Configuration Manual

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……………………….………		
Lecturer:	…………Vikas Sahni………………………………….………		
Submission Due Date:	…………………………………………………………………………………………….………		
Project Title:	Assessing the Readiness of Cloud Service Providers in Ireland for the EU Cloud Services Scheme		
Word Count:	…………1539……………	**Page Count:**	……………06……….…….………

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: …03rd September 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):	

Configuration Manual

Khalimatou Samirah
Student ID: x18102263

1 Cybersecurity Act, EUCS Scheme and Cloud Security Readiness factors

The Cybersecurity Act 2019 aim to reinforce the role of ENISA in the EU and layout base requirements for ICT products, services, and processes cybersecurity certifications. These certifications should be recognised across the European member countries. Through these certifications, the regulation will establish a safe environment for organisations and customers based on the trust of ICT products. The requirements of the certification process include several stakeholders such as the National Cybersecurity Certification Authority (NCCA), the National Accreditation Body (NAB), Conformity Assessment Bodies (CAB), testing laboratories (ITSEF) and the organisations that develop products requiring certificates (EUR-Lex, 2019).

The regulation also defines the base responsibilities of each stakeholder. However, it remains challenging to fulfil these requirements based on the regulation alone. These challenges include the heterogeneity of ICT products, services and processes that present different characteristics and cannot be certified following the same standards. Furthermore, the certifications performed currently across certain European member countries are only recognised within those countries and present certain limitations. Because of this, ENISA provides upon request candidate schemes to assist European member countries in the implementation of the Cybersecurity Act (EUR-Lex, 2019). In line with the requirements of this regulation, ENISA issued a European candidate scheme for cloud services (EUCS).

The first version of the EUCS has been issued in 2021 to guide cloud services cybersecurity certifications. It provides in annexes mandatory requirements to assess and evaluate the cloud service to certify depending on the level of assurance required to achieve the level of assurance laid out in the Cybersecurity Act. It also guides with regards to the management of vulnerabilities related to the product or affecting it, how to maintain compliance and its validity period, the label on the certificate and other aspects of the certification process. The development of the EUCS is based on international standards for cloud security developed by ISO and national cybersecurity schemes applied in other EU member countries. As such it provides in its Annex A – SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES, a list of requirements for cloud services based on international standards such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017 (ENISA, 2020). These requirements have been mapped against a model composed of factors that impact organisations readiness and compliance towards a set of predefined requirements or controls.

The Cloud Security Readiness (CSR) model factors are Technology, Organisation, Policy, Stakeholder, Culture, Knowledge and Environment (Nur Ilyani Ahmad, 2019). Each factor corresponds to a set of requirements of the EUCS. The requirements have subsequently been used to draft questions to assess the readiness of the organisation with regards to the requirements.

2 Questionnaire and data collection

The questions have been drafted to assess what requirements are met by CSPs. While there are multiple requirements, the number of questions have been reduced to provide a user-friendly experience to the participants. Each question has been developed to meet multiple requirements of the EUCS scheme and is expecting Yes, No, N/A type answers. For example, the following question "Are input and output interfaces clearly documented?" addresses the requirements below in Table 1.

Table 1: EUCS requirements A.11, PI-01 - DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES

PI-01.1	The cloud service shall be accessible by cloud services from other CSPs or cloud customers' IT systems through documented inbound and outbound interfaces
PI-01.2	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data
PI-01.3	Communication on these interfaces shall use standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements
PI-01.4	Communication over untrusted networks shall be encrypted according to CKM-02
PI-01.5	The CSP shall allow its customers to verify the interfaces provided (and their security) are adequate for its protection requirements before the start of the use of the cloud service, and each time the interfaces are changed

The data used for the analysis involved the readiness scores and levels of each CSP as well as additional company data such as cloud services provided and company size. Selected CSPs were contacted individually with regards to their benefits in participating in the research. The EUCS questionnaire is presented in an excel workbook with complementary sheets such as:

- The "EUCS CSR model requirements" sheet presents a mapping of the Cloud Service Readiness (CSR) model and the requirements of the EUCS scheme.
- The "EUCS CSR model detailed" sheet presents a mapping of the CSR model and the requirements of the EUCS scheme with specific details about the requirements of the scheme.
- The "Questionnaire" sheet presents a mapping of CSR domains with questions to assess the readiness of the cloud service provider with regards to EUCS cybersecurity certification.

- The "Results" sheet presents the readiness scores and level of the CSP, graphic visuals of the score per domain and general recommendations to improve the CSP's posture with regards to EUCS cybersecurity certification.

The EUCS questionnaire was sent out when they expressed interest in contributing to the research. The data were collected from the responses provided by CSPs, information on their website and LinkedIn page as shown in Table 2 below.

Table 2: CSP Dataset collection

CSP in Ireland			CSR domains score							
N	**Company**	**SME Category**	**Tech**	**Org**	**Pol**	**Sta**	**Cul**	**Kno**	**Env**	**Readiness level**
1	**A**	**Small**	3.652	3.333	3.636	4	4	4	4	**Likely High**
2	B	Small	4	4	3.818	4	4	4	4	**Likely High**
3	C	Micro	1	2	0.812	3	2	3	4	**Likely Intermediate**
…	…	…	…	…	…	…	…	…	…	…
	Arithmetic mean		2.88	3.111	2.751	3.667	3.333	3.667	4	**Likely High**

The colour code used through the document respects the following criteria

🟥 '**Not ready**' = CSP meets less than 25% of the requirements
🟧 '**Likely Low**' = CSP meets between 25% and 50% of the requirements
🟨 '**Likely Intermediate**' = CSP meets between 50% and 75% of the requirements
🟩 '**Likely High**' = CSP meets between 75% and 100% of the requirements

3 Monthly Internship reports

June Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Khalimatou Samirah	Student number:	x18102263
Company:	NSAI	Month Commencing:	June

- Contribution on the slides for the presentation of the A4CEF project
- Meetings and preliminary work for the project webpage
  Introduction to the Cybersecurity Act and EU candidate common criteria and cloud schemes
- Adoption of a topic for the internship research

Employers comments

Khalimatou has been a pleasure to work with these past weeks. She is punctual, diligent and has applied herself very well in the context of the tasks assigned to her pertaining to the EU project A4CEF. In the short time she has been with NSAI, she has taken onboard advice provided and now in a position to really make progress with respect to her dissertation.

Industry Supervisor Signature:	Stewart Hickey	Date	29.6.21
Student Signature:	Khalimatou Samirah	Date	30.6.21

July Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Khalimatou Samirah	Student number:	x18102263
Company:	NSAI	Month Commencing:	July

- Completion of the presentation for the A4CEF project
- Development of the EUCS readiness questionnaire
- Contact with CSPs to take part in the research evaluation
- Attendance and contributions to meetings for the A4CEF project website
- Design of the layout of the website and contribution for activities executive summaries

Employers comments

Khali has been a pleasure to work with over the last month. She is diligent, takes direction very well, always punctual for meetings, has shown excellent engagement with project partners and applies the theory and skills she has learned during her MSc to a high degree.

Industry Supervisor Signature:	Stewart Hickey	Date	29.7.21
Student Signature:	Khalimatou Samirah	Date	29.7.21

August Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Khalimatou Samirah	Student number:	x18102263
Company:	NSAI	Month Commencing:	August

- Attendance and contributions to meetings for the A4CEF project website
- Contribution to website building
- Collection of Data from CSPs and evaluation
- Follow up meetings with CSPs
- Report writing

Employers comments

The work completed in the final month of the Internship has been excellent. In addition to the above contributions, Khali helped NSAI to secure a SME CSP to participate in one of the EU Cyber Project pilot certifications. We highly value the significant contributions Khali has made during her internship. She has been an absolute pleasure to work with.

Industry Supervisor Signature:	Stewart Hickey	Date	18.8.21
Student Signature:	Khalimatou Samirah	Date	18.8.21

References

ENISA, 2020. *EUCS – CLOUD SERVICES SCHEME*, s.l.: ENISA.

EUR-Lex, 2019. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Union.*

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.