National College of Ireland

Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme

MSc Research Project
MSc in Cybersecurity

Khalimatou Samirah
Student ID: x18102263

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: …Khalimatou Samirah……

Student ID: …x18102263……

Programme: …MSc in Cybersecurity…… **Year:** …2021……

Module: …Internship……

Supervisor: …Vikas Sahni……

Submission Due Date: …06 Sept 2021……

Project Title: Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme

Word Count: ……6750…… **Page Count**……20……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

Signature: ……Khalimatou Samirah……

Date: ……06th August 2021……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme

Khalimatou Samirah
x18102263

Abstract

The increase of cybercrime has raised trust concerns in ICT products and services in the industry at national and international levels. To address these concerns, the European Commission has adopted the Cybersecurity Act 2019 that defines the European cybersecurity certification framework and lays out a base of requirements for cybersecurity certification of ICT products, services, and processes. As part of this framework the European Agency for Cybersecurity, ENISA develops cybersecurity certification schemes upon request from the European Commission such as the European Cloud Services (EUCS) scheme. The European Commission has provided funding supports under the Connecting Europe Facility (CEF) Telecom Work Programme to facilitate a series of projects to build cybersecurity certification capabilities in European member countries. Involved in one of these projects, the National Standards Authority of Ireland (NSAI) must take part in building capabilities for EUCS scheme certification and conduct pilot certifications for Cloud Services Providers (CSPs) in Ireland. To efficiently achieve this goal, it is important to understand the readiness of CSPs concerning the EUCS scheme requirements. The contributions of this research include complementing an existing Cloud Security Readiness (CSR) model with EUCS scheme requirements, developing a questionnaire to assess the readiness of CSPs to take part in the EUCS scheme certification and an evaluation to confirm the efficiency of the solution. The results show the sample of CSPs that participated in the research, satisfy more than 75% of the requirements of the EUCS scheme.

1 Introduction

Cybercrime has always been an issue for organisations and states security. However, since the pandemic there has been a significant increase in cyberattacks in Ireland[1] and globally. Colleges and national services have been impacted by highly disruptive cyberattacks early this year. In 2021, a ransomware attack disrupted for weeks, the operations of the National College of Ireland[2] (NCI) and the Health Services[3] (HSE). The Federal Bureau of Investigation (FBI) reports cybercrime increase of 300% since the pandemic started[4]. Also, cyberattacks are not

[1] shorturl.at/tJKU6

[2] https://www.thejournal.ie/tu-dublin-ransomware-attack-ongoing-5403034-Apr2021/

[3] https://www.thejournal.ie/hse-cyber-attack-ransonware-started-5443370-May2021/

[4] https://www.varonis.com/blog/cybersecurity-statistics/

limited by state borders. As such, a cyberattack can impact multiple countries[5]. These attacks impact organisations and countries from a financial, operational, and even procurement perspective. Global losses from cybercrime total over $1 trillion in 2020[6] and is expected to increase significantly in the coming years unless appropriate safeguards are put in place.
Governments around the world are responding to the issue and within the European Union (EU), the EU Cybersecurity Act came into force in 2019, laying out a base of requirements for cybersecurity certifications of ICT products, services, and processes. The Cybersecurity Act also strengthen the role of the European Network and Information Security Agency (ENISA[7]) that issues certification schemes in line with the regulation, towards a cybersecurity certification framework. The cybersecurity certification process as defined in the Cybersecurity Act involves multiple stakeholders as depicted in Figure 1 below.

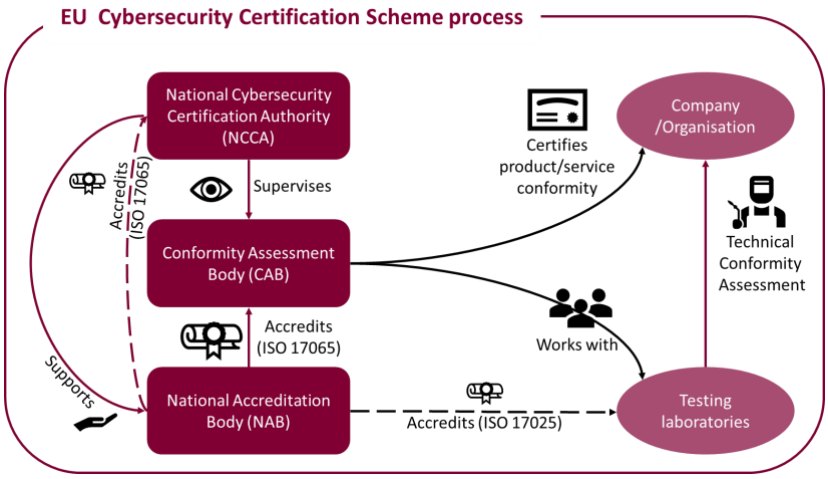


Figure 1: EU Cybersecurity Certification Process

The stakeholders involved in the EU Cybersecurity certification process include at the national level a National Cybersecurity Certification Authority (NCCA), a National Accreditation Body (NAB), Conformity Assessment Bodies (CAB), testing laboratories and vendors. ENISA will provide governance at the EU level. As part of the EU Cybersecurity Certification Framework, the EU commission is funding a series of projects to build capabilities for cybersecurity certifications in EU member countries. One of these projects is the *A4CEF - Advancing Cybersecurity Certification Capabilities with Cross-border exchange and Enhancing (business) Flows*[8]. This project involves stakeholders from France, Cyprus, and Ireland. The National Standards Authority of Ireland (NSAI) is involved as a Conformity Assessment Body (CAB), in the process of establishing a Cybersecurity Certification Ecosystem for the cybersecurity certification of cloud services in Ireland, based on the EU cloud services (EUCS) scheme.

[5] shorturl.at/gipEZ
[6] https://bit.ly/3fz7rf3
[7] https://www.enisa.europa.eu/
[8] https://www.a4cef.eu/

The process involves building capabilities for the EUCS scheme certification and performing several pilot certifications for Cloud products and services in Ireland. As the Cybersecurity Act and the EUCS scheme are new in the industry, likely, CSPs are not aware of it. To minimize cost and time during the pilot certifications, it is important to raise awareness amongst CSPs about the new cybersecurity certification scheme.
The EC has indicated that Cybersecurity Schemes will be mandated for certain products and services before the end of 2023. Furthermore, according to the new rules, product and service vendors in the EU will be required to certify their services a single time before placing them on the European market. It is also important for authorities involved in the process of cybersecurity certification to understand the readiness status of the industry with regards to the new certification scheme, to inform their communication and engagement strategies efficiently, minimising certification cost and time. This raises the following questions:

- How to measure the readiness of CSPs with regards to the EUCS scheme certification?
- What is the posture of CSPs in Ireland with regards to the EUCS requirements?

While there are multiple definitions of readiness level, in this context, readiness level refers to the maturity level to which CSPs meet the requirements of the EUCS scheme. To address the aforementioned questions, research was conducted to determine the readiness of CSPs in Ireland for EUCS Scheme certification. This study complements an existing model that assesses the readiness of CSPs individually with the EUCS scheme requirements and extends the assessment to address the readiness of CSPs collectively.
The participation of CSPs in this research has exposed them to the EUCS scheme requirements, provided their EUCS readiness level and recommendations on how to improve their security posture. It has also allowed them to identify potential security gaps in existing products and services, informed the development of future products and services portfolios in line with future regulation and increased the probability of getting successfully certified the first time when the mandates about products and services come into force in the coming years.
The results of this research will allow cybersecurity certification bodies to understand the posture of CSPs in Ireland and inform communication and engagement strategies with them. Furthermore, the artefact produced as part of this research will be useful to other EU member states that are or will be involved in determining the industry readiness for EUCS scheme certification in their respective countries.
The dissertation is structured as follows; Section 2 looks at related work on the definition of readiness and associated frameworks, Section 3 outlines the steps followed in the research methodology, Section 4 details the techniques and frameworks included in the design specification, Section 5 describes the implementation of the proposed solution and Section 6 presents the results of the evaluation. In Section 7, a summary of the findings and presentation of the limitations of this research are available in addition to possible avenues for future research.

2 Related Work

There have been several peer-reviewed works on readiness assessment published in the last decade. While there is a lack of specific work with regards to assessing the readiness of an

industry sector to undertake a certain certification, the literature review focused on readiness assessment and compliance readiness frameworks/models for information systems. This literature review provided an understanding of the state of the art in assessing the readiness of organisations.

Researchers have developed readiness assessments frameworks and models based on a set of domains that encompass the requirements against which organisations are assessed. Certain researchers reviewed previous literature to understand the factors affecting the readiness of organisations in their sector of the industry. These factors were then used as domains in their framework to assess the readiness of organisations. In other published works, researchers have based their models on previous frameworks and aligned their proposed frameworks current environments and standards.

2.1 Literature-based domains/factors

Several researchers extracted the factors that influence the readiness of organisations against a set of requirements from their literature review. For example, Cheang developed a model to assess the cybersecurity readiness of public organisations by providing a security index at the national level. Measured with factors such as Human resources, Infrastructure, and Environment, this model aims to inform policymakers on the security issues in the industry. With this knowledge, appropriate best practices and policies can be developed and implemented (Cheang, 2009).

Nisreen et al. developed a model to assess the security of Bring Your Own Device (BYOD) at work as it poses a serious risk to the data of organisations. The model is based on theories developed around BYOD security in the workplace and result in several domains involving the behavioural factors of employees that are usually omitted in national and international security standards (Nisreen Ameen, 2021).

Straub established a cybersecurity readiness level model to assess the security level of cybersecurity systems. This model is based on Technology Readiness Levels used in the USA and the EU for other systems. The level to which cybersecurity systems are evaluated depending on the risk associated with regards to its criticality and the impact of systems being compromised (Straub, 2021).

The model presented by Babkin et al. is in line with SMART education, to assess the readiness of universities to move to a new educational model. The model is based on factors of the fourth industrial revolution and others such as innovation, environment, and Internet technologies (Babkin Alexandr V., 2018).

Esa performed a quantitative study aimed to assess the readiness of organisations with regards to the implementation of an Information Security Management System (Esa, 2019).

Barclay et al. presented a cybersecurity maturity model to inform organisations on their security posture. The model covers a wider scope of organisational factors than the previous cybersecurity maturity models it is based on (Barclay, 2014).

Heru et al. developed a framework to assess information security compliance based on six domains/factors. The authors used this framework to assess the readiness level for multimedia information security compliance (Heru Susanto, 2012).

The readiness assessment model proposed by Husam and Tugrul is based on previous literature results to inform organisations on their posture with regards to carrying out big data projects (Husam Barham, 2020).

Some researchers have developed automated alternatives of assessment. For example, Syed et al. created a system to evaluate the security readiness of CSPs from the cloud service user (CSU) perspective. The model aims to allow users to make informed decisions with regards to their migration to the cloud and help them understand which CSP has appropriate security safeguards (Syed Rizvi, 2020).

Multiple researchers have developed models based on the Technology Organisation Environment (TOE) framework. Shaikha et al. cybersecurity readiness model is aligned with the TOE Framework. This model is based on the factors that affect the posture of organisations concerning cybersecurity. The factors used in this study have been gathered from previous work on the factors affecting cybersecurity readiness for organisations. The TOE framework has been widely discussed in research and is suitable for assessing the readiness of organisations against specific requirements. It has been used in line with multiple factors, frameworks, and standards. (Shaikha Hasan, 2021).

Fasil Alemeye developed a framework to assess the readiness of IaaS and SaaSCSPs. The framework provides as a result which cloud model is appropriate for the migration of an organisations (business operations?) to the cloud. This framework is based on the TOE framework, the Technology Acceptance Model (TAM) and Diffusion of Innovations (DOI) theory (Fasil Alemeye, 2015).

A variety of studies focused on the Internet of Things (IoT) and cloud systems. Nurul Huda et al. presented a framework to assess the readiness of organisations with regards to IoT forensic investigations. The literature review provided information on the factors based on theories used to develop the model behind the framework to associate organisations with a level of readiness (Nurul Huda Nik Zulkipli, 2021).

Ahmed et al. developed a model to assess the forensic readiness of CSPs. The factors of the model are based on literature including technological, legal, and organisational factors (Ahmed Alenezi, 2020).

Umar and Shareeful established a framework to assess the transparency of CSPs from a cloud service customer's (CSC) perspective. Additionally, they propose a tool that assesses evidence gathered from CSPs and issues a conformity score with regards to transparency. To reach this goal the framework requires organisations to go through a set of activities including the definition of requirements specific to their operations, assets, stakeholders, and risk management (Umar Mukhtar Ismail, 2020).

David et Solange assessed the attitude of organisations towards cloud computing based on a survey they developed (David Simms, 2013). Mpho Percy et al. developed a framework to assess the digital forensic readiness of CSPs. The framework development is based on literature and observations of organisations processes including the social behaviours of employees. This framework aims to help organisations in assessing the risks of selecting a CSP for their migration to the cloud. It might also be useful for CSPs to assess their posture with regards to digital forensics, to improve their overall security posture (Mpho Percy Makutsoane, 2014).

Ali developed a model to assess the cybersecurity readiness of organisations based on employee's cybersecurity readiness to respond to cybersecurity threats and attacks. The

framework was developed based on factors influencing cybersecurity readiness in organisations found in literature and a survey response from employees. The results confirm that employee's readiness contributes significantly to the overall cybersecurity readiness of organisations (AlEnezi, 2020).

2.2 Frameworks-based and standards-based domains/factors

Several works based on popular frameworks and international standards have also been published. For example, Sara N. et al. proposed a risk-based automated approach to assess the security level for IoT products. This approach is based on popular international standards and other technologies and approaches suitable for IoT products (Sara N. Matheu-García, 2019).

Valentina et al. focused on ensuring the security of cloud-based applications in their design phase. Several gaps were identified with regards to the state of the art in producing secure cloud-based applications that are time and resource consuming. Their semi-automated security-by-design methodology based on the National Institute of Standards and Technology (NIST) Controls Framework SP-800-53 (Technology, 2020), allowed non-security professionals to assess their cloud-based applications and identify the security gaps in the early stages of their development (Valentina Casola, 2021).

Jamal et al. developed a framework to evaluate the security posture of governmental organisations based on local and international standards. With this framework they called GoSafe, they provide tools that allow organisations to engage in self-assessment of their security program against standards and regulatory requirements that are applicable. This framework might also be used by non-governmental organisations that are interested in improving their overall security posture. However, it might not be useful in this case, as it deals with published and well-established standards that organisations are familiar with (Jamal N. Al-Karakia, 2020).

Aristeidis et al. provided a tool to assess the readiness of small and medium-enterprises (SME)s to partake in GDPR certification. The tool covers the GDPR requirements and provides scores based on the implementation of these requirements by the organisation. This can be useful in assessing the readiness of CSPs against the EUCS. However, the scheme is not complete yet and is still under review. As such, critical information such as guidance is not available at the time of writing. (Aristeidis Chatzipoulidis, 2019).

Sugandh and Jyoteesh developed a readiness model to assess CSPs with regards to several factors affecting the security of cloud services, identified in the literature review phase. This model aims to help organisations in assessing the risks related to their migration to the cloud. It is based on the hexagonal information security framework factors and two additional factors identified by the authors during the literature review. Knowing their security posture with regards to state-of-the-art security considerations at the time of writing, organisations can securely plan their migration to the cloud (Sugandh Bhatia, 2018).

Muhammad and Vito assessed the effectiveness of the international standard for information security ISO 27001 (ISO/IEC, 2013) for CSP categories: in house, IaaS, PaaS, and SaaS. They argue that while this standard is a good base for CSP security, it does not cover all aspects of their organisation and cannot guarantee a secure environment for their business operations (Muhammad Imran Tariq, 2016).

Several methodologies aligned the TOE framework with popular international standards. Hans et al. used the TOE framework to understand the factors affecting the adoption of cloud services in the industry (Hans P. Borgman, 2013).

Nur Ilyani et al. developed a Cloud Security Readiness (CSR) model based on two frameworks. The TOE and the six-layer framework. The TOE framework is generally used to examine technological and environmental factors and organisation readiness influencing the organisation in the adoption or improvement of new technologies. The second framework is used to assess the readiness of organisations with regards to information security based on ISO 27001 (ISO/IEC, 2013). To assess the readiness of CSPs the authors developed their model based on the previous frameworks, replacing ISO 27001 (ISO/IEC, 2013) with ISO 27017 (ISO/IEC, 2017) which is the international standard for Cloud Security (Nur Ilyani Ahmad, 2019).

From the previous paragraphs, many academics have used multiple resources to assess the readiness of organisations based on specific criteria to fulfil a diverse range of objectives. Other researchers were able to automate the readiness assessment process as they were based on well-established frameworks and standards in their fields. The literature review showed that readiness assessment has common methodology traits regardless of the field it is applied. Researchers have assessed the readiness of organisations based on certain factors. These factors were then used as domains often mapped with popular standards to establish the criteria that must be satisfied for organisations to be ready. However, despite the plethora of academic studies, there is a lack of academic instruments to assess the readiness of organisations before taking part in certifications. While this research is based on previous work, it is novel in the sense that it aims to support future certification processes based on a new set of requirements that have yet to be implemented. Table 1 presents a summary of the literature-based and framework-based readiness models.

Table 1: literature-based and framework-based readiness models

Author	Context	Methodology
Nisreen Ameen, 2021	Security assessment of BYOD in the organisation	Questionnaire mapped to BYOD domains
Cheang, 2009	Cybersecurity readiness index for public organisations	Popular domains influencing security based on popular security index frameworks
Straub, 2021	Cybersecurity readiness levels to assess cybersecurity maturity of cybersecurity systems	Cybersecurity readiness levels are based on technology readiness levels used by organisations
Babkin Alexandr V., 2018	Readiness assessment to move to a new educational model	Readiness domains in line with SMART education
Esa, 2019	Readiness assessment for ISMS implementation	Readiness domains in line with ISMS controls

Heru Susanto, 2012	Information security compliance assessment based on six-layer framework	Information security controls mapped to six-layer domains
Husam Barham, 2020	Readiness assessment for big data projects	Literature-based domains determining the level of readiness of organisations to carry out big data projects
Syed Rizvi, 2020	CSP readiness assessment from CSU perspective	Security assessment against literature-based inference rules
Shaikha Hasan, 2021	Cybersecurity readiness assessment for organisations	Popular factors affecting cybersecurity in organisations mapped to the TOE framework
Fasil Alemeye, 2015	Readiness assessment for Iaas and Saas cloud services	Domains combining the TOE framework, the technology acceptance model (TAM) and the diffusion of innovations (DOI) theory
Nurul Huda Nik Zulkipli, 2021	Readiness assessment for IoT forensic investigations	Popular domains affecting forensic investigation for IoT systems based on literature
AlEnezi, 2020	Employee security readiness contribution to the security posture of organisations	Popular domains affecting overall security posture of organisation systems based on literature
Ahmed Alenezi, 2020	Forensic readiness for cloud service providers	Popular domains affecting forensic readiness of CSP based on literature
Umar Mukhtar Ismail, 2020	Transparency levels of CSP from a CSU perspective	Conformity domains based on agreements between CSP and CSU
David Simms, 2013	Organisation's acceptance of cloud services	Survey response
Mpho Percy Makutsoane, 2014	Forensic readiness for cloud service providers	Popular domains affecting forensic readiness of CSP based on literature and authors expertise
Sara N. Matheu-García, 2019	Security level assessment of IoT products	Domains based on previous frameworks and international standards for IoT systems
Valentina Casola, 2021	Security assessment of cloud bases applications in the design phase	Domains based on previous frameworks and international standards for IoT systems

Jamal N. Al-Karakia, 2020	Security maturity assessments of governmental organisations	Domains based on regulations
Aristeidis Chatzipoulidis, 2019	Readiness assessment of organisations to take on GDPR certification	Domains based on GDPR
Nur Ilyani Ahmad, 2019	Security readiness assessment of CSPs	Domains based on two popular frameworks mapped with international standards for cloud security
Hans P. Borgman, 2013	Assessment of factors affecting the adoption of cloud services	Popular domains affecting forensic readiness of CSP based on literature and the TOE framework
Sugandh Bhatia, 2018	Security readiness assessment of CSPs	Domains affecting security readiness of CSP hexagonal framework and literature
Muhammad Imran Tariq, 2016	Effectiveness of international standards for CSP security assessment	Domains based on international standards

3 Research Methodology

This research follows a methodology based on previously published works that assessed the readiness of CSPs against a specific set of requirements (Nur Ilyani Ahmad, 2019) (Heru Susanto, 2012). The Cloud Service Readiness (CSR) domains are based on the Technology Organisation Environment (TOE) framework and the six-layer framework to achieve a holistic view of the factors affecting the security posture of organisations. These domains are factors that affect the readiness and compliance of organisations. The requirements of the EUCS scheme were mapped to each of the CSR domains. Subsequently, survey questions were drafted per CSR domain based on requirements present in each domain. It is necessary to point out that all the requirements were not included in the questionnaire as it is a new scheme, and it is probable that CSPs are unaware of specific terms used in its context. The answers expected for the questionnaire are ‘Yes’, ‘No’ and ‘N/A’. These answers were used to determine a readiness score in each CSR domain. The overall score is the average of the scores.

The mapping, the questionnaire and the score calculation methodology were reviewed by a cloud security industry expert. Feedback was considered for each of the elements of the framework and the questionnaire was circulated to preselected CSPs for testing purposes. The CSPs were selected across SMEs in Ireland. The responses were used to assess readiness and specifically answer the following questions:

- What is the average score of CSPs by categories of SMEs in Ireland?
- What is the factor that scored higher amongst CSPs?
- What is the factor that scored lower amongst CSPs?

To answer these questions, the means of all factors and overall scores were calculated. The mean of the overall scores was used to determine the answer to the average score of the sample of CSPs selected for the study. The factor that scored higher was determined by the highest mean value across all factors. Similarly, the factor that scored lower was determined by the lowest mean value. A summary of the steps of the research methodology is presented in Figure 2.

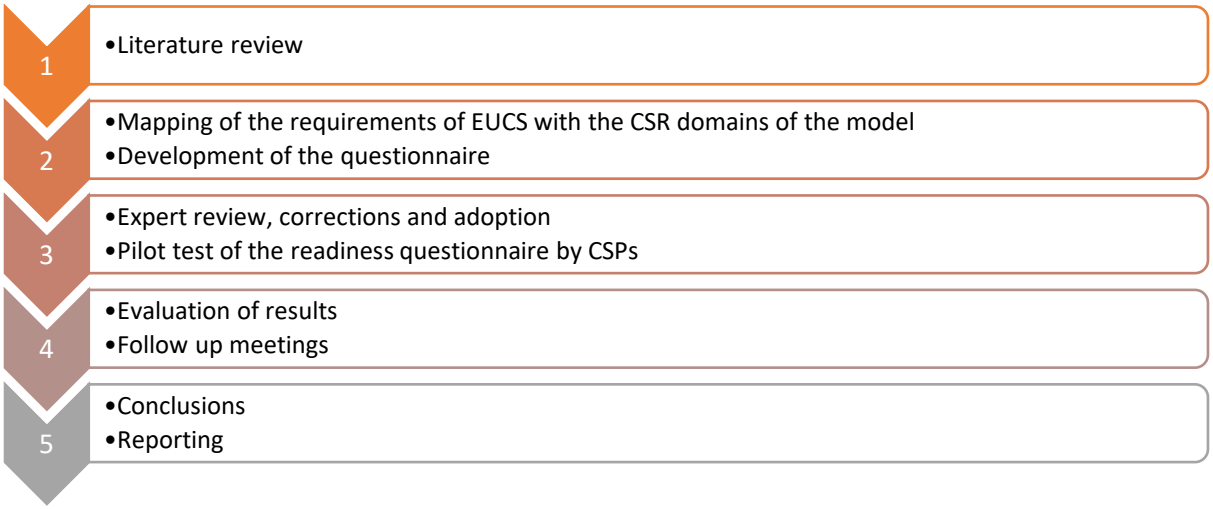


Figure 2: Research methodology

4 Design Specification

The CSR domains are based on previous studies that assessed the security readiness of CSPs based on popular frameworks such as the TOE framework and the six-layer framework (Nur Ilyani Ahmad, 2019) (Heru Susanto, 2012). In the studies, the model domains are mapped with the security controls provided in an international standard for cloud security, ISO 27017 (ISO/IEC, 2017). For this research, the controls were based on the EUCS scheme requirements that are aligned with assurance levels Basic, Substantial and High. The EUCS scheme defines assurances levels that determine the depth to which cloud services are assessed to be successfully certified. These were included in the EUCS CSR model as priorities to assist CSPs in the implementation of additional compensatory controls, to improve their security posture. The CSR model is built over seven domains including Technology, Organisation, Policy, Stakeholders, Culture, Knowledge and Environment as shown in Table 2.

Table 2: CSR domains

CSR domains	Definition	Scope
Technology	Technology and tools that support a CSP's operation (Heru Susanto, 2012)	Asset and risk management, security of tools and communications
Organisation	A structured unit of people managed to meet a collective goal associated with the industry (Heru Susanto, 2012)	Organisation's legal and regulatory responsibilities

Policy	Set of rules that guide decisions to achieve rational outcomes (Heru Susanto, 2012)	All policies affecting the security of an organisation
Stakeholder	A party that has a stake in an organisation (Heru Susanto, 2012)	All parties that have an impact or are impacted by the organisation's operations
Culture	The culture that determines the values and behaviours that contributes to the environment of organisations (Heru Susanto, 2012)	Acceptable and non-acceptable, important, and non-important, right, or wrong, workable, or not (Heru Susanto, 2012)
Knowledge	Knowledge held by an organisation and its employees (Heru Susanto, 2012)	Intellectual property, employees', and users' documentations
Environment	The environment in which the operations are carried out	Physical and logical environment

Each requirement of the EUCS scheme was mapped against the CSR domains in Table 2. Table 3 below presents the mapping after the application of corrections taken from the feedback received from the cloud security industry expert.

Table 3: EUCS CSR mapping

CSR Domains		EUCS Scheme Requirements	
1	**Technology**	A.5	Asset Management
		A.3	Risk Management
		A.9	Cryptography and Key Management
		A.10	Communication Security
		A.11	Portability and Interoperability
		A.13	Development of Information Systems
		A.20	Product Safety and Security (PSS)
		A.6	Physical Security
		A.7	Operational Security
		A.17	Compliance
		A.8	Identity, Authentication, And Access Control Management
2	**Organisation**	A.1	Organisation of Information Security
		A.3	Risk Management
		A.6	Physical Security
		A.8	Identity, Authentication, and Access Control Management
		A.12	Change and Configuration Management
		A.5	Asset Management
		A.17	Compliance
		A.15	Incident Management
		A.7	Operational Security
		A.19	Dealing with Investigation Requests from Government Agencies
		A.16	Business Continuity

3	**Policy**	A.3	Risk Management
		A.5	Asset Management
		A.9	Cryptography and Key Management
		A.10	Communication Security
		A.13	Development of Information Systems
		A.15	Incident Management
		A.6	Physical Security
		A.7	Operational Security
		A.8	Identity, Authentication, And Access Control Management
		A.12	Change and Configuration Management
		A.14	Procurement Management
		A.16	Business Continuity
		A.17	Compliance
		A.2	Information Security Policies
		A.4	Human Resources
4	**Stakeholder**	A.11	Portability and Interoperability
		A.14	Procurement Management
		A.4	Human Resources
		A.1	Organisation of Information Security
		A.15	Incident Management
		A.17	Compliance
5	**Culture**	A.17	Compliance
		A.15	Incident Management
6	**Knowledge**	A.10	Communication Security
		A.11	Portability and Interoperability
		A.17	Compliance
		A.15	Incident Management
		A.18	User Documentation
		A.4	Human Resources
		A.15	Incident Management
7	**Environment**	A.13	Development of Information Systems
		A.7	Operational Security
		A.6	Physical Security
		A.12	Change and Configuration Management
		A.6	Physical Security

Following the mapping, a questionnaire was developed based on the EUCS scheme requirements as shown in Figure 3.

	CSR domains	Questionnaire	Answers	Rationale
1	Technology	Are your assets managed in accordance with the results of your risk assessment?		
		Are your assets classified and labelled?		
		Are data encrypted at rest and in transit?		
		Are your network technical safeguards in line with the results of your risk		
		Are the input and output interfaces clearly documented?		
		Are contractual agreements for the provision of data between the CSP and the CSC in line with regulations?		
		Are Data securely deleted after the termination of a CSC contract?		
		Are the dependencies to hardware and software documented?		
		Is procurement for the development of the cloud service included in the risk		
		Is the history of changes in source code available?		
		Are tests environments involved in the development lifecycle of the information system of the cloud service?		
		Are tests environments segregated from production environments?		
		Is security involved by design in the development of cloud services?		
		Are cloud services tested for vulnerabilities?		
		Are sub contractors involved in the risk assessment?		
		Are outsourced development activities in line with the CSP secure		
		Are interfaces for error handling and logging mechanisms available to CSCs?		
		Is session management implemented to protect CSCs against known attacks?		
		is software defined networking for CSCs in line with the network security		
		Are changes to images for virtual machines and containers monitored and		
		Are your commitments with regards to location of data processing and storage enforced by the cloud service architecture?		
		Is capacity in personnel and IT resources monitored?		
		Are the backups regularly tested?		
		Is the history of logs monitored?		
2	Organisation	Is an ISMS implemented in line with ISO 27001?		
		Is the segregation of duties implemented in line with the results of the risk		
		Is the CSP aware of trending security threats and vulnerabilities?		
		Are projects managed in line with the results of a risk assessment?		
		Are data monitored during legal investigations?		
		is business continuity implemented in line with the business impact analysis		

Figure 3: EUCS readiness questionnaire

Certain values are associated with the possible answers to calculate the readiness scores ('Yes' = 1, 'No' = 0, 'N/A' is not considered). The answers collected for each domain allow the calculation of the readiness score, *q*, of the domain based on the following formula.

$$q = \frac{y}{v-z} \times 4$$ (Nur Ilyani Ahmad, 2019)

Where *q* is the total score in each domain; *y* is the total number of answers 'Yes'; *v* is the total number of questions; *z* is the total number of answers 'N/A'; considered for 4 levels of readiness (not ready, likely low, likely intermediate, likely high).
The overall score is determined by *x* based on the following formula

$$x = \sum_{i=1}^{7} \frac{q_i}{7}$$ (Nur Ilyani Ahmad, 2019)

The levels of readiness are defined as follows:

- $0 \leq x \leq 1$ is equal to "Not ready" meaning that the CSP likely meets less than 25% of the EUCS scheme requirements
- $1 < x \leq 2$ is equal to "Likely Low" meaning that the CSP likely meets between 25% and 50% of the EUCS scheme requirements
- $2 < x \leq 3$ is equal to "Likely Intermediate" meaning that the CSP likely meets between 50% and 75% of the EUCS scheme requirements
- $3 < x \leq 4$ is equal to "Likely High" meaning that the CSP likely meets between 75% and 100% of the EUCS scheme requirements

5 Implementation

The mapping, questionnaire and results were collated in an excel worksheet that provides the CSPs with readiness scores in each CSR domain, an overall readiness level, as well as recommendations to improve these scores. The excel worksheet is structured as follows:

- **Introduction**

The 'Introduction' tab presents the purpose of the tool. Definitions and acronyms are also provided for the CSP to get a better understanding of how to use the tool. An extract of the 'Introduction' tab is presented in Figure 4.

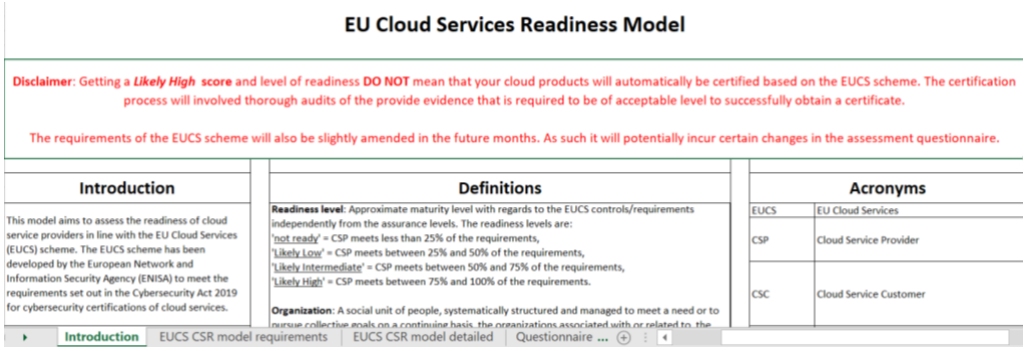


Figure 4: 'Introduction' tab

- **EUCS CSR model requirements**

This tab presents the mapping of the CSR domains against the EUCS requirements as shown in Figure 3. The 'EUCS CSR model requirements' tab is useful to CSPs who might get a high-level understanding of the EUCS requirements and to which CSR domain they correspond.

- **EUCS CSR model detailed**

This tab presents detailed requirements of the EUCS. The 'EUCS CSR model detailed' tab is useful for CSPs after they get their readiness level and wish to improve their security posture. The detailed requirements provide an understanding of specific and clear requirements that must be met to improve the overall security level. Also, priorities are provided as guidance for additional compensatory controls implementation from 1 to 3, in line with assurance levels as shown in Figure 5.

4	Stakeholder	A.4	HUMAN RESOURCES	HR-03	EMPLOYEE TERMS AND CONDITIONS	HR-03.1	The CSP shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures	1
						HR-03.2	The CSP shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	1
						HR-03.3	The CSP shall give a presentation of all applicable information security policies and procedures to internal and external employees before granting them any access to customer data, the production environment, or any component thereof.	1
						HR-03.4	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof.	2
						HR-03.5	The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.	3
		A.1	ORGANISATION OF INFORMATION SECURITY	OIS-02	SEGREGATION OF DUTIES	OIS-02.1	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the cloud service.	1
						OIS-02.2	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the CSP: i) Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-09) ii) Development, testing and release of changes (cf. DEV-01, CCM-05); and i) Operation of the system	1
						OIS-02.3	The CSP shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.	1
						OIS-02.4	The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.	3
				OIS-03	CONTACT WITH AUTHORITIES AND INTEREST GROUPS	OIS-03.1	The CSP shall stay informed about current threats and vulnerabilities.	1
						OIS-03.2	The CSP shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.	2
						OIS-03.3	The CSP shall maintain regular contact with its CAB and NCCA to stay informed about current threats and vulnerabilities.	3
		A.15	INCIDENT MANAGEMENT	IM-05	INVOLVEMENT OF CLOUD CUSTOMERS IN THE EVENT OF INCIDENTS	IM-05.1	The CSP shall periodically inform its customers on the status of the incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual	1
						IM-05.2	As soon as an incident has been closed, The CSP shall inform its customers about the actions taken, according to the contractual agreements.	1
				CO-01	IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS	CO-01.1	The CSP shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service.	1
						CO-01.2	The CSP shall document and implement procedures for complying to these contractual	2
						CO-01.3	The CSP shall provide these procedures when requested by a CSC.	3
						CO-01.4	The CSP shall document and implement an active monitoring of the legal, regulatory and	3

Figure 5: Detailed requirements of the EUCS scheme

The assurance levels are defined in the EUCS scheme as basic, substantial, and high. A product, service or process that must be certified to a High Assurance level should meet all the requirements of the EUCS scheme. Likewise, a product that requires a Substantial assurance level certification must meet the basic and substantial requirements while a product, service or process that is required to be certified at the basic level must meet only the basic level requirements.

In this context, *priority 1 = basic assurance level requirements*, *priority 2 = substantial assurance level requirements* and *priority 3 = high assurance level requirements*. This means that all the requirements of *priority 1* must be met before those of *priority 2*. Going for requirements of *priority 3* means that the requirements of *priority 1* and *2* have been satisfied.

- **Questionnaire**

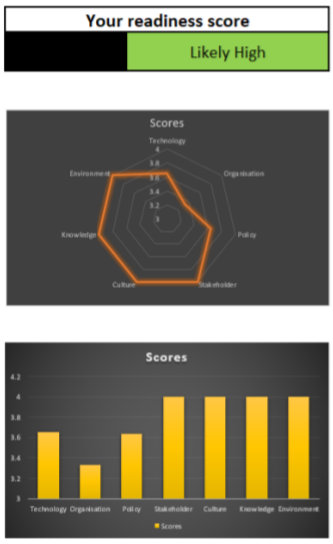
This tab is the only tab that takes input from the CSPs. The answers are provided in a dropdown and a rationale is expected for each 'N/A' response as shown in the extract below in Figure 6.

	CSR domains	Questionnaire	Answers	Rationale
1	Technology	Are your assets managed in accordance with the results of your risk assessment?	Yes	Assumtion: A cloud service provider is a third-party company offering a cloud-based platform, i
		Are your assets classified and labelled?	Yes	
		Are data encrypted at rest and in transit?	Yes	
		Are your network technical safeguards in line with the results of your risk assessment ?	Yes	
		Are the input and output interfaces clearly documented?	Yes	
		Are contractual agreements for the provision of data between the CSP and the CSC in line with regulations?	Yes	
		Are Data securely deleted after the termination of a CSC contract?	Yes	
		Are the dependencies to hardware and software documented?	Yes	
		Is procurement for the development of the cloud service included in the risk assessment?	Yes	
		Is the history of changes in source code available?	Yes	
		Are tests environments involved in the development lifecycle of the information system of the cloud service?	Yes	
		Are tests environments segregated from production environments?	Yes	
		Is security involved by design in the development of cloud services?	Yes	
		Are cloud services tested for vulnerabilities?	Yes	
		Are sub contractors involved in the risk assessment?	No	
		Are outsourced development activities in line with the CSP secure development policy?	Yes	
		Are interfaces for error handling and logging mechanisms available to CSCs?	Yes	Dependent on customer agreement in place
		Is session management implemented to protect CSCs against known attacks?	No	
		Is software defined networking for CSCs in line with the network security policies	Yes	
		Are changes to images for virtual machines and containers monitored and communicated to CSCs	NA	Two diff types - 1. installed baseline images are used to set up the server, which are then contr
		Are your commitments with regards to location of data processing and storage enforced by the cloud service architecture?	Yes	
		Is capacity in personnel and IT resources monitored?	Yes	
		Are the backups regularly tested?	Yes	
		Is the history of logs monitored?	Yes	
		Is an ISMS implemented in line with ISO 27001?	Yes	

Figure 6: Questionnaire

- **Results**

Answers provided by the CSPs are used to calculate the readiness score in the 'Results' tab. General recommendations are also available as well as visual representations of the results as shown in Figure 7.



Recommendations

Technology

Review the following to ensure that they are in line with the requirements in the EUCS CSR model:
Asset management
Cryptography and key management
Communication Security
Portability and interoperability
Development of information Systems
Product Safety and Security
Operation Security

Organisation

Review the following to ensure that they are in line with the requirements in the EUCS CSR model:
Organisation of information security
Dealing with investigation requests from government agencies
Business continuity

Policy

Review the following policies to ensure that they are in line with the requirements in the EUCS CSR model:
Risk management
Asset management
Cryptography and key management
Communication security
Development of information systems
Incident management
Operational security
Identity, authentication, and access control management
Change and configuration management
Procurement management
Business continuity
Compliance
Information security policies
Human resources

Stakeholder

Review your compliance requirements and internal audit plans to ensure that they are in line with the requirements in the EUCS CSR

Culture

Review your incident response implementation to ensure that it is in line with the requirements in the EUCS CSR model

Knowledge

Review your User Documentation implementation and incident response learning process to ensure that they are in line with the requirements in the EUCS CSR model

Environment

Review your Physical Security implementation to ensure that it is in line with the requirements in the EUCS CSR model

For more information on recommendations consult the "EUCS CSR model detailed" sheet or the EUCS at the following link
https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Figure 7: Results

In Section 6 the responses to the EUCS questionnaire are collated in a single worksheet for further analysis.

6 Evaluation

The evaluation of the results obtained includes the analysis of the individual responses obtained from the EUCS questionnaire and the analysis of the overall responses provided by the 5 CSPs who participated in this study.

6.1 Analysis of the responses provided by a CSP

CSPs responded to each question included in the EUCS CSR questionnaire introduced in Section 5. The responses were used to calculate a readiness score for each CSR domain and issue an overall readiness level to the CSP. Figure 8 shows the results obtained for one of the CSPs selected.

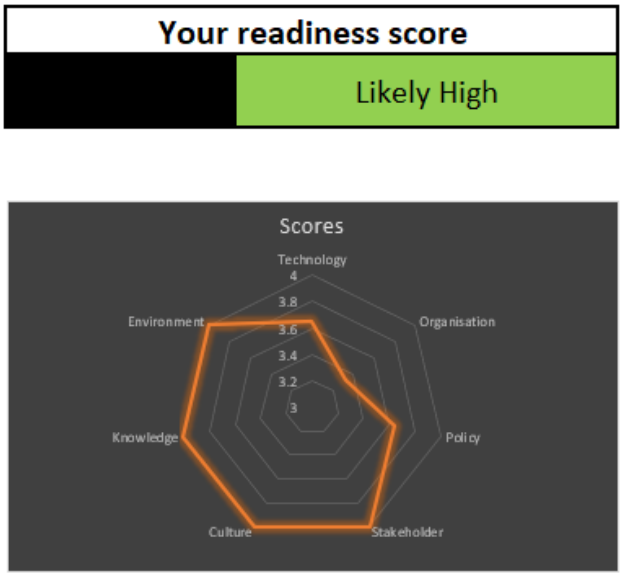


Figure 8: Readiness score and level Results

The results show that this CSP scored:

- Between 3 and 4 for Technology, Organisation and Policy domains and
- 4 for Environment, Knowledge, Culture and Stakeholder domains

These results indicate that it is probable that the selected CSP satisfies more than 75% of the EUCS scheme requirements in each domain. Their readiness level is 'Likely High'. This means that they are likely ready to take part in the EUCS certification as it is probable that they meet more than 75% of the requirements of the EUCS scheme overall.

6.2 Analysis of the overall responses provided by CSPs

From the 27 CSPs that were contacted to participate in the EUCS readiness assessment, 5 responded positively and completed the questionnaire achieving an 18.5% response rate. The

CSPs that participated in the study were SMEs that are ISO 27001 certified. The specific cloud services provided by the sample set included Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) all of which were deemed Substantial or High-Risk services. The risk is determined by the impact of threats and vulnerabilities on the services and their importance for the organisation. While CSP respondents had a lot in common, the scores emphasized the differences in their security approaches as shown in Table 4.

Table 4: CSP scores

CSP	Type of service	Tech	Org	Pol	Sta	Cul	Kno	Env	Overall score
Company A	Iaas, Paas, Saas	3.652	3.333	3.636	4	4	4	4	**3.803**
Company B	Iaas, Baas, Draas	4	3.333	4	4	4	4	4	3.905
Company C	Iaas, Draas	3.455	3	3.818	2.667	4	2.667	4	3.372
Company D	Iaas, Baas, Draas	1.333	2.4	1.455	1.333	0	4	4	2.074
Company E	Iaas, Baas, Draas	3.789	4	3.636	4	4	4	4	3.918
Mean		3.246	3.213	3.309	3.200	4.000	3.733	4	3.415

From Table 4, the overall average score of CSP participants is 3.415. This value corresponds to a readiness level of "Likely High". Table 5 shows the results of descriptive statistics performed on the sample.

Table 5: Descriptive statistics

	Technology	Orgnisation	Policy	Stakeholder	Culture	Knowlegde	Environment	Overall score
count	5.000000	5.000000	5.000000	5.000000	5.000000	5.000000	5.0	5.000000
mean	3.245905	3.213333	3.309091	3.200000	3.200000	3.733333	4.0	3.414523
std	1.087502	0.581951	1.047626	1.192570	1.788854	0.596285	0.0	0.781404
min	1.333333	2.400000	1.454545	1.333333	0.000000	2.666667	4.0	2.074459
25%	3.454545	3.000000	3.636364	2.666667	4.000000	4.000000	4.0	3.372294
50%	3.652174	3.333333	3.636364	4.000000	4.000000	4.000000	4.0	3.803124
75%	3.789474	3.333333	3.818182	4.000000	4.000000	4.000000	4.0	3.904762
max	4.000000	4.000000	4.000000	4.000000	4.000000	4.000000	4.0	3.917977

Descriptive statistics on the sample highlights that the Environment domain has a constant value of 4. It is the highest value that can be scored. This shows that all CSPs likely fulfil more than 75% of the requirements of the EUCS Environmental (physical and logical) security. It is also important to note that the Knowledge domain scored the highest minimal value of 2.667, while the Culture domain scored the lowest minimal value across domains which is zero. The

results indicate that most participants are mature in the Knowledge and Environment domains that address documentation and environmental (physical and logical) security. While the culture domain that focuses on incident response is not well developed. Furthermore, the means of all domains remain between 3 and 4. After the Environment domain (4), the Knowledge domain scores second highest (3.73) between CSP participants. Also, Culture is the domain that scored lower in terms of readiness across the sample of CSPs. The Pearson correlation matrix in Table 6 shows the relationship between these variables.

Table 6: Correlation matrix

	Technology	Orgnisation	Policy	Stakeholder	Culture	Knowlegde	Environment	Overall score
Technology	1.000000	0.820821	0.984169	0.929510	0.983134	-0.107249	NaN	0.987135
Orgnisation	0.820821	1.000000	0.729658	0.883744	0.781281	0.204926	NaN	0.879868
Policy	0.984169	0.729658	1.000000	0.853766	0.989592	-0.271653	NaN	0.944996
Stakeholder	0.929510	0.883744	0.853766	1.000000	0.875000	0.250000	NaN	0.973789
Culture	0.983134	0.781281	0.989592	0.875000	1.000000	-0.250000	NaN	0.958684
Knowlegde	-0.107249	0.204926	-0.271653	0.250000	-0.250000	1.000000	NaN	0.030211
Environment	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN
Overall score	0.987135	0.879868	0.944996	0.973789	0.958684	0.030211	NaN	1.000000

This matrix shows that there is no relationship between the Environment domain and the others as it has a constant value of 4 across the CSR domains. The remaining domains have a strong positive relationship with each other and the overall score except with the Knowledge domain. The latter domain has a weak positive relationship with the Organisation, the Stakeholder domains and overall score while it has a weak negative relationship with the Technology, Policy and Culture domains. This is also visible in the heatmap presented in Figure 9.

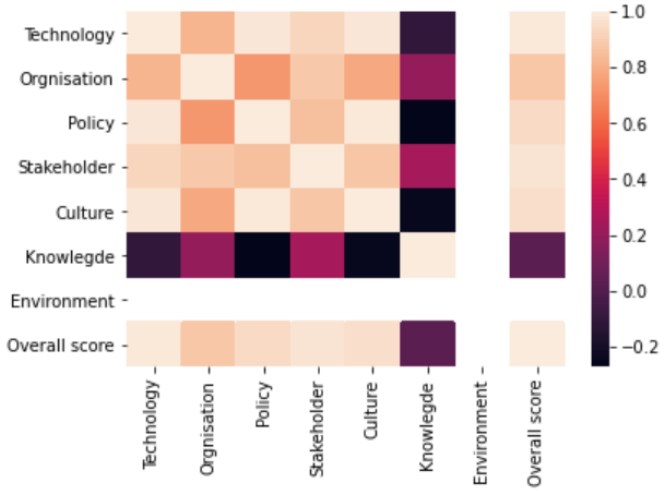


Figure 9: Correlation Matrix heatmap

Based on these results, it is probable that the CSPs that participated in this study satisfy more than 75% of the requirements of the EUCS scheme. The results also show that CSPs scored best in "**Knowledge**" and "**Environment**" while the domain "**Culture**" needs improvement.

6.3 Discussion

This research followed a two-step methodology; Section 6.1 aimed to assess the readiness of CSPs individually based on CSR domains. Selected CSPs provided answers to the EUCS questionnaire and obtained scores per CSR domains and an overall readiness level. Although the questionnaire does not cover all EUCS requirements, it provides an approximate indication of EUCS scheme readiness for CSPs as confirmed by an industry expert. Section 6.2 attempted to assess the readiness of the Cloud industry based on the sample of CSPs selected. The results show a high probability that the sample of CSPs selected fulfil more than 75% of the EUCS scheme requirements. It was also noted that despite participants' ISO 27001 certification, CSPs obtained significantly different results. This shows that the EUCS scheme requirements cover a wider scope to secure the assets of organisations than ISO 27001. While it was determined that the CSPs interviewed are likely ready to participate in the EUCS scheme certification, it is important to note the limitations of the study as follows:

- The EUCS scheme has not been officially completed and might be slightly amended in the future term. As such, the EUCS questionnaire will potentially incur certain changes.
- Guidance for each of the EUCS requirements has not been provided in the scheme. The guidance is helpful to assess the suitability of the implementation of the security controls for cloud services. For this reason, the assessment had to be based on responses of the CSPs only, instead of what is acceptable or not in the context of the scheme. As such, the readiness level provided cannot be definite. The EUCS questionnaire will require certain updates in the future once the EUCS scheme is amended with final comments and guidance for audits will be officially published.
- The response rate of 18.5% may not be reflective of the entire Cloud Sector. Due to time constraints, the sample of data collected is small and not representative of the cloud market in Ireland
- All the respondents are SMEs that are ISO 27001 certified. It is likely that these qualification criteria have had an impact on the responses received. Performing the tests on a significant sample with a larger and diverse number of participants will provide more representative results of the status quo in the cloud market in Ireland.

These results provided a better understanding of the security status of CSPs to the stakeholders involved in the EUCS scheme certification process. To efficiently respond to the increasing threat of cybercrime it is important to establish appropriate communication and engagement strategies across stakeholders. In that sense, the sample of CSPs selected for the study will be included if interested in future EUCS scheme pilot certifications and workshops as part of the A4CEF[9] project.

[9] https://www.a4cef.eu/

7 Conclusion and Future Work

This research attempted to determine the readiness level of CSPs in Ireland with regards to the new EU cybersecurity certification scheme for cloud services, the EUCS scheme. The study followed a two-step approach including determining the readiness of CSPs individually, and subsequently determining a readiness score for CSPs on a collective basis.

The CSR model domains used to determine the CSP readiness level individually is based on the TOE framework used to assess the readiness of organisations with regards to certain criteria and the six-layer framework used to assess the compliance of organisation mapped against a set of requirements. In the context of this study, the requirements are from the EUCS scheme. These domains are assessed based on a survey, aiming to provide readiness scores of the CSP in each domain. CSPs were identified to participate in the research, expected to provide Yes, No, N/A type answers to the questionnaire. These answers were associated with values to determine the score for each domain, which contributed to determining the overall readiness level of the CSP. The scores of each CSR domain and the overall readiness level of CSPs were used to calculate the collective readiness level of the sample of CSPs. The results showed CSPs are likely ready to participate in future EUCS scheme certification.

Although the research questions were successfully addressed, it is important to note the limitations associated with the analysis complete. As the readiness assessment methodology is performed before the scheme has come into force, certain requirements have not been considered in the scope of the EUCS questionnaire. As such, the assessment provides an approximate readiness level. Furthermore, the assessment is limited to identifying the EUCS requirements achieved by CSPs instead of assessing the level of suitability of their security implementation as it is done during a certification assessment. Also, the sample used to determine the collective readiness level only involves ISO 27001 certified SME CSPs and its size is not representative of the market in Ireland. As such, the results cannot extend to the other categories of SMEs and CSPs in Ireland.

Further improvements include updating the questionnaire to include the future guidance that the EUCS scheme will provide for certifications, extend the assessment to audits and include a larger and diverse number of participants in the evaluation. This will provide results that are representative of the Irish market.

References

Ahmed Alenezi, H. F. A. G. B. W., 2020. Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing: Advances, Systems and Applications*, 8(11).

AlEnezi, A., 2020. *Internet of Things & Cybersecurity Readiness*, Kuwait: Kuwait University.

Aristeidis Chatzipoulidis, T. K. T. T., 2019. A readiness assessment tool for GDPR compliance certification. *Computer Fraud & Security*, pp. 14 - 19.

Babkin Alexandr V., T. G. I. T. I. A., 2018. *Methods of Assessment of Compliance of the Regional University as a Driver of Innovation with the Principles of SMART-education.* s.l., s.n.

Barclay, C., 2014. *SUSTAINABLE SECURITY ADVANTAGE IN A CHANGING ENVIRONMENT: THE CYBERSECURITY CAPABILITY MATURITY MODEL (CM2).* St. Petersburg, s.n.

Cheang, S., 2009. *CONCEPTUAL MODEL FOR CYBERSECURITY READINESS ASSESSEMENT.* Seoul, s.n.

David Simms, S. G., 2013. *Structured and unstructured data in the Cloud: A Swiss perspective on readiness and internal controls.* Barcelona, s.n.

Esa, F. S. B. M., 2019. *READINESS OF LOCAL AUTHORITIES IN IMPLEMENTING INFORMATION,* s.l.: Universiti Teknologi Malaysia.

Fasil Alemeye, F. G., 2015. *Cloud Readiness Assessment Framework and Recommendation System.* Addis Ababa, s.n.

Hans P. Borgman, B. B. H. H. F. S., 2013. *Cloudrise: Exploring Cloud Computing Adoption and Governance.* Wailea, s.n.

Heru Susanto, M. N. A. Y. C. T. M. S. A., 2012. I-SolFramework: An Integrated Solution Framework Six Layers Assessment on Multimedia Information Security Architecture Policy Compliance. *International Journal of Electrical & Computer Sciences IJECS-IJENS,* 12(01).

Husam Barham, T. D., 2020. The use of readiness assessment for big data projects. *Sustainable Cities and Society,* 60(102233).

ISO/IEC, 2013. *Information technology — Security techniques — Information security management systems — Requirements,* s.l.: ISO/IEC.

ISO/IEC, 2017. *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services,* s.l.: ISO/IEC.

Jamal N. Al-Karakia, A. G. S. E.-Y., 2020. GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences.*

Mpho Percy Makutsoane, A. L., 2014. *A Conceptual Framework to Determine the Digital Forensic Readiness.* Pretoria, s.n.

Muhammad Imran Tariq, V. S., 2016. *Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing.* Catania, s.n.

Nisreen Ameen, A. T. M. H. S. N. M. J. P., 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity. *Computers in Human Behavior,* 114(106531).

Nur Ilyani Ahmad, I. M. M. D. A. D. J. N. A. H., 2019. *Cloud Service Provider Security Readiness Model: The Malaysian Perspective.* Bandung, s.n.

Nurul Huda Nik Zulkipli, G. B., 2021. *An Exploratory Study on Readiness Framework in IoT Forensics.* s.l., s.n.

Sara N. Matheu-García, J. L. H.-R. A. F. S. G. B., 2019. Risk-based automated assessment and testing for the cybersecurity. *Computer Standards & Interfaces,* Volume 62, pp. 64 - 83.

Shaikha Hasan, M. A. S. K. R. T., 2021. Evaluating the cyber security readiness of organizations and its influence. *Journal of Information Security and Applications,* 58(102726).

Straub, J., 2021. *Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems.* Vancouver, s.n.

Sugandh Bhatia, J. M., 2018. CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy. *International Journal of Electrical and Computer Engineering (IJECE),* 8(5), pp. 3756-3766.

Syed Rizvi, J. M. A. R. M. R. R. I. W., 2020. A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers. *Journal of Cloud Computing: Advances, Systems and Applications,* 9(42).

Technology, N. I. o. S. a., 2020. *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations,* s.l.: National Institute of Standards and Technology.

Umar Mukhtar Ismail, S. I., 2020. A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications,* 54(102594).

Valentina Casola, A. D. B. M. R. U. V., 2021. A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. *The Journal of Systems and Software,* 163(110537).