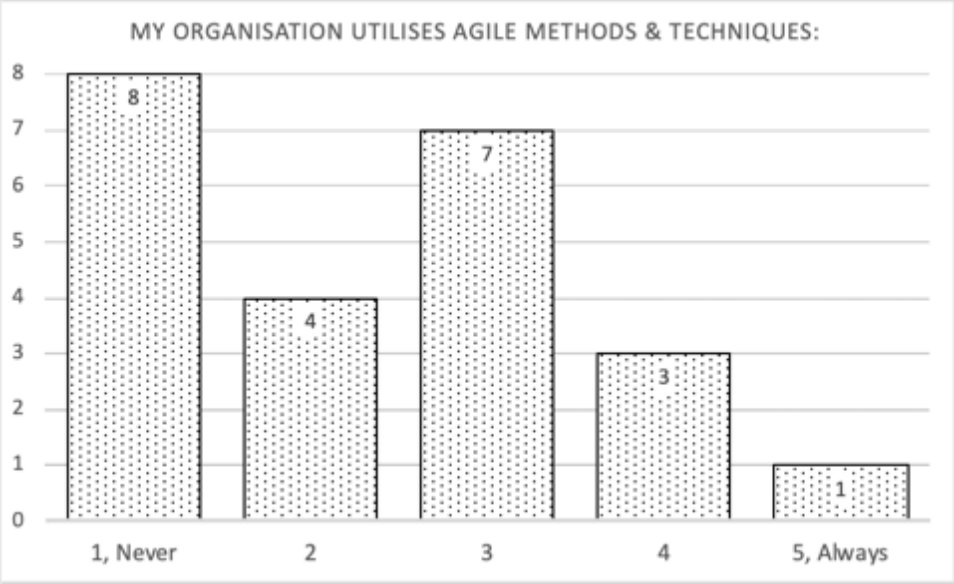


Figure 17 – Usage of Agile Methods & Techniques.

Again, the level of experience with Agile Methods and Techniques is only reported as high for less than 20% (n=4,f=17.39%) of organisations (Mdn=2,n=7,f=30.43%).

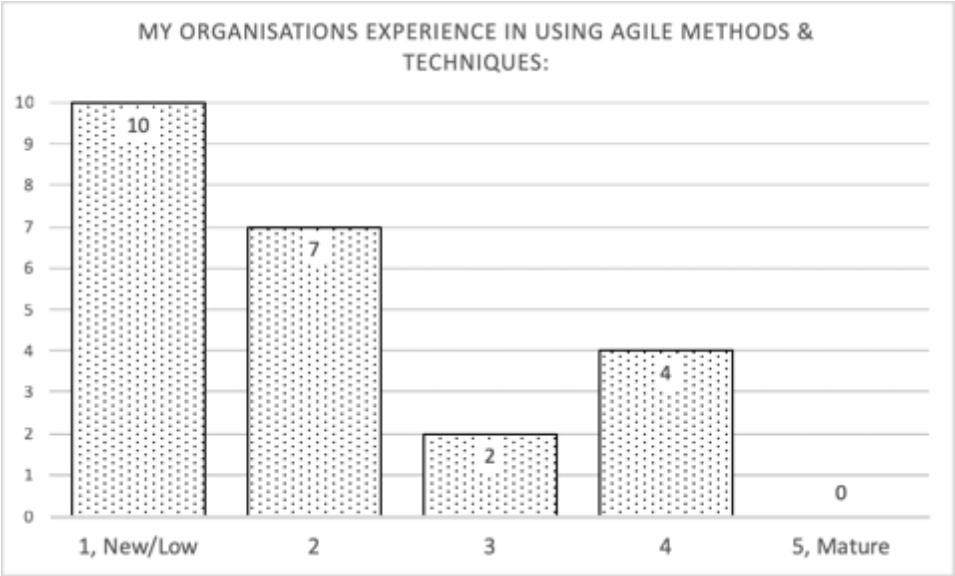


Figure 18 – Agile Maturity.

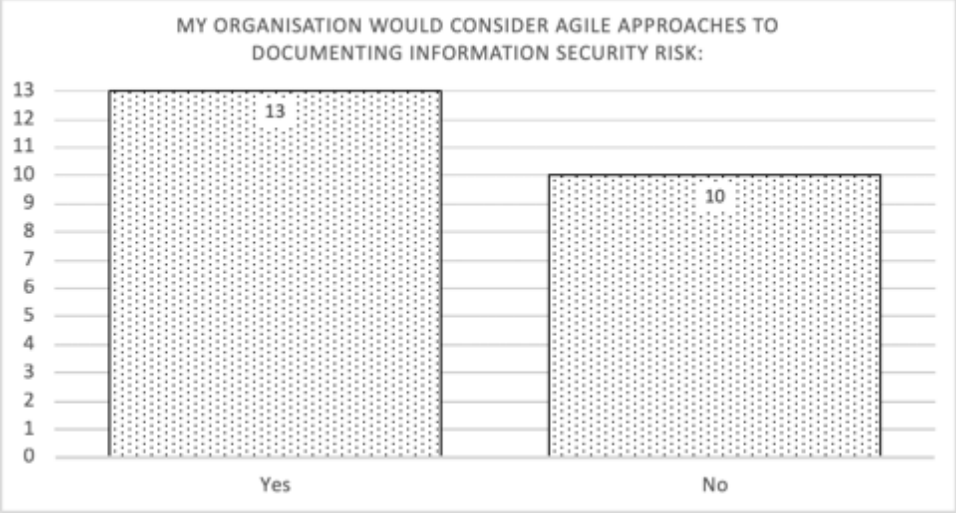


Figure 19 – Willingness to Utilise Agile Methods for Information Security Risk Documentation.

Figure 14 shows that more than half of organisations (n=13,f=56.52%) would consider utilsiing Agile Methods when documenting Information Security Risk.

A score based upon the organisations rating for their Experience of Agility and their Utilisation of Agile was computed by simple addition. A histogram (**Figure 15**) of these values mapped for both the group willing to use Agile Methods and for the group who would not wish to utilise Agile Methods.

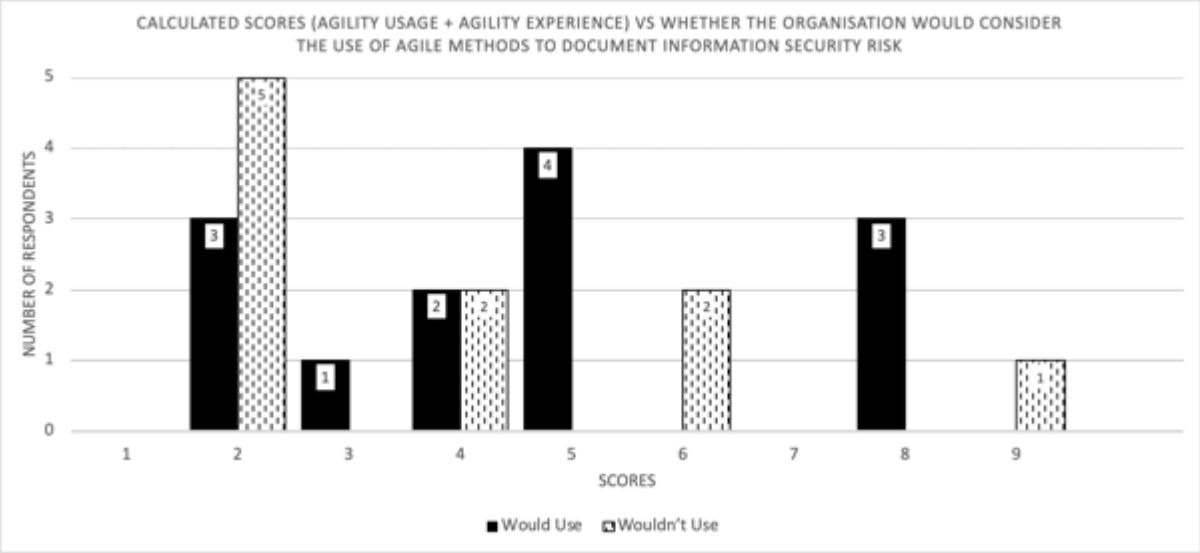


Figure 20 - Calculated Agility Scores vs Willingness to Use Agile Methods for Information Security Risk

A Mann-Whitney [116] test showed no statistical significance between the group who reportedly would consider using Agile Methods to Information Security vs those who would not (U=50.5,p=0.3843).

7.4 Survey Discussion

A recent study [11] revealed that only 2% of Further Education organisations have dedicated Cyber Security posts, somewhat less than results found in this study (n=4,f=17.39%). As a contrast the figure amongst Higher Education institutions is markedly higher at 65% [11]. Interestingly the same parallels can be seen when HE (circa £140,000+) vs FE (circa £18,000) [11] mean Cyber Security Budgets are considered. This raises the question as to whether funding levels for Cyber Security within the Further Education sector are adequate.

Three quarters of organisations [3] senior managers say that Cyber Security is a priority, our respondents reported a similar outlook (n=15,f=65.22%) rating overall Cyber Security priority as being of High or Vital Importance.

As we look to Cyber Security Certifications we see that an equivalent number (n=14,f=60.87%) of respondents reported having achieved or considering Cyber Essentials Certification than in other studies (60%) [11]. Lower figures (n=7,f=30.43%) are seen when looking at Cyber Essentials Plus Certification as in the recent JISC study (45%) [11]. The JISC study reported that

only 22% of FE organisations were considering full ISO27001 Certification and this aligns with these findings (n=5, f=21.74%).

A government funded study [3] showed that 32% of organisations have documented their Cyber Security Risks, alignment can be seen with respondents in this study (n=8,f=34.78%). The same study reported that 33% of organisations have a formal policy covering Cyber Security, approximately half the proportion of survey respondents (n=15,f=65.22%).

Previous reports showed 88% of Further Education organisations utilise Penetration Testing [11] though in these findings only slightly over a third of respondents rated it of High or Vital Importance (n=8,f=34.78%).

Respondents reported above half of all organisations consider Cyber Security Training for Staff (n=12, f=52.17%) of High or Vital Importance. We can see from the JISC Study that 55% [11]of FE Colleges confirmed that Staff Training was mandatory. A similar story is repeated for Student training 31% [11]. These figures exceed those shown across all businesses (30%) in a government funded study [3].

When considering the threats faced to organisations within the FE sector, the standout threat came from that of Lack of Awareness (n=13,f=69.57%), the JISC Study [11] also ranked this as the greatest Threat. A government funded study [3] highlighted Ransomware as the biggest Threat though 72% of breaches reported by their respondents concerned Phishing emails. Further analysis of these Top 5 threats [11] can be found in **Table 1.**

Threat	**Rank in JISC Study**	**Breaches Ranked in Government Study**	**Results**	**Rank**
Lack of Awareness	1	N/A	69.57%	1
Phishing/Social Engineering	3	1 & 3	56.52%	2
Ransomware/Malware	2	4 & 2	39.13%	3=
External Attack	4	5 & 6	39.13%	3=
Denial of Service	5	7	34.78%	4

Table 4 – Ranking of Threats (JISC vs Government vs Survey Respondents).

Previous research has shown that less than a quarter (n=7, f=23.33%) [112] of all organisations within Further Education have adopted Agile. This correlates with the results of this survey for High (4+) levels of Utilisation (n=4,f=17.39%) and Experience (n=4,f=17.39%).

The lack of any statistical significance between the group who would consider the use of Agile Methods and their counterparts could be interpreted as there being an openness to consider new techniques across all organisations in the sector.

7.5 Survey Conclusions

It appears from the survey results, that there is alignment across the sector regarding perceived Threats and prioritised Mitigations. A positive response (n=13,f=56.52%) is also seen from Colleges who would consider the use of Agile Methods to document Information Security Risk.

Though set against a background of unusually low levels of Agile Adoption (<25%) [112], given the low proportion who have carried out such a Risk Assessment (n=8,f=34.78%), there is a compelling argument that experimenting in this area could provide a positive impact.

8 Action Research - Data Gathering

Throughout the study, a number of techniques were used to gather and analyse data. At the outset of the study, a survey was utilised to gauge the team's attitudes towards the effectiveness of current Information Security Risk Analysis methods. Following each cycle, the same question set was again deployed in order to document perceived improvements.

Notes were taken during each phase following observation of the team, and of the various outputs.

8.1 Prior to Improvements

Presently nearly 1 in 200 incidents reported to the College's Service Desk relate to some form of Information Security Incident. Of those 40% relate to instances where data may have been exfiltrated or corrupted.

Confidentiality	Integrity	Availability	Total	Total Incidents
3	1	6	10	1997

Table 5 - Incident Statistics (Inc Info. Sec.)

8.2 Outset & Post Cycle Team Surveys

At the outset of the project, and following each Cycle of improvement, a simple survey was sent to participants. The aim of the questions are to gauge the impact of the changes proposed during each cycle in order to track improvement and understanding.

The questions posed remained the same across each Cycle to ensure that the results are comparable. An example of the survey, which was delivered via Google Forms can be found in Appendix 5 – Team Survey.

The short survey first identifies the Cycle and the Team the respondent reports to be from. Following which a set of Likert [113] type questions are featured:

1. It is easy to Identify Security Requirements
2. It is easy to Prioritise Security Requirements
3. Security Requirements can be Modelled easily
4. Agile tools are effective for Identifying, Prioritising and Modelling Security Requirements
5. My team are able to attend to Security Requirements.

Figure 21 - Likert Style Questions from the Team Survey

A short comment was also permitted to be recorded by each participant, however this remained optional.

Following each phase, the perceived improvement was analysed by reviewing the survey responses.

9 Action Research - Cycles

9.1 Prior to Cycles

Prior to commencement of the initial cycle, the team were sent the first link to the survey.

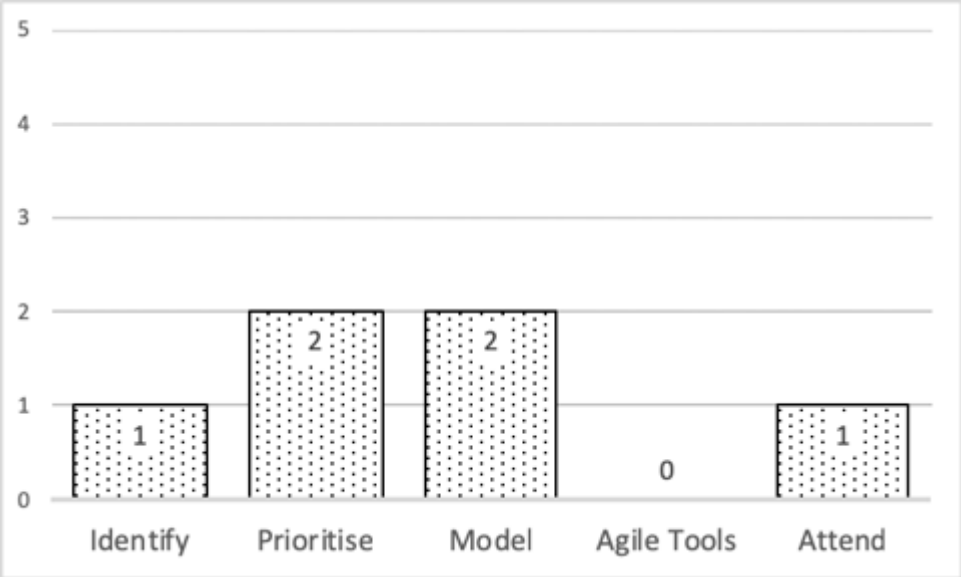


Figure 22 – Plot of Median Responses to Pre Project Questions

The results highlight that the team appear to have little confidence that they are able to carry out a number of processes in regards to Information Security. Specifically, it is clear to see also that the team have no experience in utilising Agile techniques and tools in order to Identify, Prioritise or Model Security Requirements.

The small number of text comments received, revealed that members of the team felt that at that moment, they were unprepared to incorporate Information Security concepts into their normal practices. One comment alluded to it adding additional burden, echoed with a comment related to the level of complexity as far as implementing ISO27001. A further message revealed was that due to the cost of external Penetration Testing, when it did take place the team felt caught out by the findings.

These results could be interpreted as a basis on which to build, and to build utilising Agile techniques to keep the 'burden' light.

9.2 Initial Cycle

Planning

In line with [103] and based upon the overarching research questions, the issues to be explored in the first cycle have been documented. Each area for investigation has been allocated as a sub-question.

Question	Research Issue	Research Question	Proposed Value	Options (*Chosen **)
RQ2.1	What threats does the college face.	How do we identify the high level threats facing the college.	Identification of High Level Information Security Threats.	*Rich Picture ** Threat Analysis ISO27005 Risk Assessment ISO27005
RQ2.2	Who or where do these threats come from?	How do we begin to explore the types of user we may face threats from and their motives.	Consideration for the types of Miscreant Actor who may threaten the College. Background understanding of the motivations and threat level of these persons.	*Attacker Personas ** Threat Analysis ISO27005

Table 6 - Issues, Questions and Value for the First Cycle

The chosen options for investigation in the first cycle are the use of a Rich Picture and Attacker Personas. These were selected over the more in-depth processes available in the ISO27000 suite of standards due to their lightweight Agile approach.

Rich Picture

At the outset of the project, the team participated in a Facilitated Workshop in order to identify the high level cyber threats facing the College's infrastructure. Prior to the workshop an outline agenda had been shared (Appendix 6.1 – First Cycle, Rich Picture of High Level Threats Workshop).The workshop began with an initial briefing on the theory behind the use of Rich Pictures.

The threats are represented as part of a Rich Picture which also features an overview of the College's network, datacentres and power protection.

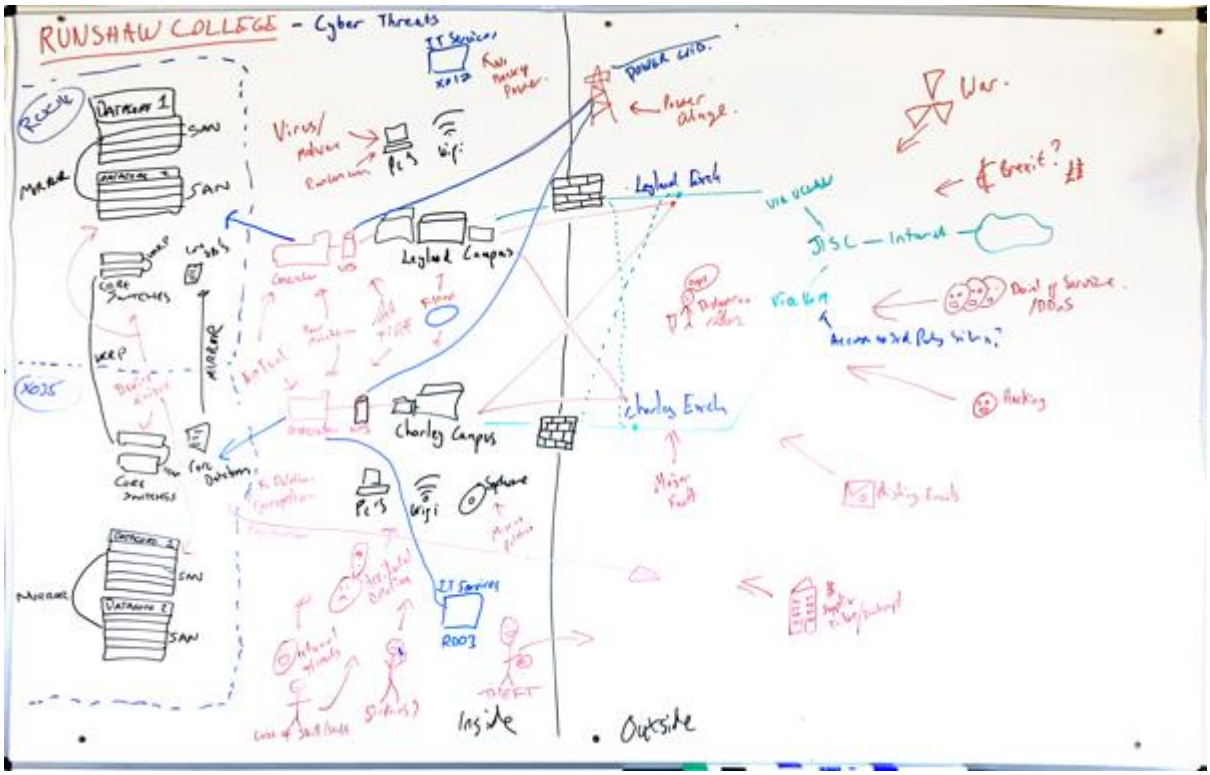


Figure 23 - Initial Threats Rich Picture

Attacker Personas

Prior to a second Facilitated Workshop (Appendix 6.2 – First Cycle, Attacker Persona Workshop), the team were all sent a link to an online training video which briefly covers the creation of traditional Personas in an Agile environment [117]. The aim was to ensure that during the workshop all attendees would have some form of background knowledge regarding Personas.

At the outset of the workshop, the team re-visited the Rich Picture which had been previously created to review some of the classes of threat which had been identified. The team were then divided into pairs and assigned an archetypal Miscreant actor as listed below.

1. Lazy Student
2. Botnet Farmer
3. Malicious Student
4. Insider Threat (Staff)
5. Social Engineer

Figure 24 - Miscreant Types

Following this the teams started to define their Attacker Personas using pencil & paper. (An example of an initial paper Attacker Persona can be found below). The small groups quickly started to share their ideas with others, and engaged in lively debate about the motivations and threats posed by these initial Miscreants.

Figure 25 - Attacker Persona (Paper)

Traditionally during the Persona creation, participation with end users is encouraged in order that the Personas may take on their characteristics and needs [59]. Given the nature of our Miscreant users however, this wasn't possible and thus it could be argued the Personas may be left lacking. Nonetheless, feedback received from the team leads us to believe that this was again an worthwhile task.

Late on in the session, a suggestion was made to create a new template in the Jira system to host the Personas. The justification being that then the Personas can be linked to other Jira issue types, such as User Stories.

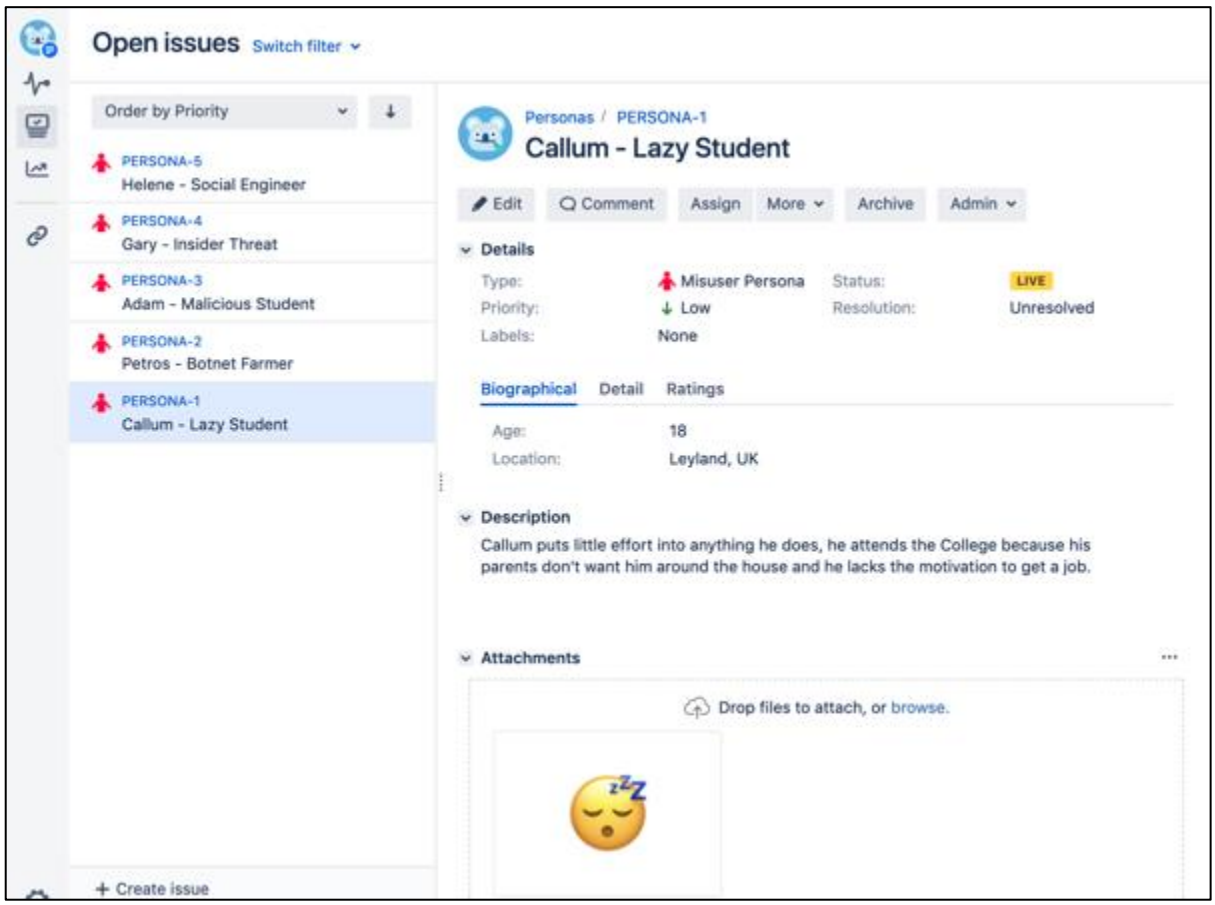


Figure 26 - Attacker Persona (Electronic)

One of the key observations made is that the teams attention often becomes focused on utilising the tool rather than on collaborating to create artefacts. However this was counteracted by encouraging discussion and creation using the basic paper templates prior to input.

Post Cycle Review & Retrospective

Following the first cycle, the team were sent a second copy of the survey questions used previously including a general comments section. In line with Agile practices a Retrospective [45], [47] meeting also took place and feedback in the College's preferred form "What Went Well" and "Even Better If" [118] was captured. The resultant analysis highlights that that the

team found benefit from the activities which took place. Equally a number of good ideas were also put forward by the team for future consideration.

What Went Well	**Even Better If**
Personas, really useful to get into the mind of the Attacker.	We should use Personas for representing a deeper look on our users too.
Personas.	Struggled to see the benefit of the picture. I don't feel that it would be easy to translate into a specification.
Rich Picture. Tool useful for drawing anything, not a fixed format like some other diagrams.	Can we have more workshops to discuss security.
Both seem to be good tools.	Do more!
Good opportunity to engage with colleagues from other teams and bring different perspectives into play.	I didn't feel these two ideas would fully cover all of the Cyber Risks the College faces.

Table 7 - Cycle 1 WWW & EBI.

Specifically, as had been observed by their interaction the Infrastructure team reported that the use of a Rich Picture enhanced their understanding of the threats facing the College.

> *"Drawing things out is better than spending lots of time writing complicated risk assessments."*
>
> *(IT INFRASTRUCTURE TEAM MEMBER)*

> *"The Rich Picture made a lot of sense, my team who already use a lot of diagrams were able to think about our environment and then add to that areas where we may be weak or where we might get attacked."*
>
> *(IT INFRASTRUCTURE TEAM MEMBER)*

Speculation as to why the Rich picture technique worked better with Infrastructure team than had previously worked with Systems team revolves around the way the team normally use diagramming. The Infrastructure team often utilise less formal diagrams to describe changes to network configurations, services to be deployed and for other major changes. Conversely the Systems teams preference can lay toward formal diagramming e.g. Entity Relationships, Class Diagrams, Data Flows.

Looking at the scoring, the most notable increase can be seen when looking at the score for the use of Agile Tools (See Below), originally indicating that the team were sceptical or lacking in knowledge (Cycle 0 - Mdn=0,n=7,f=88.89%) the median score in this area rose by three points (Cycle 1 -Mdn=3,n=7,f=55.56%).

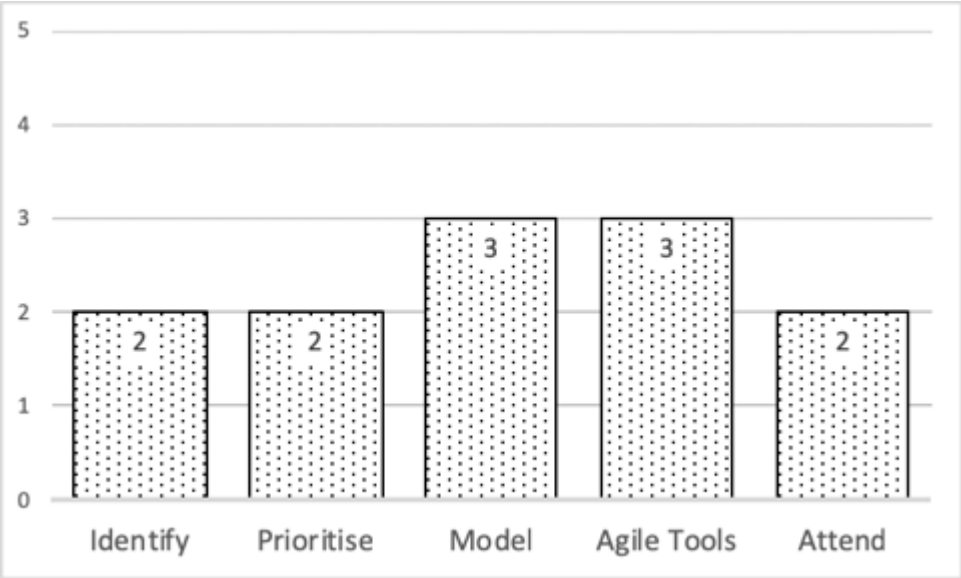


Figure 27 - Plot of Median Responses to Post Cycle 1 Questions

Other areas of feedback relate to the use of Personas, one respondent commented that they felt that their use makes more sense for traditional users, this correlated with feedback in the Even Better If section. A further comment received highlighted a point of improvement for a future cycle, relating to prioritising which threats or risks to mitigate or defend against.

Using the model defined by [103], the outcomes of the first cycle have been documented. Furthermore, a number of opportunities to explore in future cycles were identified.

Question	Research Issue	Research Question	Chosen Option	Evidence	Follow Up
RQ2.1	What threats does the college face.	How do we identify the high level threats facing the college.	Rich Picture	Positive survey scores. Positive observations of the Infrastructure Team. Completed Rich Picture.	Consider further why the Systems team do not find use in the Rich Picture method. Explore how the systems team could use Agile Methods in their developments in order to consider Threats and Risk.
RQ2.2	Who or where do these threats come from?	How do we begin to explore the types of user we may face threats from and their motives.	Attacker Personas	Positive survey scores. Positive observations. Completed Attacker Personas. New Persona Issue type in Jira instance.	Utilise Personas for other projects e.g. in Developments. Explore methods for Prioritising Risks mitigations.

Table 8 - Outcomes of the First Cycle

9.3 Second Cycle

Planning

Following the outcome of the first cycle, two ideas for further improvements were identified and considered. Again alignment with the overarching research questions was made and a single sub-question has been proposed for experimentation and analysis.

Question	Research Issue	Research Question	Proposed Value	Options (*Chosen **)
RQ1.1	The Systems team need to be able to document security risks and threats on a software project.	How do we identify the risks and threats to a particular software system in development.	The development of methods for analysing the threats and risk relating to a specific system.	*Use Case Diagram ** *User Stories ** Threat Analysis ISO27005. Risk Assessment ISO27005. ISO27002 14.1 Security requirements of information systems. ISO27002 14.2 Security in development and support processes.

Table 9 - Issues, Questions and Value for the Second Cycle

In light of the perceived success relating to the application of a Rich Picture and Personas, further Agile techniques were selected for the second cycle. These include both an investigation of Use Case Diagrams and User Stories in their negative forms Abuse Cases, Abuser Stories.

Participants for the second cycle were narrowed, and included the Systems team, and the Infrastructure and Service Desk team leaders. This approach was chosen in order to concentrate the work on a particular system in development utilising the expertise of other senior colleagues at a high level.

At the outset of this Cycle, the team had already begun to carry out a high level analysis ahead of the first sprint on a new project. The project involves an overhaul of the College's online/cashless payment platform dubbed RunshawPay.

Abuse Case Diagram

As with the previous Cycle, the experiment was performed within the confines of a Facilitated Workshop (Appendix 6.3 – Second Cycle, Abuse Case Workshop). Prior to this session, the existing Use Case diagram was shared with the participants along with a paper covering Abuse Cases [66].

During the workshop, the team, with reference to the Attacker Personas created during the previous cycle selected a number of new Mis-Actors. The process followed the outline proposed in the paper [67], for each of the traditional Use Cases a discussion took place surrounding what miss-use may look like and relevant Abuse Cases were added to the diagram.

The team took the decision that these Abuse Cases and Mis-Actors would be represented in Red as opposed to intended Use Cases and Actors in Green to further highlight the differences.

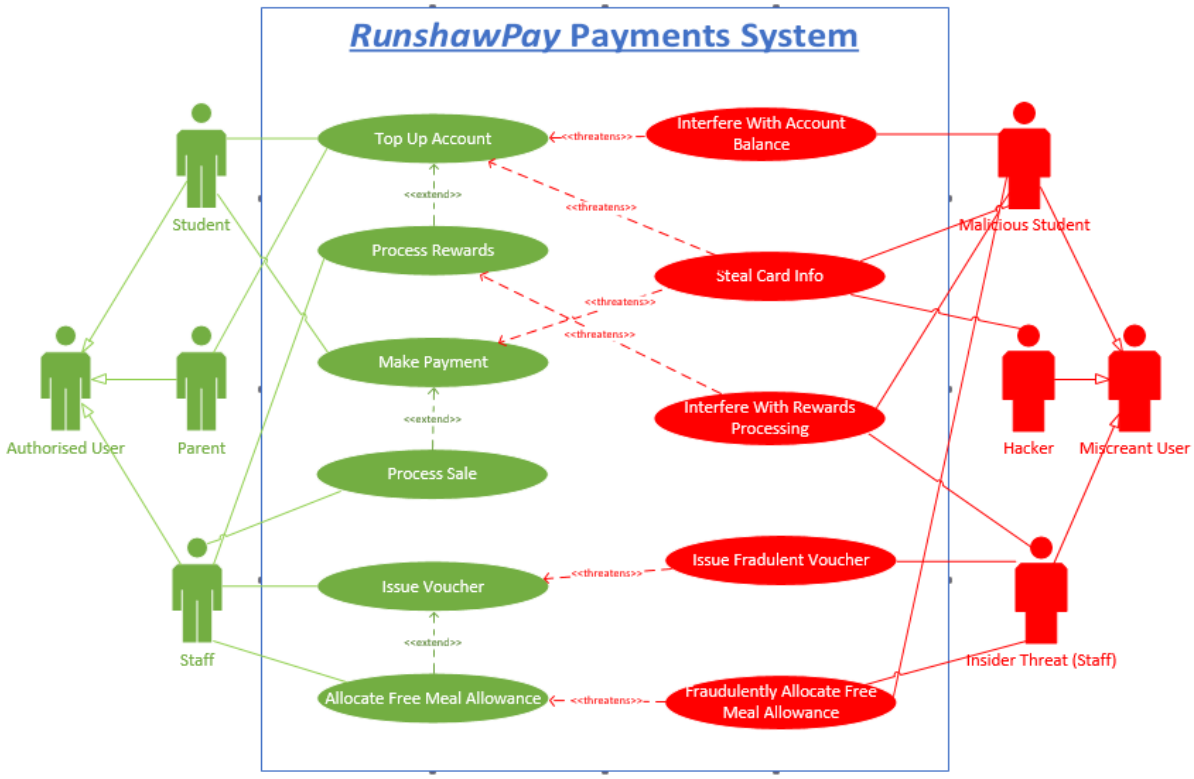


Figure 28 - Abuse Cases and Mis-Actors added to a Use Case Diagram

Previous to this activity taking place, the team had only briefly considered security requirements when considering constraints against traditional Use Cases and User Stories.

During the observation of this session, it was noted that the Systems team appeared more comfortable with this type of diagramming probably attributed to their existing processes adopting Use Case Diagrams.

Abuser Stories

The latter portion of the project's first Story Writing Workshop was reserved in order for the team to focus on Abuser Stories. Previous to the session the team had elicited a number of high level epics (below) and User Stories during discussion with key stakeholders.

Summary	Description
Rewards Processing	As the Catering Manager, I want to operate a reward scheme to encourage the use of the cashless payments.
Voucher Issue	As the Finance Director, I want teams to be able to issue vouchers for specific purposes so that students can use them to pay.
Top Up RunshawPay	As the Catering Manager, I'd like everyone to pay using Runshaw Pay so that there is No Delay!

Table 10 - Epics in the RunshawPay Project

At the outset of the session, the team were shown a video to set the scene and help to focus on the approach [119], previous to this two papers' had also been shared [74], [78].

What became immediately clear during the session is just how difficult the stories are to write, one of the team members commented that:

"these seem impossible to write because we don't have a customer to bounce the idea off."

However with that said, the team were able to identify and discuss a number of Abuser Stories linked to the original epics. These for the most part aligned with the Abuse Cases identified in the previous Cycle.

Abuser Story
As a Hacktivist, I want to overwhelm the RunshawPay app with traffic so that students aren't able to top up in and the ensuing chaos will cause reputational damage.
As a hacker, I want to take over the RunshawPay topup system and convince users to top-up via my fraudulent solution in order to steal their money.
As a hacker, I want to acquire RunshawPay users details so that I can steal money via a bitcoin Phishing campaign.
As a Malicious Student, I want to be able to allocate myself Free College Meals status so that I can have free Chicken Wraps at lunch.
As a Malicious Student, I want to be able to issue vouchers so that I can attend trips and get products without paying.
As a malicious Student, I want to interfere with the rewards process so that I can acquire free credit to use on Runshaw Cookies and Chicken Wraps
As a hacker, I want to intercept Credit Card information so that I can use the details to make transactions and profit.
As a Malicious Student, I want to modify my RunshawPay balance so that I can get Runshaw Cookies and Chicken Wraps without paying.

Table 11 - Abuser Stories

As is common for the team, as each story was discussed it was then input into the Project's management system (Jira Software) and assigned to the relevant epic (below).

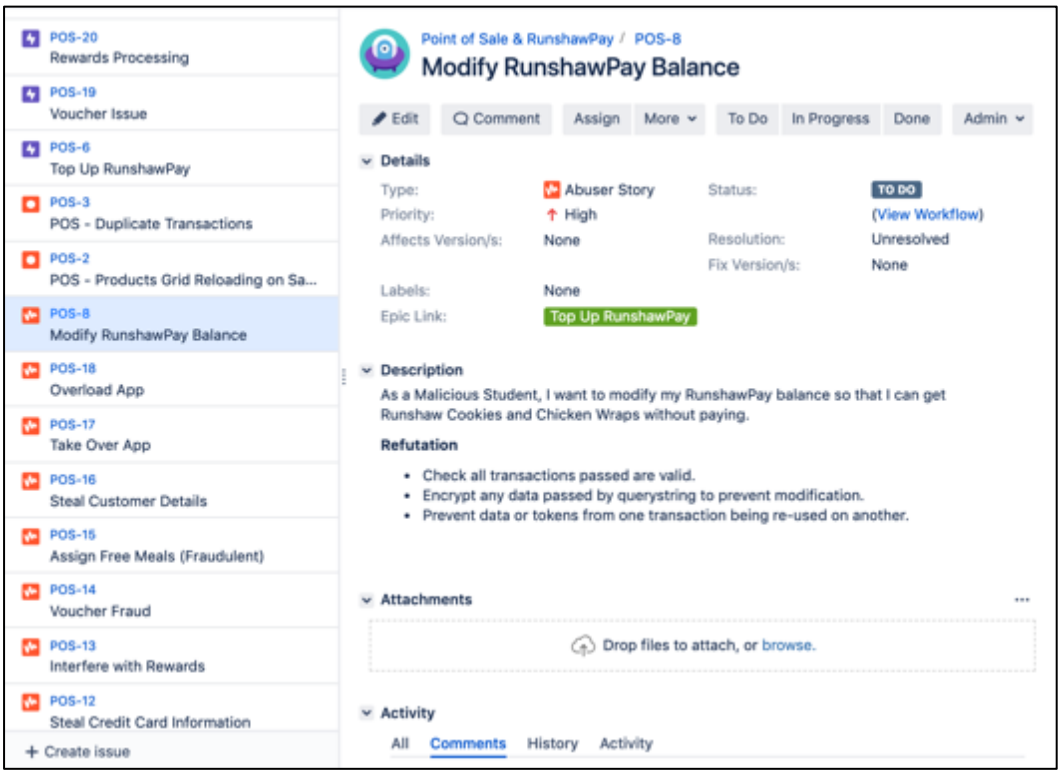


Figure 29 - Abuser Stories in the Jira Project

The project's Agile Board within Jira Software was updated to include on of the Abuser Stories in the first iteration (below).

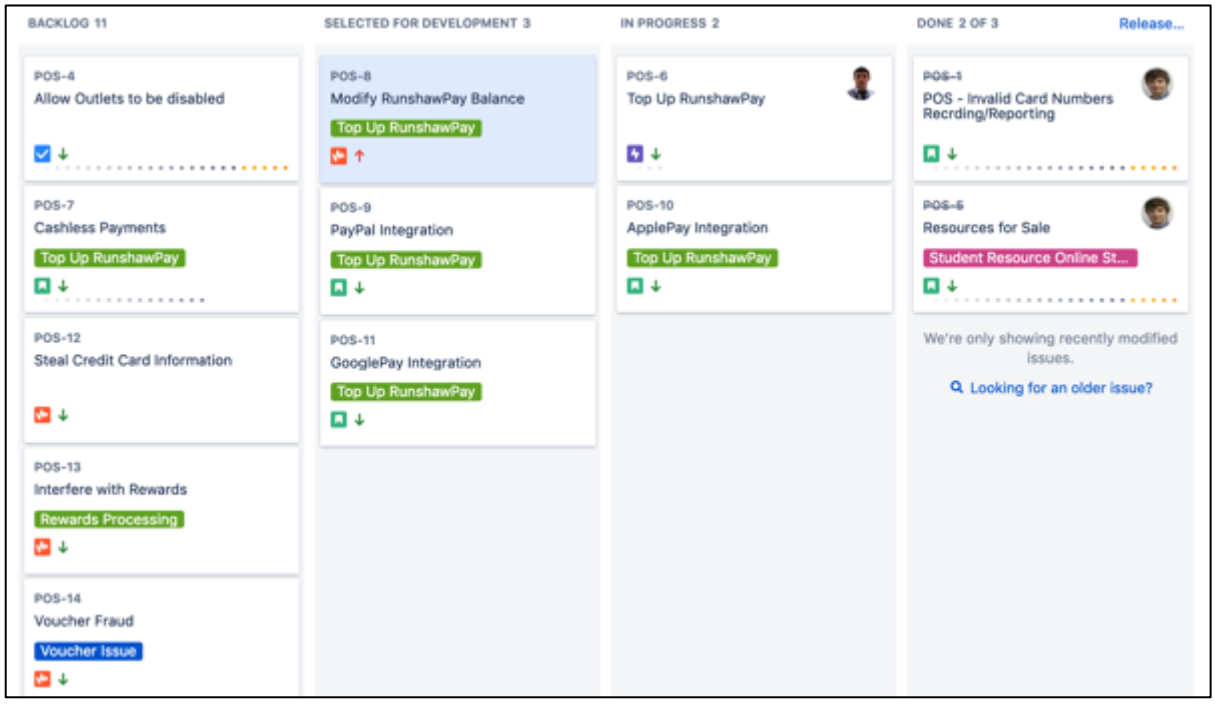


Figure 30 - Abuser Stories on the Project Kanban Board

Post Cycle Review & Retrospective

A retrospective discussion, and retrospective survey both took place at the end of the second cycle as had occurred during the first cycle.

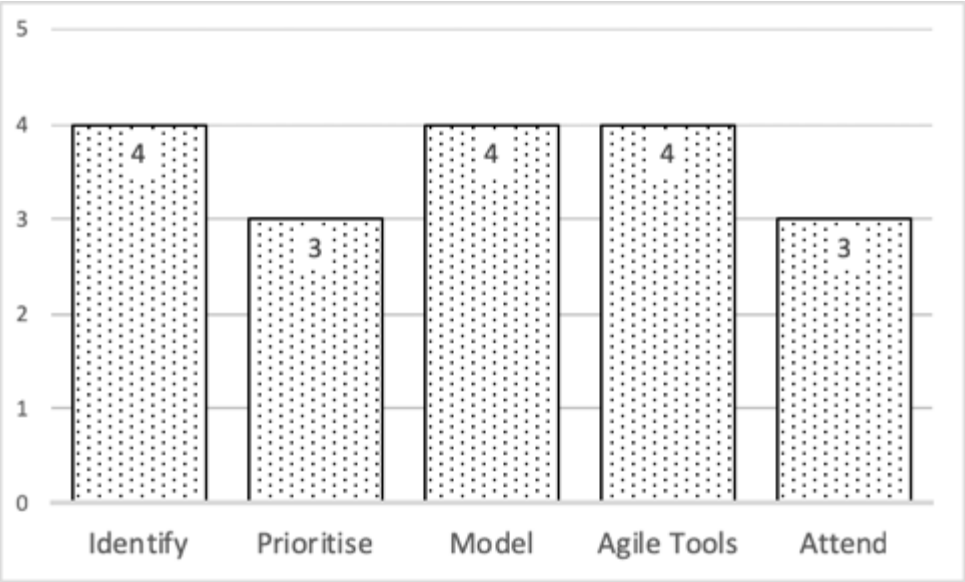


Figure 31 - Post Cycle 2 Scores

These both showed that the team valued the approaches, and that confidence in the use of Agile methods also increased (Mdn=4,n=3,f=60%).

What Went Well (Post Cycles Only)	Even Better If (Post Cycles Only)
Capturing ideas using the diagram.	Somehow get a better grip on what the negative users may do.
We already use the use case diagram and user stories so these additional types are easy to fit into our existing process.	It's not as easy to do Abuser Stories because there is no customer to talk with.

Table 12 - WWW & EBI From Cycle 2

Of the few items of 'Even Better If', again a resurgent theme from the session appeared. The team showed concern that without customers (the negative customers) it's difficult to elicit the Abuser Stories. The team enjoy a very positive working relationship with our customer base and User Story workshops generally result in lots of collaboration and the creation of detailed stories.

In a private email following the session, a request was also sent asking whether it was possible to call the Abuser Stories something else. Their reasoning was that given our educational context, and the work of colleagues in the Safeguarding team the title may give rise to concern and confusion.

The lowest scoring area of the survey in this cycle related to the ability to prioritise Information Security Risk, and this was chosen to be the subject of the third and final Cycle. The cycle outcome grid was completed (below).

Question	**Research Issue**	**Research Question**	**Chosen Option**	**Evidence**	**Follow Up**
RQ1.1	The Systems team need to be able to document security risks and threats on a software project.	How do we identify the risks and threats to a particular software system in development.	Abuse Case Diagram Abuser Stories	Positive survey scores. Positive observations of the Systems Team. Completed Abuse Case Diagram. Abuser Stories and Epics.	Consider new title. Work out how to increase comfort with prioritisation. Further work to help with identification due to lack of 'Customer' for collaboration.

Table 13 - Outcomes of the Second Cycle

Cycle 2 – Post Script

Of some interest, early in the development of the first sprint for the project the team have begun to identify additional Abuser Story scenarios, and these are being actively added to the backlog and worked.

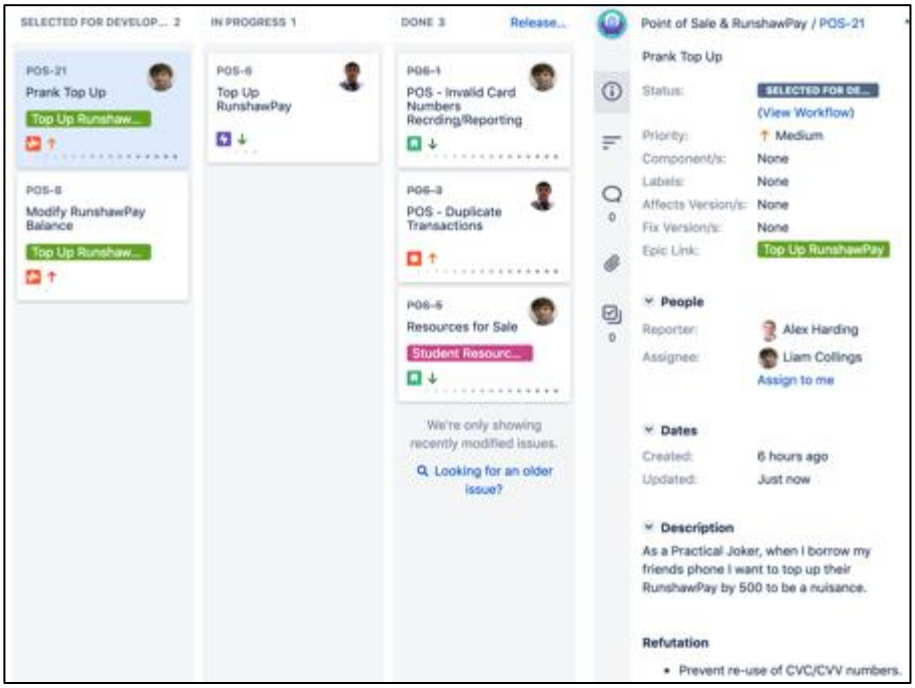


Figure 32 - Additional Abuser Story

9.4 Final Cycle

Planning

Following the second Cycle, it became clear that in order to fully appreciate the Threats and Risks facing the College that time must be set aside to carry out a comprehensive Risk Assessment, and to begin to devise a Risk Mitigation Plan.

With that in mind, and keeping the theme of utilising Agile methods and tools where available and relevant, the idea that once Risks have been identified, and assessed that they should be prioritised in a similar fashion to the team's User Stories was discussed.

Question	Research Issue	Research Question	Proposed Value	Options (*Chosen **)
RQ2.3	The team need to be able to efficiently carry out an Information Security Risk Assessment, and prioritise mitigations.	How do we assess the risks and threats and prioritise mitigations.	The development of methods assessing and prioritising risk.	*Risk Assessment ISO27005.* *Moscow Prioritisation.*

Table 14 - Issues, Questions and Value for the Third Cycle

As with the second Cycle, a single sub-question has been posed and will be investigated. A the heart of any Information Security Management System is a comprehensive Risk Assessment and Risk Management Regime [13], [16], [88], [97].

Risk Assessment

Risk Management Policy

Prior to the outset of this study, the College had no formal method for documenting Information Security Risk, an overall Risk Management policy however did exist. This policy [120] set the bar for the College's risk tolerance at LOW. Any risk seen to exceed this level is therefore required to be mitigated.

As we saw earlier, the accepted method of calculating the level of risk involves a simple calculation:

Risk= Likelihood * Impact

Figure 33 - Risk Measurement Calculation.

The categorisation of both factors, Likelihood and Impact had already been identified in the overarching Risk Management Policy.

Impact	**Likelihood**
1 - Negligible	1 - Improbable – No instances within a 3-year time period.
2 - Minor / Localized	2 - Unlikely - No instances within a 2-year time period.
3 - Moderate / Limited	3 - Likely - Occasional occurrence.
4 - Significant / Large	4 - Very Likely - Frequent occurrence.
5 - Extensive / Widespread	5 - Almost Certain – Multiple occurrences per year.

Figure 34 - Impact & Likelihood Scores

The computation of these factors then results in the identification of the score for a particular risk, this can be charted using the matrix below:

Impact / Severity	Likelihood / Probability				
	1 Improbable	**2 Unlikely**	**3 Likely**	**4 Very Likely**	**5 Almost Certain**
1 Negligible	1	2	3	4	5
2 Slight	2	4	6	8	10
3 Moderate	3	6	9	12	15
4 High	4	8	12	16	20
5 Very High	5	10	15	20	25

Figure 35 - Risk Impact / Severity Matrix

The high level Risk Management Policy, also then defines those risk levels for which mitigation must be completed. That is any item that exceeds a score of 4, thus taking it into the MEDIUM risk category.

After some discussion, it was decided that an appropriate method of categorising the required activities should follow the MoSCoW [47] prioritisation method. This is also the suggestion of [121].

HIGH risks will be instantly assigned to the “Must Treat” category, and those risks identified as MEDIUM to the “Should Treat” category.

Risk	Score	MoSCoW
HIGH	10-25	Must Treat
MEDIUM	5-9	Should Treat
LOW	3-4	Could Treat
	1-2	Won't Treat (At First)

Figure 36 - MoSCoW Prioritisation for Risk

As can be seen from the figure above, the LOW risk level has been split into two, taking the line that the lowest of those risks fits most aptly into the "Won't Treat (At First)" category. Those risks in the higher division of LOW will be prioritized as "Could Treat".

A number of treatment actions in line with the College's overarching Risk Management Policy have also been defined. Their alignment to the ISO27000 [13] series has also been documented.

Treatment Action	Treatment Action (from ISO27005)	Description (from ISO27005)
Avoid	Avoidance	The activity or condition that gives rise to the particular risk should be avoided.
Transfer	Sharing	The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation.
Mitigate	Modification	The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable
Accept	Retention	The decision on retaining the risk without further action should be taken depending on risk evaluation.

Table 15 - Risk Treatment Options

The use of these various Risk Treatment Options will always depend on both the College's priorities, and financial situation as well as technical feasibilities and relevant standards.

In order to carry out the Risk Assessment process effectively, discussion also led the team to align the roles and responsibilities with ITIL's RACI [122] model. This model sets out those who are Responsible, Accountable, Consulted and Informed regarding any decision or element.

Role / **Step**	**Director of Finance**	**IT Manager**	**IT Team Leaders**	**IT Team**	**Data Protection Officer**
Risk Identification	I	A	R	C	C
Risk Acceptance Criteria	A/R	C	I	I	I
Analyse & Evaluate Risks	I	A	R	C	C
Select Controls	C	A	R	C	C
Obtain Residual Risk Approval	A	R	I	I	I
Monitor & Report	C	A	R	C	C
Regular Review	C	A	R	C	C

Table 16 - RACI Model for Information Security Risk Management/Assessment

These various aspects have been combined to become the College's Information Security Risk Management & Assessment Policy [123].

Assets

An important next phase for the team was to identify the Assets (and Services) which may be under threat, or may be made vulnerable. The team quickly decided that with the volume (100s) the best way forward was to assign priorities to both Assets and Services.

The team's Jira solution was updated to include the following priorities:

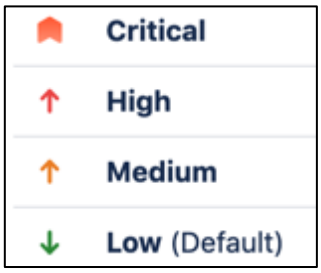


Figure 37 - Asset & Service Priorities in Jira

Once defined, the team then worked through the College's Assets and Services assigning a priority in line with business requirements. The list has been circulated to the College's Senior Management Team for ratification.

The results of this high level prioritization can then be seen across the full Jira solution, where Assets and Services are displayed and linked together.

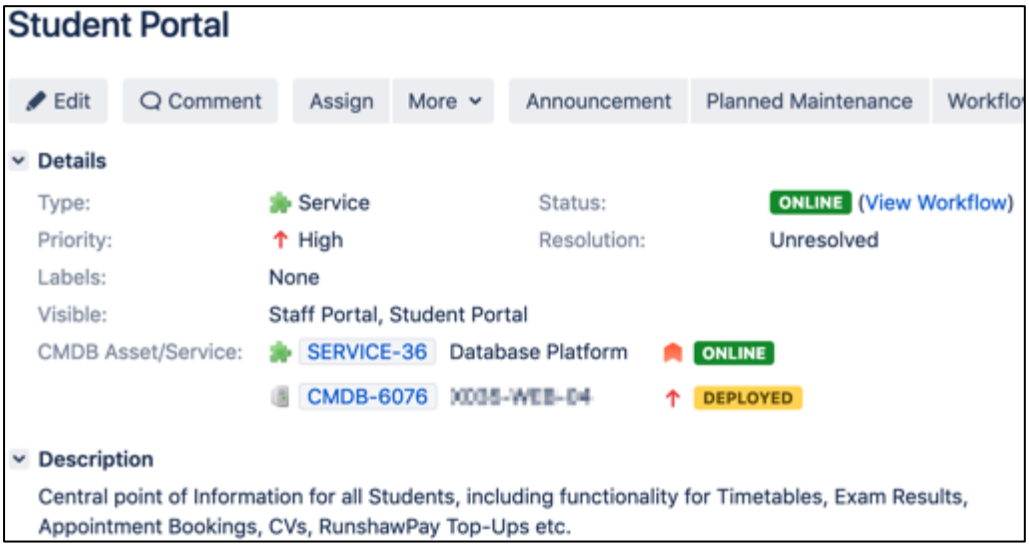
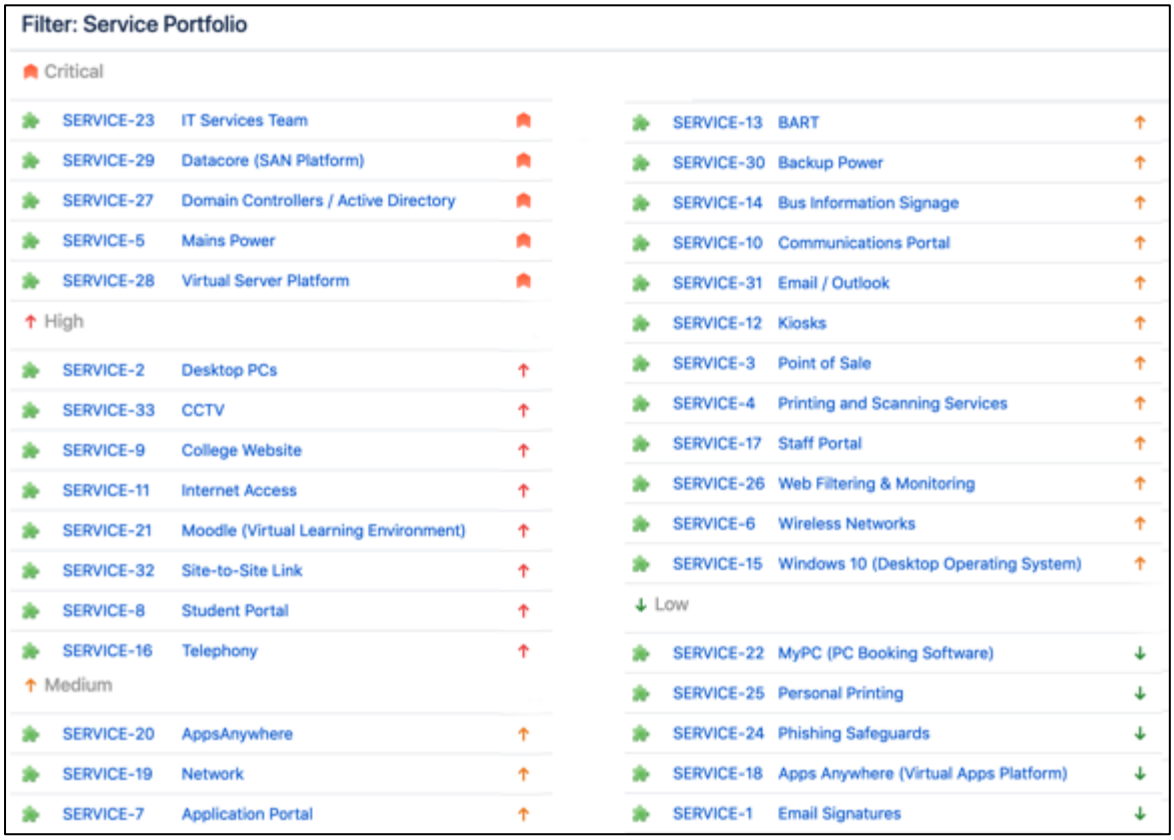


Figure 38 - Service Record from Jira Showing Priorities and Linked Assets

Additionally, the priority Icons can also be seen against individual Assets and Services.



Filter: Service Portfolio

Critical

SERVICE-23	IT Services Team		SERVICE-13	BART	↑
SERVICE-29	Datacore (SAN Platform)		SERVICE-30	Backup Power	↑
SERVICE-27	Domain Controllers / Active Directory		SERVICE-14	Bus Information Signage	↑
SERVICE-5	Mains Power		SERVICE-10	Communications Portal	↑
SERVICE-28	Virtual Server Platform		SERVICE-31	Email / Outlook	↑
↑ High			SERVICE-12	Kiosks	↑
SERVICE-2	Desktop PCs	↑	SERVICE-3	Point of Sale	↑
SERVICE-33	CCTV	↑	SERVICE-4	Printing and Scanning Services	↑
SERVICE-9	College Website	↑	SERVICE-17	Staff Portal	↑
SERVICE-11	Internet Access	↑	SERVICE-26	Web Filtering & Monitoring	↑
SERVICE-21	Moodle (Virtual Learning Environment)	↑	SERVICE-6	Wireless Networks	↑
SERVICE-32	Site-to-Site Link	↑	SERVICE-15	Windows 10 (Desktop Operating System)	↑
SERVICE-8	Student Portal	↑	↓ Low		
SERVICE-16	Telephony	↑	SERVICE-22	MyPC (PC Booking Software)	↓
↑ Medium			SERVICE-25	Personal Printing	↓
SERVICE-20	AppsAnywhere	↑	SERVICE-24	Phishing Safeguards	↓
SERVICE-19	Network	↑	SERVICE-18	Apps Anywhere (Virtual Apps Platform)	↓
SERVICE-7	Application Portal	↑	SERVICE-1	Email Signatures	↓

Figure 39 - Service Portfolio with Priorities Added

Physical - Server/Appliance/Host ⓘ Edit queue Delete queue

Key	Server Type	P	Summary	Updated	Asset Manufacturer	Asset Model	IP Address	Status
CMDB-6087	Server (Physical)		[redacted]	27/03/2019	Dell	R530	[redacted]	DEPLOYED
CMDB-6088	Server (Physical)		[redacted]	27/03/2019	Dell	R530	[redacted]	DEPLOYED
CMDB-6089	Server (Physical)		[redacted]	27/03/2019	Dell	R530	[redacted]	DEPLOYED
CMDB-6090	Server (Physical)		[redacted]	27/03/2019	Dell	R530	[redacted]	DEPLOYED
CMDB-6078	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6079	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6080	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6081	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6082	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-5984	Appliance (Physical)	↑	[redacted]	27/03/2019	Smoothwall	S14	[redacted]	DEPLOYED
CMDB-6083	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6084	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6085	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6086	Host	↑	[redacted]	27/03/2019	HPE	DL360	[redacted]	DEPLOYED
CMDB-6091	Appliance (Physical)	↑	[redacted]	27/03/2019	Smoothwall	S8	[redacted]	DEPLOYED

1-15 of 15

Figure 40 - Selection of Physical Assets with Priorities Added

Once the Assets and Services had been prioritised, focus then moved to considering what types of threats may be present.

Threats & Vulnerabilities

Following the identification of Assets and Services with reference to the Rich Picture analysis from Cycle 1, the team then worked to identify possible threats to the Assets & Services. As with other artefacts these have been stored in the teams Information Security Management System in Jira. Each Threat has also been assigned to a category defined by combining and adapting two models [27], [28].

Key	Status	Summary	Threat Category
ISMS-136	LIVE	Fuel Shortage	Operational
ISMS-142	LIVE	Supplier Failure / Bankrupcy	Operational
ISMS-139	LIVE	IT Staff Loss of Skill	Operational
ISMS-138	LIVE	IT Staff Sickness	Operational
ISMS-150	LIVE	Accidental Loss	Human
ISMS-149	LIVE	Human Error	Human
ISMS-3	LIVE	Accidental Deletion	Human
ISMS-2	LIVE	Data Exfiltration	Human
ISMS-148	LIVE	External Miscreant	Human
ISMS-137	LIVE	Internal Miscreant	Human
ISMS-159	LIVE	Privileged Access for Unauthorised Users	Human
ISMS-151	LIVE	Severe Weather	Natural
ISMS-16	LIVE	Fire	Natural
ISMS-15	LIVE	Flood	Natural
ISMS-14	LIVE	Power Outage	Environmental
ISMS-152	LIVE	Software Failure	Technical
ISMS-143	LIVE	Phishing Emails	Technical
ISMS-4	LIVE	Hardware Failure	Technical
ISMS-153	LIVE	Malware	Technical
ISMS-144	LIVE	Denial of Service Attack	Technical
ISMS-154	LIVE	Sabotage	Phsyical
ISMS-141	LIVE	Damage to Cables	Phsyical
ISMS-140	LIVE	Theft	Phsyical

Figure 41 - Sample of Threats stored in Jira

Two additional categories which were also discussed as being relevant are Legal and Business, though at this stage no Threats have been assigned to them. The combination of the defined Services and Assets as well as the possible threats then leads to the documentation of Risks.

Analysing & Recording Risks

As we saw previously, A Risk relates to the potential that a given threat, may exploit Vulnerabilities of an Asset and thereby cause harm to an organisation [13]. We can measure Risk using the formula we saw above. The method agreed is that the Risk will be measured prior to, and after any mitigations have been applied, and in addition, where the resultant risk is still in excess of the College's Risk Tolerance (LOW) then it will be escalated to the Senior Management Team for sign-off and acceptance or for authorisation of additional mitigations.

The team devised a new Issue type (Risk) and a data collection screen within the Jira solution, which allowed the definition and scoring of a risk, as well as consideration for mitigation options, and resultant risk. Three tabs were created, each to compartmentalise part of the Risk Analysis process.

The first tab simply identifies which asset or service could be impacted by the Risk. Moving from there, the second tab concerns itself with analysing that risk, links are made to relevant threats and the Risk's Impact and Likelihood are scored. This second tab also has a calculated field to compute the Risk score, and Risk Level.

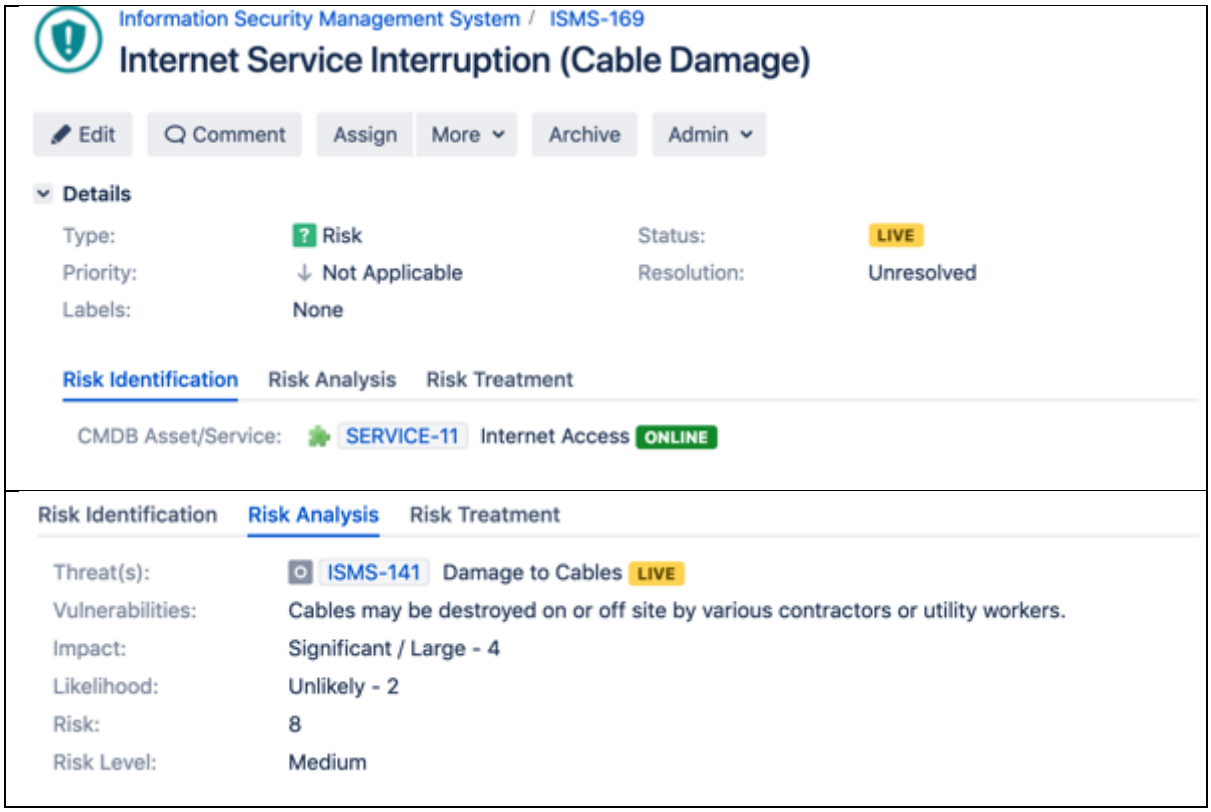


Figure 42 – Sample of Risks stored in Jira

Based upon the results of the Risk Analysis, the Treatment Suggestion is automatically populated utilisiing the MoSCoW like options defined in the first part of this Cycle.

The team are able to select applicable controls, from two defined lists, that of the ISO27002 suggested controls, and the shorter control set for Cyber Essentials. This in turn will in the future allow for simple reporting against the control areas.

Once a mitigation has been selected and implemented, the Residual Impact and Likelihood is input and a new Residual Risk and Residual Risk Level is calculated.

A sample of the Risks which were defined during this Cycle can be seen below, a number of these Risks already had live mitigations which simply required documenting. Other Risks are new and their migrations are pending review and approval.

Risks Switch Queues ⌄ Edit queue Delete queue

Key	Status	Summary	Updated	Risk	Risk Level	Treatment Suggestion	Treatment Action	Residual Risk	Residual Risk Level	Selected Mitigations
ISMS-160	NEW	Unauthorised Use of Credentials	31/03/2019	12	High	Must Treat	Mitigate	4	Low	ISMS-161 Two Factor Authentication NEW ISMS-168 Password Policy LIVE
ISMS-155	NEW	Disclosure of Information on Unattended Desks	31/03/2019	9	Medium	Should Treat	Mitigate	4	Low	ISMS-156 Clear Desk Policy NEW
ISMS-145	LIVE	Data Breach due to Phishing	31/03/2019	12	High	Must Treat	Mitigate	4	Low	ISMS-146 Staff Phishing Training LIVE ISMS-147 Email notifications EXTERNAL and SPOOF LIVE
ISMS-157	LIVE	Recycling Contractor May Not Follow Due Process	31/03/2019	8	Medium	Should Treat	Mitigate	4	Low	ISMS-158 Visit & Audit Recycling Contractor LIVE
ISMS-169	LIVE	Internet Service Interruption (Cable Damage)	31/03/2019	8	Medium	Should Treat	Mitigate	6	Medium	ISMS-170 Multiple Internet Links LIVE ISMS-171 Diversely Routed Site-to-Site Links LIVE
ISMS-18	LIVE	Power Outage	31/03/2019	8	Medium	Should Treat	Mitigate	4	Low	ISMS-134 Backup Power - UPS LIVE ISMS-135 Backup Power - Generators LIVE
ISMS-167	LIVE	Theft of PCs	31/03/2019	6	Medium	Should Treat	Mitigate	2	Very Low	ISMS-172 Padlocks/Chains - Lower Floor PCs & Macs LIVE
ISMS-17	LIVE	Generator Failure	31/03/2019	9	Medium	Should Treat	Mitigate	4	Low	ISMS-173 Generator & UPS Maintenance Contract LIVE ISMS-175 Monthly Generator Test LIVE ISMS-174 Quarterly Mains Failover Test LIVE

Figure 43 - Sample Risks defined in Jira

Prioritising Mitigations

The team also decided that having the relevant mitigations documented in their own separate record, will both allow for re-selection and for ease of reporting. These are linked directly in the Risk's Treatment tab, and also have links to the controls this particular mitigation represents.

Figure 44 - Sample Mitigation from Jira

Post Cycle Review & Retrospective

As with the previous two cycles, a further discussion was arranged in order to gather feedback on this final cycle. Of note is that this final cycle resulted in the overall median score being bolstered at 4/5 (Mdn=4,n=4,f=80%).

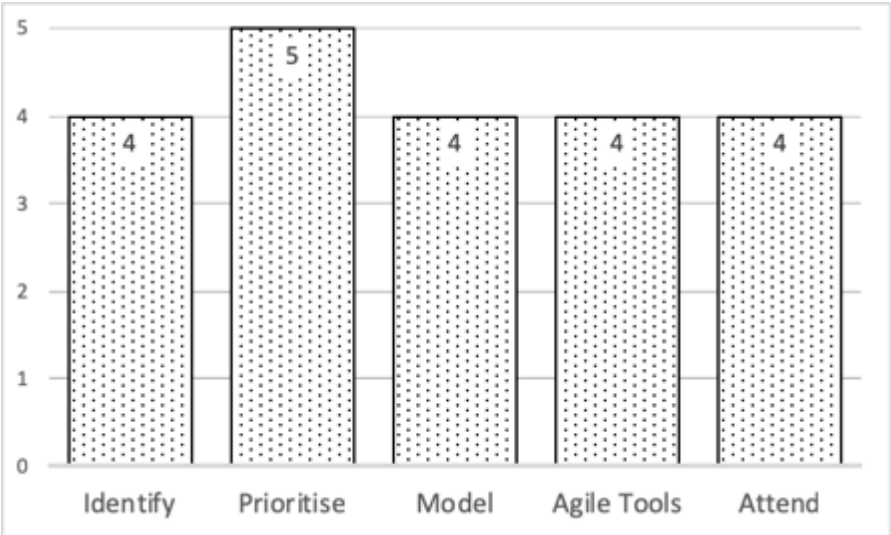


Figure 45 - Post Cycle 3 Scores

We can see from the WWW/EBI analysis, that the team found these activities informative and powerful. As a group the team were able to take the College forward, from having no Information Security Risk assessment to one with an agreed structure, and detail

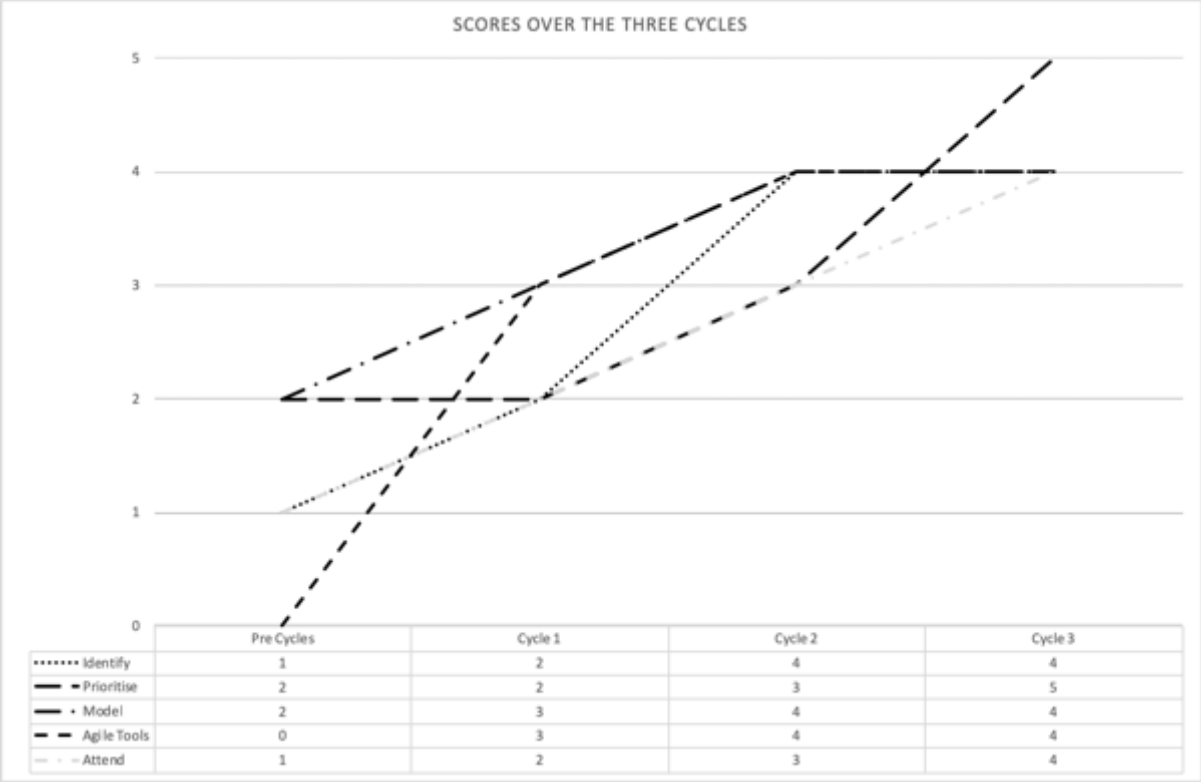
What Went Well (Post Cycles Only)	**Even Better If (Post Cycles Only)**
Jira's flexibility means we can link these new types to existing things, so maybe we have a fault that develops and we can link it to the mitigation for that device.	We need to spend more time considering the risks, we have a good method now, and the Moscow helps to decide what to sort out first.
The tools from previous stages in the project helped speed up looking at threats for example. Before this work we had no clue about all the threats we might face but we are probably missing lots still.	More time spent as a team looking at this kind of thing. I've enjoyed working with different people to look at this.
Using tools like jira makes it easier to document, scoring and prioritising risks makes it easier to know what to do, the rest can be backlog.	

Table 17 - Post Cycle 3 WWW & EBI

We can see that the Agile techniques explored in this Cycle were well received by the team and they perceived an improvement in our practices as a result.

10 Findings After Three Cycles

By looking at the survey scores across all three cycles, and the pre-cycle survey we can see a growth in knowledge and confidence across all of the areas (Identifying Risks, Prioritising Mitigations, Modelling Security Requirements and Using Agile Tools).



	Pre Cycles	Cycle 1	Cycle 2	Cycle 3
Identify	1	2	4	4
Prioritise	2	2	3	5
Model	2	3	4	4
Agile Tools	0	3	4	4
Attend	1	2	3	4

Table 18 - Graph Depicting Growth in Scores over the Cycles.

This growth can be further identified in the overall Median Scores for each cycle, where we see improvement in both the score itself, and with the overall percentages.

Pre Cycles	(Mdn=2,n=2,f=40%)
Cycle 1	(Mdn=3,n=2,f=40%)
Cycle 2	(Mdn=4,n=3,f=60%)
Cycle 3	(Mdn=4,n=4,f=80%)

Table 19 - Overall Median Scores (Per Cycle)

The majority of comments received were also positive (n=10,f=53.6%), highlighting a number of new areas of good practice that can be taken forward by the team. Of particular note, we see that the Rich Picture, Personas and Abuse Case workshops gathered the larger proportion

of positive remarks. Less favorable at the time of questioning was the use of Abuser Stories, though as identified later the team did begin to create, proritise and develop against new Abuser Stories as the project continued.

This also aligns with scoring where we saw the largest improvement across the three cycles for the use of Agile Tools & Techniques (Mdn=+4).

Unfortunately, due to time constraints the comparison of Information Security incident volumes following the completion of these cycles is unavailable.

11 Discussion

The posture survey revealed that a low number (n=4,f=17.39%) of respondent organisations had dedicated Cyber/Information Security Posts. Just over a third (n=8,f=34.78%) as of that time had completed any formal Information Security Risk Assessment. That withstanding, we also see a strong proportion (n=15,f=65.22%) of organisations rating Cyber Security as being of High or Vital Importance.

Combining these three components we can deduce that lightweight Methods of handling Security matters could be of interest to organisations. Survey respondents also showed alignment to this conclusion with the majority (n=13, f=56.52%) indicating a willingness to explore Agile methods to document and analyse Information Security Risk.

A question posed earlier in this paper was that regarding Information Security, is '*Just Good enough actually good enough?*'. Ultimately, the answer to this will always have to be *no*, and we can base this assertion on the simple fact that the threat landscape is ever changing [11]. We saw that demonstrated with the re-ordering of major threats between the survey results in this study and previous studies [3], [11]. Putting that thought aside however it is undeniable that the results of the exploration of Techniques in this study have brought about benefits.

As of yet, no one Technique or Method is claiming absolution nor completeness [96], and some even argue that Agile methods themselves can result in the production of less secure software [86]. Not all of the Methods uncovered by the literature review have been implemented. However all of the Techniques explored resulted in improvements in the perceived impact of Agility, cycle after cycle. The use of these Techniques also resulted in the creation of artefacts the team found of use, and that were able to expand the teams understanding of the current cyber threats facing the college.

As a result of the work linked with this study, the College now has a comprehensive Information Security Risk assessment, and now joins the growing number of organisations in the sector (n=8,f=34.78%)->(n=9,f=39.13%). One of the key themes explored in the literature [67] was the use of sequential processes leading toward a risk assessment, from the creation of Abuser Stories, which are then analysed and mitigated.

There tended to be a preference exposed by the team toward high level Techniques, especially those resulting in the creation of diagrams rather than lengthy prose. We can likely attribute this more to the learning styles of colleagues (and myself) than use it as a means of critiquing the Techniques themselves.

Regrettably one piece of feedback received concerned the emotive nature of the names chosen for some of the Techniques. Within the education sector, one of the essential duties at present is that of Safeguarding [124]. Essentially, protecting both children and vulnerable adult students from harm, or what we might also call *Abuse*. The term Abuse appears over 100 times in the overarching Safeguarding legislation [124].

An Abuser may have originally been defined in simple terms as 'A person who misuses, misapplies, distorts, or takes improper advantage of something.' [125], this definition certainly fits the bill for our negative actors. Modern usage however, moves away from this definition towards those who would Abuse drugs, or worse carry out acts of violation, mistreatment and injury [125].

The level of emotion, surrounding the term Abusers may also be felt with some of the other popular terms such as Attackers and even Misusers. The latter again feeling some alignment with the drink or drug abusers.

Term/Title	**Total**	**Percentage**
Negative User Stories / Negative User Story	12	10.43%
~~Abuser Stories / Abuser Story~~	23	20.00%
~~Attacker Stories / Attacker Story~~	2	1.74%
Evil User Stories / Evil User Story	11	9.57%
Security Stories / Security Story	42	36.52%
~~Misuse Story / Misuse Stories~~	24	20.87%
~~Misuser Story / Misuser Stories~~	1	0.87%
	115	**1**

Table 20 - Terms with Emotive Entries Struck-through

If we discount these other titles, what's left is very little. Negative User Stories (n=12, f=10.43%) & Negative Use Cases as well as Evil User Stories (n=11, f=9.57%) do not feature regularly in the literature.

Security Stories (n=42,f=36.52%) is certainly a phrase that features more often, and Security Cases seems a sensible phrase too. There is a possible danger that this phrase in the negative form we need, does not always align with intended use of Security Stories [75] as perhaps the solution to an Abuser Story.

Language and emotion is a matter that has been studied widely [126]. Ultimately, human emotion is such that if the nomenclature doesn't aid both understanding the topic, and feeling comfortable with the phrasing then it's unlikely it will receive sufficient traction to become mainstream. One option would be to carry out a future Emotion Perception Study [126] to consider the way these varying titles affect the reader.

For now, in the absence of such a study the proposal is to call our new class of stories: Misuser Stories. This offers alignment with XML Misuse Cases [67].

A further point of discussion, is also whether Misuser Stories fit the true bill of an Agile Technique, thinking surrounding this is along the lines that were raised by a member of the team. There was a comment made that the Misuser Stories were difficult to write as we lacked a user to interact with, a point that has been echoed in the literature to some extent [86]. The Agile Manifesto teaches us that Customers & Collaboration as well as Individuals & Interaction are paramount [40].

Have we now answered the question of '*how do agile methods ensure that security requirements are continually met?*' [43]. This study has merely touched on a small proportion of the Techniques and Methods reporting to consider Security in an Agile way [127]. Ultimately as the author who posed this question suggests, Security within Agile is most certainly an area for further future exploration [43].

12 Critical Evaluation

Retrospectives [45] guide Agilists to inspect what we've been doing and adapt our practice, ITIL concurs with this approach too [48]. A number of models [128] exist to facilitate the capture of critical feedback, however the simple "What Went Well" and "Even Better If" [118] has been used to capture an initial overview.

What Went Well	Even Better If
Posture survey results of benefit to the education sector. Highlights key areas for improvement and consideration.	Time pressures and conflicting priorities hampered progress at some stages. Ultimately things caught up and the Just In Time approach prevailed.
Engagement from colleagues across the sector with the research and agile aspects added motivation.	Initial scope as per Plan too wide. Completion of all ISO27001 components unfeasible in the allotted time. Prioritisation of which components to include in this project too place.
Colleagues and the College's Senior Team took a keen interest in the project. The teams cooperation and patience ultimately brought about the success of the project.	Literature regarding some of the key themes of this project is lacking, however widening the literature scope would have detracted from the project.
The project afforded me the opportunity to shape the practice of the IT Services function, specifically focussing attention on Cyber/Information Security.	The Abuser Story concept was the least favourable of all the techniques in the project, however it had been hoped this would have the biggest impact.
Experimentation with and Utilisation of a number of new Agile techniques.	
The use of a Kanban board to track progress on key project and documentation tasks ensured focus was given to priority items.	
The cyclical nature of the Action Research method aligned well with the iterative and incremental workflows myself and the team are accustomed to.	

Table 21 - Post Project WWW & EBI

Assumptions & Experience

As has been identified in the WWW/EBI analysis, the project set out with a scope that quickly proved to be too expansive. During the initial planning, it became apparent that the ISO27000 series is a challenge to implement, as had been identified by authors previously [23]. The

research questions were then refined to take this into consideration and reduce the scope to a number of key processes and techniques which were felt to be of most benefit.

At the outset, time was depleted considering whether this project would be best suited and reflected as an Action Research or Case Study. Ultimately the decision was taken that as I was to be part of the project team, that an Action Research approach was most suited. Alignment is found with the literature, which promotes the use of Action Research in reflective practice. Specifically where the practitioner themselves leads the change and is embedded as part of it [102], [103]. The method also encourages the tracking of learning and development for all participants [102], [103].

As part of my role within the IT Services function, I have been at the coalface as regards the migration in 2015 away from a traditional, document heave waterfall approach toward the use of Agile Methods & Techniques. This had begun considering the use of User Stories as a means for documenting and prioritising requirements, and soon moved into a Scrum like process being adopted by the team. The adoption of Agility by the team brought about a marked change in the quality, consistency and speed of production. It therefore was assumed that additional use of Agile Methods and Techniques within both the Systems/Development team and wider IT Services function would result in the same deep embracing and success.

Whilst the majority of Techniques which were deployed produced high quality output, and benefit to the organisation I was concerned to see that the Abuser Story concept did not fare as well during the initial experimentation. My background research had highlighted this as a growing approach [74], [86], [91]. The reasons for the poor uptake can be seen in the previous discussion section. Pleasingly however, post project the team have begun to adopt this Technique across projects, specifically to highlight security implications where they do not naturally fit as constraints within a traditional User Story.

Conversely, all of the Techniques which resulted in the production of diagrams were quickly adopted by the team. What transpired here is likely as a result of individual colleagues preferred learning and communication styles, though more research would be needed to confirm this assumption.

In recent years we have seen Agile escape from software development and begin to shape the wider business community [51], [129]. Further to the success of this study, the recent publication of a number of papers and guides encouraging the use of Agile practices across all areas of IT Service Management [130], [131] is also of note. In its fourth incarnation, the ITIL [132] best practice framework now makes heavy reference to utilising Agile techniques and implementing processes only as far as is necessary [130]. As of yet, the Information Security frameworks however have not formally adopted Agile approaches, but with that said there are a number of Agile organisations who have achieved ISO Certification [133], [134].

Value of Research & Findings

Completing this project using empirical methods has resulted in findings which should be of interest to IT Practitioners within Further Education and beyond. Additionally as had been expressed by scholars previously [84] this empirical research may be of use to the academic community too.

The College's culture is such that feedback loops, including surveys feature across all processes and thus the use of a survey prior to the project and following each cycle was felt most appropriate to gather feedback from colleagues. This was combined with simple observational note taking and the combination has resulted in statistical data, and meaningful insight alike. Suggestion had been made regarding the use of interviews to gather feedback and data however in the neuro-diverse IT Services function (Overall approx. 75% Neurotypical) this was a technique I wished to avoid.

Project Management & Completion

Given that the project experimented with and implemented a number of Agile Techniques and Methods, it was felt appropriate to also keep with the Agile theme as far as project management.

The original brief required the inclusion of a Gantt chart to track the elements of the project, however it's widely accepted in the Agile community that though these can be used as a high level tool, they rarely turn out to be accurate [129]. Instead a high level overview consisting

of four planned work sprints, with a foundation sprint was created (Appendix 7 - Project Management).

The teams Jira tool was invaluable for documenting and prioritising individual project tasks, prioritising and progressing them via the use of a Kanban [86] board (Appendix 7 - Project Management). These techniques both gave a large degree of visibility [86], [93], [130], so that I could inspect my progress, and also allowed for re-prioritisation and reordering of items as work progressed.

13 Conclusion

This study set out to explore two research questions:

RQ1. Are Abuse Cases and Abuser Stories effective means of documenting Information Security Risk in a Software Project.

RQ2. Can Specific Agile Approaches succeed in aiding the prioritisation and treatment of Information Security Risk.

In essence, the study did just that, successfully exploring a number of Agile Techniques and Methods to approach Information Security within the College.

The literature review revealed opinion pointing toward a need for more empirical research in this area [84]. The findings of this study showed that there is promise in the application of a number of Agile Methods & Techniques, however also brought about a number of questions and concerns. With that in mind, it's clear that further research would in fact be of benefit to the sector, wider Information Security community and academia.

References

[1] R. B. Kvavik and J. Voloudakis, *Information technology security: Governance, strategy, and practice in higher education*. Educause, 2003.

[2] J. Chapman, "How safe is your data? Cyber-security in higher education," p. 6, 2019.

[3] R. Klahr, "Cyber security breaches survey," University of Portsmouth, 2016.

[4] HM Government, "Cyber Essentials - About," *Cyber Essentials*, 16-Oct-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/about. [Accessed: 17-Dec-2017].

[5] "Government mandates new cyber security standard for suppliers - GOV.UK." [Online]. Available: https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers. [Accessed: 08-Dec-2017].

[6] S. A. H. Scottish Government, "A Cyber Resilience Strategy for Scotland: Public Sector Action Plan, 2017/18," 08-Nov-2017. [Online]. Available: http://www.gov.scot/Publications/2017/11/6231. [Accessed: 08-Dec-2017].

[7] "Cyber Resilience - Update - a Freedom of Information request to Scottish Government," *WhatDoTheyKnow*, 20-Mar-2019. [Online]. Available: https://www.whatdotheyknow.com/request/cyber_resilience_update. [Accessed: 23-Apr-2019].

[8] European Parliament, *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, vol. 27. 2016.

[9] "Enforcement action," 10-Sep-2018. [Online]. Available: https://icoumbraco.azurewebsites.net/action-weve-taken/enforcement/. [Accessed: 20-Mar-2019].

[10] HM Government, "Businesses and charities urged to take action to prevent cyber attacks," *GOV.UK*, Mar-2019. [Online]. Available: https://www.gov.uk/government/news/businesses-and-charities-urged-to-take-action-to-prevent-cyber-attacks. [Accessed: 04-Apr-2019].

[11] J. Chapman, J. Francis, and L. Harre, "Cyber Security Posture Survey 2018 Research Findings," p. 37, Jul. 2018.

[12] Information Commissioners Office, "Information Risk Review - Higher Education." 2019.

[13] ISO/IEC, *ISO/IEC 27001*. Switzerland, 2013.

[14] "44 U.S. Code § 3542 - Definitions," *LII / Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/uscode/text/44/3542. [Accessed: 08-Sep-2018].

[15] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress, 2014.

[16] HM Government, "Ten Steps to Cyber Security." 2015.

[17] "GCHQ relaunches '10 Steps to Cyber Security' Guide for end user organisations," *Risk UK*, 21-Jan-2015. .

[18] J. M. Such, J. Vidler, T. Seabrook, and A. Rashid, *Cyber security controls effectiveness: a qualitative assessment of cyber essentials*. Lancaster University, 2015.

[19] "[Withdrawn] 10 Steps: Summary - GOV.UK." [Online]. Available: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary. [Accessed: 17-Dec-2017].

[20] C. D. Heitzenrater and A. C. Simpson, "Policy, statistics and questions: Reflections on UK cyber security disclosures," *J Cyber Secur*, vol. 2, no. 1, pp. 43–56, Dec. 2016.

[21] "National Cyber Security Strategy 2016 to 2021," *GOV.UK*. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. [Accessed: 20-Mar-2019].

[22] HM Government, "Cyber Essentials - Three Steps to Certification," *Cyber Essentials*, 27-Sep-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/getting-certified/. [Accessed: 17-Dec-2017].

[23] R. Henson and J. Garfield, "What Business Environment Changes Are Needed to Cause SME's to Take a Strategic Approach to Information Security?," 2015.

[24] A. Rison, "13 effective security controls for ISO 27001 compliance," 2016. [Online]. Available: https://azure.microsoft.com/en-gb/blog/13-effective-security-controls-for-iso-27001-compliance/. [Accessed: 17-Dec-2017].

[25] R. Sheikhpour and N. Modiri, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management," *Indian Journal of Science and Technology*, vol. 5, no. 2, pp. 2170–2176, 2012.

[26] J. Clinch, "ITIL and information security," *Best Management Practice*, 2009.

[27] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of Security Threats in Information Systems," *Procedia Computer Science*, vol. 32, pp. 489–496, Jan. 2014.

[28] J. J. Cebula and L. R. Young, *A Taxonomy of Operational Cyber Security Risks*. 2010.

[29] M. Howard and S. Lipner, *The security development lifecycle*, vol. 8. Microsoft Press Redmond, 2006.

[30] "Black hat," *Wikipedia*. 10-Oct-2018.

[31] "Grey hat," *Wikipedia*. 05-Sep-2018.

[32] R. J. Sciglimpaglia Jr, "Computer Hacking: A Global Offense," *Pace International Law Review*, vol. 3, no. 1, p. 199, 1991.

[33] "LulzSec," *Wikipedia*. 08-Sep-2018.

[34] C. C. Palmer, "Ethical hacking," *IBM Systems Journal*, vol. 40, no. 3, pp. 769–780, 2001.

[35] "White hat (computer security)," *Wikipedia*. 02-Oct-2018.

[36] "Ryan Ackroyd," *Wikipedia*. 05-Sep-2018.

[37] R. Sabillon, J. Cano, V. Cavaller, and J. Serra, "Cybercrime and cybercriminals: a comprehensive study," *International journal of computer networks and communications security*, vol. 4, no. 6, p. 165, 2016.

[38] T. Caldwell, "Ethical hackers: putting on the white hat," *Network Security*, vol. 2011, no. 7, pp. 10–13, 2011.

[39] "White Hat to Black Hat: What Motivates the Switch to Cybercrime," *Dark Reading*. [Online]. Available: https://www.darkreading.com/threat-intelligence/white-hat-to-black-hat-what-motivates-the-switch-to-cybercrime/d/d-id/1332521. [Accessed: 10-Oct-2018].

[40] K. Beck *et al.*, "Manifesto for Agile Software Development," 2001.

[41] W. Royce, "The software lifecycle model (Waterfall Model)," in *Proc. WESTCON*, 1970.

[42] T. Nicolaysen, R. Sassoon, M. B. Line, and M. G. Jaatun, "Agile Software Development: The Straight and Narrow Path to Secure Software?," *International Journal of Secure Software Engineering*, vol. 1, no. 3, pp. 71–85, Jul. 2010.

[43] R. Hoda, N. Salleh, and J. Grundy, "The Rise and Evolution of Agile Software Development," *IEEE Software*, vol. 35, no. 5, pp. 58–63, Sep. 2018.

[44] "13th Annual State of Agile Survey | The Largest, Longest-Running Agile Survey," *CollabNet VersionOne*. [Online]. Available: http://stateofagile.versionone.com/. [Accessed: 16-Mar-2019].

[45] K. Schwaber and J. Sutherland, "The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game.," *Scrum Alliance*, vol. 21, 2011.

[46] K. Beck, *Extreme programming explained: embrace change*. addison-wesley professional, 2000.

[47] Agile Business Consortium, "The DSDM Agile Project Framework (2014 Onwards)," *Agile Business Consortium*, 09-Nov-2015. [Online]. Available: https://www.agilebusiness.org/content/people-teams-and-interactions. [Accessed: 06-Aug-2017].

[48] K. Karu, K. Ferris, L. Hunebeck, B. Rae, and S. Rance, "ITIL Practitioner," *The Stationery Office*, 2016.

[49] A. Craddock, B. Roberts, K. Richards, J. Godwin, and D. Tudor, "The DSDM agile project framework for scrum," *Dynamic Systems Development Method (DSDM) Consortium*, 2012.

[50] P. Link and M. Lewrick, "AGILE METHODS IN A NEW AREA OF INNOVATION MANAGEMENT," p. 18.

[51] "Business Agility," *Agile Business Consortium*, 23-Jun-2017. [Online]. Available: https://www.agilebusiness.org/business-agility. [Accessed: 18-Mar-2019].

[52] Agile Business Consortium, "The 9 Principles of Agile Leadership." 2017.

[53] J. Stapleton, *DSDM, dynamic systems development method: the method in practice*. Cambridge University Press, 1997.

[54] P. Checkland and J. Scholes, "Soft systems methodology in action," *New York (US): John Wiley & Sons*, 1990.

[55] D. Bustard and F. Keenan, "Soft systems methodology: An aid to agile development?," in *Information Systems Development*, Springer, 2009, pp. 25–38.

[56] P. Checkland, "Soft Systems Methodology: a thirty year retrospective," in *Systems Research and Behavioral Science*, 1999, pp. 11–58.

[57] A. J. Dix, J. Finlay, R. Beale, and G. Abowd, *Human-computer interaction*. Pearson Education UK, 2004.

[58] A. Cooper, "The Inmates Are Running the Asylum: Why High-Tech Products Drive Us Crazy and How to Restore the Sanity," *SAMS. ISBN: 0-67231-649-8*, 1999.

[59] A. L. Massanari, "Designing for imaginary friends: information architecture, personas and the politics of user-centered design," *new media & society*, vol. 12, no. 3, pp. 401–416, 2010.

[60] A. Cooper, "The origin of personas | Cooper," 2008. [Online]. Available: http://www.cooper.com/journal/2008/5/the_origin_of_personas. [Accessed: 12-Nov-2017].

[61] L. Penelon, "How to create the perfect User Personas in 3 Steps?," *MVP Workshop*, 19-Sep-2017. .

[62] "Persona-centred information security awareness." [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S0167404817301566?token=619F9429081C5F3102A3D29E16D704EF9D7D0E028B28C2CBA503F9C90D6A336614D269541E6461FD0ED09A69BB164C90. [Accessed: 02-Feb-2019].

[63] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Flechais, "Here's Johnny: A Methodology for Developing Attacker Personas," in *2011 Sixth International Conference on Availability, Reliability and Security*, Vienna, Austria, 2011, pp. 722–727.

[64] C. Moeckel, "From user-centred design to security: building attacker personas for digital banking," in *Proceedings of the 10th Nordic Conference on Human-Computer Interaction - NordiCHI '18*, Oslo, Norway, 2018, pp. 892–897.

[65] S. W. Ambler, *The object primer: Agile model-driven development with UML 2.0*. Cambridge University Press, 2004.

[66] J. McDermott and C. Fox, "Using abuse case models for security requirements," *Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC).*, vol. IEEE Computer Society Press., 1999.

[67] G. Sindre and A. L. Opdahl, "Eliciting security requirements by misuse cases," in *Proceedings 37th International Conference on Technology of Object-Oriented Languages and Systems. TOOLS-Pacific 2000*, 2000, pp. 120–131.

[68] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering*, vol. 10, no. 1, pp. 34–44, Jan. 2005.

[69] M. Cohn, *User stories applied: For agile software development*. Addison-Wesley Professional, 2004.

[70] G. Lucassen, F. Dalpiaz, J. M. E. M. van der Werf, and S. Brinkkemper, "The Use and Effectiveness of User Stories in Practice," in *Requirements Engineering: Foundation for Software Quality*, 2016, pp. 205–222.

[71] R. Jeffries, "Essential XP: Card, conversation, confirmation," *XP Magazine*, vol. 30, 2001.

[72] B. Wake, "INVEST in good stories, and SMART tasks," *Retrieved December*, vol. 13, p. 2011, 2003.

[73] J. R. Fitzer, *Agile Information Security: Using Scrum to Survive in and Secure a Rapidly Changing Environment*. BookBaby, 2015.

[74] J. Peeters, "Agile security requirements engineering," in *Symposium on Requirements Engineering for Information Security*, 2005.

[75] V. Asthana, I. Tarandach, N. ODonoghue, B. Sullivan, and M. Saario, "Practical security stories and security tasks for agile development environments," *Online, July*, 2012.

[76] "Agile Software Development: Don't Forget EVIL User Stories - OWASP." [Online]. Available: https://www.owasp.org/index.php/Agile_Software_Development:_Don%27t_Forget_EVIL_User_Stories. [Accessed: 04-Oct-2018].

[77] P. Kamthan and N. Shahmir, "A Characterization of Negative User Stories.," in *SEKE*, 2016, pp. 579–582.

[78] J. Neher, "Abuser Stories: Thinking Like the Bad Guy to Reduce Security Vulnerabilities," in *Presented, Emerging Applications of Agile, Workshop Conference: Agile http://conferences. agilealliance. org/sessions/13318# sthash. EWKMZECN. dpuf.[Accessed on 12/06/2014]*, 2012.

[79] F. Paetsch, A. Eberlein, and F. Maurer, "Requirements engineering and agile software development," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on*, 2003, pp. 308–313.

[80] E. Bjarnason, K. Wnuk, and B. Regnell, "A case study on benefits and side-effects of agile practices in large-scale requirements engineering," in *Proceedings of the 1st Workshop on Agile Requirements Engineering*, 2011, p. 3.

[81] I. Inayat, S. S. Salim, S. Marczak, M. Daneva, and S. Shamshirband, "A systematic literature review on agile requirements engineering practices and challenges," *Computers in human behavior*, vol. 51, pp. 915–929, 2015.

[82] E.-M. Schön, J. Thomaschewski, and M. J. Escalona, "Agile Requirements Engineering: A systematic literature review," *Computer Standards & Interfaces*, vol. 49, pp. 79–91, 2017.

[83] P. Heck and A. Zaidman, "A systematic literature review on quality criteria for agile requirements specifications," *Software Quality Journal*, vol. 26, no. 1, pp. 127–160, 2018.

[84] H. Villamizar, M. Kalinowski, M. Viana, and D. M. Fernández, "A Systematic Mapping Study on Security in Agile Requirements Engineering," *arXiv:1806.01366 [cs]*, Jun. 2018.

[85] G. Boström, J. Wäyrynen, M. Bodén, K. Beznosov, and P. Kruchten, "Extending XP practices to support security requirements engineering," in *Proceedings of the 2006 international workshop on Software engineering for secure systems*, 2006, pp. 11–18.

[86] M. Alotaibi, "Modelling Security Requirements Through Extending Scrum Agile Development Framework," 2016.

[87] W. M. Farid, "The normap methodology: Lightweight engineering of non-functional requirements for agile processes," in *Software Engineering Conference (APSEC), 2012 19th Asia-Pacific*, 2012, vol. 1, pp. 322–325.

[88] J. Broad, *Risk management framework: a lab-based approach to securing information systems*. Newnes, 2013.

[89] D. Mougouei, N. F. M. Sani, and M. M. Almasi, "S-Scrum a Secure Methodology for Agile Development of Web Services," p. 5, 2013.

[90] A. S. Sonia and J. Balwani, "Analysing Security and Software Requirements using Multi-Layered Iterative Model," 2014.

[91] J. Peeters and P. Dyson, "Cost-effective security," *IEEE Security & Privacy*, no. 3, pp. 85–87, 2007.

[92] A. Singhal and H. Banati, "Fuzzy logic approach for threat prioritization in agile security framework using DREAD model," *arXiv preprint arXiv:1312.6836*, 2013.

[93] O. Sandén, *Threat Management in Agile Organisations: Using the Results of a Threat Analysis in Agile Software Development*. 2018.

[94] I. A. Tondel, M. G. Jaatun, and P. H. Meland, "Security requirements for the rest of us: A survey," *IEEE software*, vol. 25, no. 1, 2008.

[95] M. Howard and D. LeBlanc, "Writing Secure Code," p. 732.

[96] S. Bartsch, K. Sohr, and C. Bormann, "Supporting Agile Development of Authorization Rules for SME Applications," in *Collaborative Computing: Networking, Applications and Worksharing*, 2009, pp. 461–471.

[97] V. N. Franqueira, Z. Bakalova, T. T. Tun, and M. Daneva, "Towards agile security risk management in RE and beyond.," in *EmpiRE*, 2011, pp. 33–36.

[98] M. G. Jaatun, J. Jensen, P. H. akon Meland, and I. A. Tøndel, "A Lightweight Approach to Secure Software Engineering," in *A Multidisciplinary Introduction to Information Security*, Chapman and Hall/CRC, 2011, pp. 209–242.

[99] C. Ebert, "Success Factors for Security Engineering," 2015.

[100] S. W. Ambler, "Agile model driven development is good enough," *IEEE Software*, vol. 20, no. 5, pp. 71–73, Sep. 2003.

[101] R. L. Baskerville and A. T. Wood-Harper, "A critical perspective on action research as a method for information systems research," *Journal of information Technology*, vol. 11, no. 3, pp. 235–246, 1996.

[102] D. E. Avison, F. Lau, M. D. Myers, and P. A. Nielsen, "Action research," *Communications of the ACM*, vol. 42, no. 1, pp. 94–97, Jan. 1999.

[103] J. McNiff, *All you need to know about action research*. London: SAGE, 2006.

[104] "Vulnerability assessment and information service," *Jisc*. [Online]. Available: https://www.jisc.ac.uk/vulnerability-assessment-and-information-service. [Accessed: 21-Jan-2019].

[105] A. Harding and D. Sharrock, "Information Security Policy." 2018.

[106] Atlassian, "Atlassian | Software Development and Collaboration Tools," *Atlassian*, 2017. [Online]. Available: https://www.atlassian.com. [Accessed: 06-Aug-2017].

[107] D. S. Burge, "The Systems Thinking Tool Box," p. 5, 2015.

[108] T. Dyba and T. Dingsøyr, "Empirical studies of agile software development: A systematic review," *Information and software technology*, vol. 50, no. 9, pp. 833–859, 2008.

[109] L. Barroca, H. Sharp, D. Salah, K. Taylor, and P. Gregory, "Bridging the gap between research and agile practice: an evolutionary model," *International Journal of System Assurance Engineering and Management*, vol. 9, no. 2, pp. 323–334, 2018.

[110] E. Weippl, S. Schrittwieser, and S. Rennert, "Empirical Research and Research Ethics in Information Security," in *International Conference on Information Systems Security and Privacy*, 2016, pp. 14–22.

[111] D. Dittrich and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," *CAIDA*, 2012. [Online]. Available: http://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/index.xml. [Accessed: 03-Feb-2019].

[112] A. Harding and J. C. Read, "A Study into the Adoption of, and Enthusiasm for Agile Development Methodologies Within Further Education.," *26th International Conference On Information Systems Development (ISD2017 Cyprus)*, 2017.

[113] R. Likert, "A technique for the measurement of attitudes," *Archives of psychology*, 1932.

[114] Association of Colleges, "Colleges in England as at 11 January 2019," Jan-2019. [Online]. Available: https://www.aoc.co.uk/sites/default/files/262%20colleges%20in%20England.pdf. [Accessed: 12-Jan-2019].

[115] J. E. Barlett, J. W. Kotrlik, and C. C. Higgins, "Organizational research: Determining appropriate sample size in survey research," *Information technology, learning, and performance journal*, vol. 19, no. 1, p. 43, 2001.

[116] H. B. Mann and D. R. Whitney, "On a test of whether one of two random variables is stochastically larger than the other," *The annals of mathematical statistics*, pp. 50–60, 1947.

[117] "(76) Creating Personas for Effective User Stories - YouTube." [Online]. Available: https://www.youtube.com/watch?v=tCAeHfvsjoM. [Accessed: 11-Mar-2019].

[118] M. Harris, *How to Develop the Habits of Outstanding Teaching: A practical guide for secondary teachers*. Routledge, 2016.

[119] SolutionsIQ, *Abuser Stories - Think Like the Bad Guy with Judy Neher - at Agile 2015*. .

[120] J. Ivill, *Risk Management Policy*. Runshaw College.

[121] A. Moran, *Agile Risk Management and DSDM Pocketbook*. Agile Business Consortium.

[122] The Stationary Office, *ITIL*. TSO, 2008.

[123] A. Harding, *Information Security Risk Management and Assessment Policy*. Runshaw College.

[124] HM Government, *Keeping children safe in education*. Department for Education.

[125] "abuser, n.1," *OED Online*. Oxford University Press.

[126] K. A. Lindquist and M. Gendron, "What's in a Word? Language Constructs Emotion Perception," *Emotion Review*, vol. 5, no. 1, pp. 66–71, Jan. 2013.

[127] K. Rindell, S. Hyrynsalmi, and V. Leppänen, "Busting a myth: Review of agile security engineering methods," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, p. 74.

[128] J. Fook, S. White, and F. Gardner, "Critical reflection: a review of contemporary literature and understandings," p. 18.

[129] T. Streule, N. Miserini, O. Bartlomé, M. Klippel, and B. G. de Soto, "Implementation of Scrum in the Construction Industry," *Procedia Engineering*, vol. 164, pp. 269–276, 2016.

[130] Atlassian, "Atlassian's guide to agile ways of working with ITIL 4," *Atlassian*. [Online]. Available: https://www.atlassian.com/whitepapers/itil4. [Accessed: 12-Apr-2019].

[131] B. Verlaine, I. Jureta, and S. Faulkner, "How Can ITIL and Agile Project Management Coexist?," in *Exploring Services Science*, vol. 247, T. Borangiu, M. Dragoicea, and H. Nóvoa, Eds. Cham: Springer International Publishing, 2016, pp. 327–342.

[132] "ITIL® Foundation, ITIL 4 edition." [Online]. Available: https://www.tsoshop.co.uk/AXELOS-Global-Best-Practice/ITIL-4/?DI=650015. [Accessed: 12-Apr-2019].

[133] "The Surprising Combination of an ISO-Audit and our Agile Organisation," *Sievo*, 06-Jul-2017. [Online]. Available: https://sievo.com/blog/the-surprising-combination-of-an-iso-audit-and-our-agile-organisation. [Accessed: 12-Apr-2019].

[134] D. Hutchinson, C. Armitt, and D. Edward-Lear, "The application of an agile approach to it security risk management for SMES," *12th Australian Information Security Management Conference. Held on the 1-3 December*, vol. 2014 at Edith Cowan University, p. Western Australia.-, 2014.

Appendices

Appendix 1 – Email to JISC CMIS and UK Security Groups

From: Alex Harding
Sent: 19 November 2018 18:00
To: CMIS-NETWORK@JISCMAIL.AC.UK; 'uk-security@jiscmail.ac.uk'
Subject: FE Cyber Security Survey

Hi All,
First of all, my apologies for cross posting.

I wonder if I could ask you to take a few moments to complete a short survey about Cyber Security, specifically how it impacts the FE Sector and your organisations approaches. The survey should take no more than about five minutes to complete, and your responses will be invaluable to the research I'm completing as part of my Masters project. The survey doesn't require any personal data, however at the end it would be good if you could let me know your Role/Job Title.

I will share the results with the same lists used to send out the survey once the analysis is complete. Those with a keen eye may notice that some of the questions are aligned with those in the JISC Cyber Security Posture Survey and there's good reason for that 😆. JISC's results will be a good basis for comparison. Those of you in HE are more than welcome to have a look and complete too, however from the results of JISCs survey and discussions at the JISC Security Conference it does look like you're both more able to resource and are more pro-active than in FE.

The survey:
https://docs.google.com/forms/d/e/1FAIpQLSf-M5cy2gbRelWIQ4-XT8N1itTjvUh1HTmWR2m75G1Ax2Rceg/viewform

Thanks in advance.

Alex

Alex Harding
Alex Harding | IT Services & Print Shop Manager

01772 642037 (2257 / 2037) / harding.a@runshaw.ac.uk
IT Services, Runshaw College, Langdale Road, Leyland PR25 3DQ
Like us on Facebook | Follow us on Twitter | Visit our website

Appendix 2 – Survey Questions

Cyber Security in FE - Survey

Cyber Security in FE - Survey

Thank you for taking the time to complete this survey, your responses will form part of the data capture phase of my Masters project. My project concerns attitudes towards Information Security within the FE Sector, and is attempting to study the use of Agile techniques and tools to improve efforts to document Information Security risk.

Any personal details provided will be used solely to distribute the results of this survey and will be kept no longer than is necessary to carry out this function.

* Required

1. **Your Organisation** *
   Mark only one oval.
   - ◯ We are a Further Education Institution (e.g. Sixth Form College, Tertiary College)
   - ◯ We are a Higher Education Institution (e.g. University)
   - ◯ Other: _____

Staffing and Certifications

2. **Within your organisation is there a dedicated team/person that looks after Cyber Security?** *
   Mark only one oval.
   - ◯ There's a dedicated Role. (e.g Information Security Officer)
   - ◯ A Team carries out this role (e.g. Computer Security Response Team)
   - ◯ The role is formally part of another function (e.g. Network Team)
   - ◯ None of the above.

3. **Has your organisation completed any of the below:** *
   Mark only one oval per row.

	N/A - No Plans	Considering	Achieved
Cyber Essentials Certification	◯	◯	◯
Cyber Essentials Plus Certification	◯	◯	◯
ISO27001 Certification	◯	◯	◯

Policies & Risk Assessment

4. **Does your organisation have a specific Information Security/Cyber Security Policy?** *
   Mark only one oval.
   - ◯ Yes
   - ◯ No

https://docs.google.com/forms/d/1wA09XfUlbC1TPW4wIGuU1Lbl6rYYkG_UHtZeY8OEgsI/printform

Cyber Security in FE - Survey

5. **Has your organisation carried out an Information Security Risk Assessment?** *
Mark only one oval.

- ◯ Yes
- ◯ No

Importance of Cyber Security

To what level of importance does your organisation regard/place upon:

6. **Cyber Security** *
Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

7. **Cyber Security Training for Staff** *
Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

8. **Cyber Security Training for Students** *
Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

9. **Cyber Security Certifications** *
Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

10. **Information Security Risk Assessments** *
Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

https://docs.google.com/forms/d/1wA09XfUlbC1TPW4wlGuU1Lbl6rYYkG_UHtZeY8OEgsI/printform

Cyber Security in FE - Survey

11. **Regular Penetration Testing** *

Mark only one oval.

	1	2	3	4	5	
Not Important	◯	◯	◯	◯	◯	Vitally Important

Risks

To what extent do you feel that the following threats pose a risk to your organisation

12. **Lack of Awareness**

Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

13. **Insider Threats (Staff)**

Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

14. **Students (Malicious/Curious)**

Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

15. **Social Engineering & Phishing**

Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

16. **External Threats / Hackers**

Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

https://docs.google.com/forms/d/1wA09XfUlbC1TPW4wIGuU1Lbl6rYYkG_UHtZeY8OEgsI/printform

Cyber Security in FE - Survey

17. **Denial of Service / DDoS**
Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

18. **Malware / Virus**
Mark only one oval.

	1	2	3	4	5	
No Risk	◯	◯	◯	◯	◯	Imminent Risk

Agility

19. **My Organisation utilises Agile Methods & Techniques:** *
Mark only one oval.

	1	2	3	4	5	
Never	◯	◯	◯	◯	◯	Always

20. **My Organisations experience in using Agile Methods & Techniques:** *
Mark only one oval.

	1	2	3	4	5	
New/Non Existant	◯	◯	◯	◯	◯	Mature

21. **My Organisation would consider Agile Approaches to documenting Information Security Risk:** *
For example, utilising (negative) User Stories to document threats. Using techniques such as MoSCoW prioritisation to identify areas to provide mitigations for first.
Mark only one oval.

- ◯ Yes
- ◯ No

https://docs.google.com/forms/d/1wA09XfUlbC1TPW4wIGuU1Lbl6rYYkG_UHtZeY8OEgsI/printform

Appendix 3 – Email to Mike Cohn

Hi Mike,

As part of my Masters Thesis, I'm exploring the use of Abuser Stories, and experimenting with their use in a Scrum project. Part of my background reading has highlighted that you may have previous works in this area.

http://itsadeliverything.com/abuser-story-user-stories-to-prevent-hacking

I picked the above out from Stephen Thomas' blog, though as he suggests most of the literature points towards Peeters as the source of Abuser Stories. Are you able to confirm whether there's anything you may have published that I can read (or even unpublished)

Any help or pointers would be gratefully received!

Alex

MSc Agile Leadership

University of Central Lancashire / Runshaw College

Appendix 4 – Participation Statement

Participation Details

FE Agile/Cyber Security Research

Dear Colleague,

Throughout the Winter and Spring term, I will be completing a research project concentrating on the use of a number of Agile techniques in order to improve the speed and quality of Information Security Risk Analysis. This will be of benefit to all three IT Services teams, the Service Desk, IT Systems and IT Infrastructure.

During the project, alongside yourselves I will suggest and we will explore a number of techniques and I will need to make brief notes about our progress. I would also be grateful for your completion of a number of short surveys to gauge your feelings toward the proposed improvements. These notes and survey will be recorded in an anonymous fashion.

You are free to withdraw your participation at any stage throughout the project, and where required and possible your inputs and any data will be disregarded.

Should you have any queries or would like to discuss the project further please do not hesitate to make contact using the details below.

Kindest Regards

Alex

Alex Harding

Alex Harding | IT Services & Print Shop Manager

01772 642037 (2257 / 2037) **/** harding.a@runshaw.ac.uk
IT Services, Runshaw College, Langdale Road, Leyland PR25 3DQ

Appendix 5 – Team Survey

Security Analysis - Team Survey

Dear colleagues, as ever I thank you for your agreeing to participate in this project. I would be grateful if prior to starting work to improve our practice in the area of Information Security, and following each cycle for your completion of this survey.

The results will be utilised to track our progress, but not at an individual level.

*Required

1. **I am completing this survey following Cycle:**
   Mark only one oval.
   - ◯ 0 - Prior to any Cycles
   - ◯ 1 - Post Cycle 1
   - ◯ 2 - Post Cycle 2
   - ◯ 3 - Post Cycle 3

2. **My Team**
   Mark only one oval.
   - ◯ Service Desk
   - ◯ Infrastructure
   - ◯ Systems
   - ◯ Outside of IT

3. **Based upon current techniques (following the current cycle). I feel that:** *
   Mark only one oval per row.

	0 - Unknown / NA	1 - Strongly Disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
It is easy to Identify Security Requirements	◯	◯	◯	◯	◯	◯
It is easy to Prioritise Security Requirements	◯	◯	◯	◯	◯	◯
Security Requirements can be modelled easily	◯	◯	◯	◯	◯	◯
Agile tools are a effective for identifying, prioritising and modelling Security Requirements	◯	◯	◯	◯	◯	◯
My team are able to attend to Security Requirements.	◯	◯	◯	◯	◯	◯

4. **Any Comments (All Cycles & Pre Cycle)**

5. **What Went Well (Post Cycles Only)**

6. **Even Better If (Post Cycles Only)**

Powered by Google Forms

Appendix 6 – Facilitated Workshop Agendas

Appendix 6.1 – First Cycle, Rich Picture of High Level Threats Workshop

Workshop/Meeting Agenda	
Date/Time/Location	January 16th / 10:00-12:00 / M101
Attendees	Redacted (10 Attendees)
Objectives	• To explore the concept of Rich Pictures. • To create a Rich Picture looking at cyber threats.
Outputs (Intended)	• Rich Picture

Appendix 6.2 – First Cycle, Attacker Persona Workshop

Workshop/Meeting Agenda	
Date/Time/Location	January 17th / 10:00-12:00 / M101
Attendees	Redacted (10 Attendees)
Objectives	• Explore Personas and Attacker Personas
Outputs (Intended)	• A collection of Attacker Personas

Appendix 6.3 – Second Cycle, Abuse Case Workshop

 **Workshop/Meeting Agenda**	
Date/Time/Location	February 13th / 13:00-14:30 / R008
Attendees	Redacted (6 Attendees)
Objectives	• Recap on Use Cases • Paper on Abuse Cases • Review high level requirements for RunshawPay 2.0 Project • Create Abuse Case Diagram
Outputs (Intended)	• Abuse Case Diagram

Appendix 6.4 – Second Cycle, User Story Workshop

 **Workshop/Meeting Agenda**	
Date/Time/Location	February 14th / 09:00-10:30 / R008
Attendees	Redacted (6 Attendees)
Objectives	• Paper on Abuser Stories • Video on Abuser Stories • Review high level requirements for RunshawPay 2.0 Project • Review Abuse Case Diagram
Outputs (Intended)	• Abuser Stories

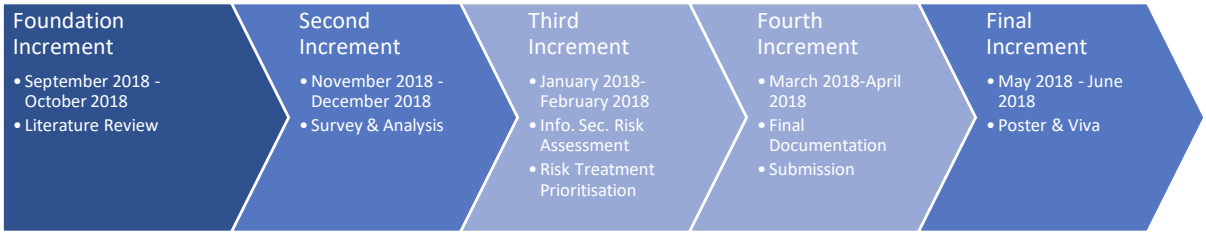
Appendix 6.4 – Third Cycle, Risk Day

Workshop/Meeting Agenda

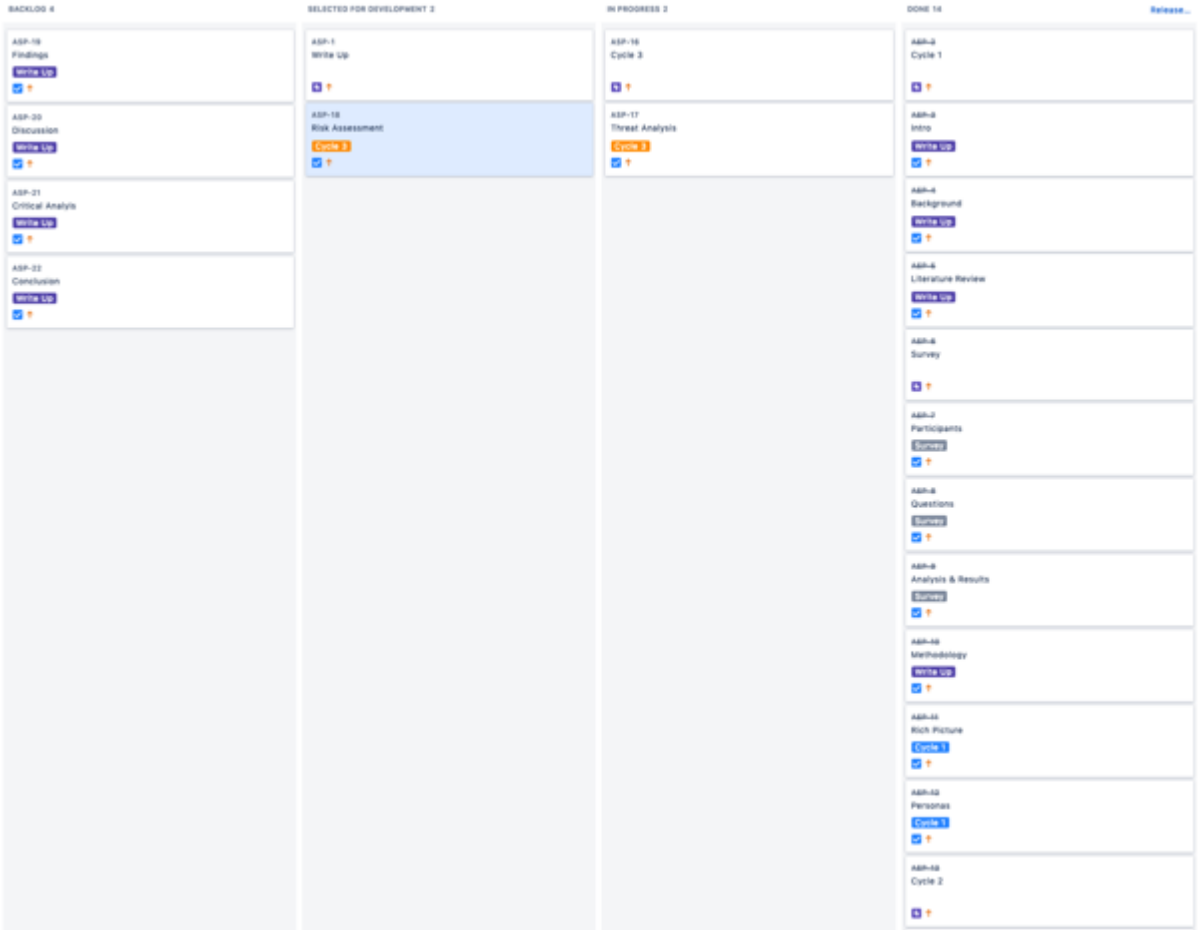
Date/Time/Location	March 14th / 08:30-16:00 / F103
Attendees	Redacted (4 Attendees)
Objectives	• Recap of High Level Threat Risk Picture • Review Information Security Risk Assessment Policy • Review CMDB & Services • Define Risk Template • Create Sample Risks • Create Sample Mitigations
Outputs (Intended)	• Complete Asset & Service Listing • Defined Risk Assessment/Analysis Template • Risks • Mitigations

Appendix 7 - Project Management

During the planning of the project, a high level Sprint plan had been defined, this consisted of a foundation increment, and four work increments that followed it.



In order to track activities, a Kanban Board was created in Jira in order to track work items. At the time of writing, 24 discrete activities exist within the project.



Appendix 8 – Data

AHProjectData.xlsx

1. Survey Responses
2. Literature Review Data
3. Rejected Survey Responses
4. Cycle Surveys Overview
    a. Pre Cycles
    b. Cycle 1
    c. Cycle 2
    d. Cycle 3
5. Incident Stats
6. Scottish Government FOI Data