A close up of a sign

Description automatically generated



The Qufaro CyberEPQ Journal 2021

The Journal is an essential document which will indicate your engagement with the Modules which align with the Chartered Institute for Information Security - CIISEC (formerly the IISP) Skills Framework as well as the National Occupational Standards (NOS) for Information Security and the latest Cyber Security Body of Knowledge (CyBOK) framework.

Throughout the online studying, you will be expected to produce a Journal entry for each module which will record your activities (what you have learnt, found interesting etc) concerning your studies for the course based on the taught modules. There are 10 core modules to complete and 3 specialist modules. At least one of the Specialist Modules must be completed, but you may do more than one.

This document shall be used to evidence your progress throughout the Modules and that your skills and knowledge align with NOS and the CIISEC (formerly the IISP) Cyber Security Skills Framework which will be rewarded with the Qufaro CyberEPQ Certificate of Completion. Students who do not give due diligence to this may find that this aspect of their CyberEPQ is not recognised.

The Reflections in these Journal entries will also assist you in discussing and formulating ideas with your supervisor as to what you will choose to investigate and report on in your project. The Journal should also be referred to in your Production Log as it also aids part of the evidencing of the planning and development of your project. As the online study comes to a close, your time will be dedicated to the time and project management of the project, the essay, Production Log, evaluation of sources and the presentation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date**   1. **Introduction to Cyber Security** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **22nd September 2021**  **/ journal submitted on 11th oct 2021** | **Completed the first module , “introduction to cyber security”. Learnt about the computer misuse act then did the quiz.** | **Not doing the journal entry straight after completing the module** | **Doing the journal after I finish lol** |  |
| **Date**   1. **History of Computing & Cryptography** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **5th October 2021**  **/ journal submitted on 12th oct 2021** | **Learnt history of computing including enigma, some information about the historical computers in the national museum of computing, and early internet.**  **This module also included cryptography, in which I learnt about :**  **public-key and symmetric cryptography, hash functions, message authentication codes,**  **security services such as confidentiality, data integrity, data origin authentication, non-repudiation and entity authentication.**  **And more** | **Also doing this journal late** | **Doing it at the right time** |  |
| **Date**  **3.Cybercrime** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **October 20th 2021** | **In this module I read “Who are the bad guys and what do they want?” and did the two “online sessions”, which involved topics such as: cybercrime statistics, some common forms of cyber attacks, the cyber kill chain and why systems cannot be 100% secure** | **I missclicked on some of the quiz questions lol** | **Just dont** |  |
| **Date**  **4. Risk Assessment, Management & Governance (1)** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **October 21st 2021/journal submitted on 28th october 2021** | **Information security risk management, assessment, mitigation, identification, analysis and control.**  **Classifying threats and risk.**  **Risk appetite/tolerance.**  **Residual risk.**  **GDPR vs DPA.** | **Journal submission a week after doing the module** | **yes** |  |
| **Date**  **5. Risk Assessment, Management & Governance (2)** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **28th october 2021** | **Information security risk concepts and management.**  **Risk appetite and tolerance.**  **Risk evaluation, attitude, aversion.**  **Attacker groups and motivations.**  **Difference between information security policies, standards, procedures and guidelines.**  **Infosec business resilience concepts.** | **The interactive web module whatever you want to call them are like half broken most of the time and it wont let me click stuff** | **I wish there was one :(** |  |
| **Date**  **6. Security Testing & Vulnerability Assessment** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **28th october 2021** | **Security testing. Pentesting.**  **Threats, vulnerabilities, attacks.**  **Vulnerability assessment**  **legal requirements for pentesting.**  **Asset inventory, information management, risk assessment, vulnerability assessment, reporting and remediation tracking, response planning.**  **Malware scanning** | **One of the videos in one of the module things is dead.** | **Resurrect it with magic** |  |
| **Date**  **7. Digital Forensics** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **28th october 2021** | **Incident management.**  **Concepts of forensic examination such as phases of an investigation, preparing evidence for presentation.**  **Digital forensic examination procedures. Digital crime scene investigation. Forensic examination codes of conduct** |  |  |  |
| **Date**  **8. Incident Response Management** | **What I have learnt from this module** | **0Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **23th november 2021** | **Information security anomalies.**  **Detection of infosec anomalies. Automatic anomaly detection.**  **Reviewing system log files.**  **Analysing infosec anomalies.**  **Infosec incident response.**  **Network analysis/monitoring.**  **Service level agreements.**  **threat/vulnerability databases.**  **Information security incident concepts.**  **Incident management.**  **Stages of incident management** |  |  |  |
| **Date**  **9. Identity & Access Management (Authentication, Authorisation & Accountability)** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
| **7th december 2021** | **Identity and access management.**  **open standards.**  **OpenID authentication.**  **provisioning for IAM.**  **Authentication vs authorisation.**  **Entitlement management.**  **Types of access control.**  **Privacy policies.**  **MFA.** | **There isnt a right answer on this question lol** |  |  |
| **Date**  **10. Security Audit, Compliance & Assurance** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**  • Key elements of learning from the module  • How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
|  | **The meaning of information security governance and management.**  **Difference between infosec policies, standards, procedures and guidelines.**  **Conducting audits.**  **Importance of confidentiality in an audit.**  **Different kinds of audits.**  **Audit methodologies.**  **OPSEC.**  **Information security management systems.** |  |  |  |
| **Date**  **11. Specialist Modules**  **(Choose at least 1)**   * **Human Aspects of Cyber Security** * **Pen Testing** * **Software Security & Architecture** | **What I have learnt from this module** | **Problems Encountered** | **Potential Solution** | **Reflection**   * Key elements of learning from the module * How the learning from this module has impacted your learning – e.g. caused you to examine further a particular issue |
|  | **Specialist module B:**  **Threat vs vulnerability vs risk**  **What vulnerability assessments are**  **What penetration testing is**  **black vs grey vs white box testing**  **The legal requirements for performing penetration testing (letter of agreement, scope)**  **The need for confidentiality**  **Some tools which are used for penetration testing** |  |  |  |

Overall Journal Reflection

Briefly summarise the top five elements of learning from your completion of all of the modules and explain why. Evaluate the extent the Moodle learning has had on your skills and knowledge. Which specific parts of the Modules made more sense to you and had a greater impact on your learning? Summarise which aspects of the Module content you found particularly useful and why.