A picture containing text, electronics

Description automatically generated

Cardiff School of Technologies

### Assessment

### Brief

|  |  |
| --- | --- |
| Module Code | Module Title |
| DAT4009 | Fundamentals of Cyber Security |
| Academic Year | Semester |
| 2023- 2024 | 1 |
| Module Leader email | |
| eaukwandu@cardiffmet.ac.uk | |

Content

[Assessment Details 2](#_Toc67665314)

[Submission Details 3](#_Toc67665315)

[Assessment Criteria 3](#_Toc67665316)

[Further Information 5](#_Toc67665317)

[Who can answer questions about my assessment? 5](#_Toc67665318)

[Referencing 5](#_Toc67665319)

[Submission problems 5](#_Toc67665320)

[Unfair academic practice 5](#_Toc67665321)

[How is my work graded? 6](#_Toc67665322)

# Assessment Details

|  |  |  |
| --- | --- | --- |
| Assessment title | Abr. | Weighting |
| **Fundamentals of Cyber Security** | **WRIT1** | **50%** |
| Pass marks are 40% for undergraduate work and 50% for postgraduate work unless stated otherwise. | | |

|  |  |
| --- | --- |
| Task/assessment brief: | |
| **WRIT1 – 100% (Individual Report 2000 words equivalent)**  **Use Case One - Confidentiality**  Confidentiality aims to prevent unauthorised access or reading of information. XYZ is a specialised online banking platform dedicated to people with disabilities. Because of this, you were hired to provide a business proposition of a specialised end-user authentication system that will be suitable for these special need customer base.  **Mark: 20%**  Because of the prevailing law, the bank would also want to make sure that no customer is able to read or know other customer’s account information. What type of cryptography suite would you recommend for XYZ knowing that this is an online banking platform? State reasons and merits for using these suites. This will cover all states of data – in process, in motion and at rest.  **Mark: 20%**  **Use Case Two – Integrity**  NIST defines integrity of information as guarding against improper information modification and includes ensuring information non-repudiation and authenticity. Define these concepts in your own words and provide algorithm or technique that XYZ online bank will use to prevent against **improper modification,** ensure **non-repudiation and authenticity** on customer’s bank account entrusted to them. Provide citations and references of secondary sources used.  **Mark: 20%**  A function used in achieving information integrity can be attacked, how is the attack achieved and what are the ways of resolving it? Provide citations and references of secondary sources used to substantiate your positions and solutions.  **Mark: 10%**  **Use Case Three – Availability**  Denial of service (DoS) or distributed denial of service (DDoS) attacks are a relatively recent concern for XYZ as such attacks try to reduce access to information. As a result of the rise in DoS/DDoS attacks, data availability has become a fundamental issue in many related organisations and competitors. Therefore, Availability is a concern for XYZ online bank.  To avoid losing her customers, XYZ has asked you to offer about 6 solutions or services that will ensure at least between 97% - 99% uptime of their site. Use table to itemise the solutions or services and provide reasons for their choices. Provide citations and references of secondary sources used.  **Mark: 30%**  **Instructions:**  Students are to submit their work using CST Written Report Submission template. | |
| Word count (or equivalent): | 2000 words equivalent |
| This a reflection of the effort required for the assessment. Word counts will normally include any text, tables, calculations, figures, subtitles, and citations. Reference lists and contents of appendices are excluded from the word count. Contents of appendices are not usually considered when determining your final assessment grade. | |

|  |
| --- |
| Academic or technical terms explained: |
| Cyber Security is a compound word used to describe processes, technologies and protocols used in securing IT and OT hardware, and software systems from unauthorised access, harm, and malicious acts. It also involves process of educating peopleware from being the weakest link for carrying our malicious acts in an organisation. |

# Submission Details

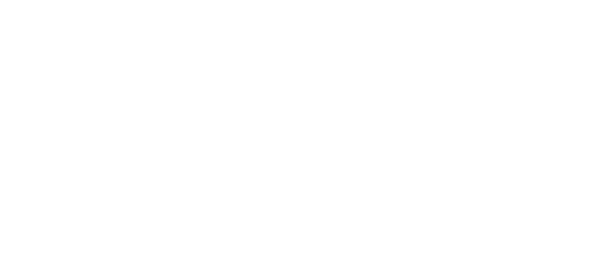
|  |  |  |  |
| --- | --- | --- | --- |
| Submission Deadline: | This will be on week 7 and will be provided on the Moodle submission point. | Estimated Feedback  Return Date | This will normally be 20 working days after initial submission. |
| Submission  Time: | By 4.00pm on the deadline day. |  | |
| Moodle/Turnitin: | **Any assessments submitted after the deadline will not be marked and will be recorded as a non-attempt unless you have had an extension request agreed or have approved mitigating circumstances. See the School Moodle pages for more information on extensions and mitigating circumstances.** | | |
| File Format: | The assessment must be submitted using the specified file format for each Part and submit through the Turnitin submission point in Moodle.  **Your assessment should be titled with your:**  **student ID number, module code and assessment ID,**  **e.g. st12345678 BHL5007 WRIT1** | | |
| Feedback | Feedback for the assessment will be provided electronically via Moodle. Feedback will be provided with comments on your strengths and the areas which you can improve. View the [guidance](https://learn.cardiffmet.ac.uk/mod/glossary/showentry.php?courseid=8107&eid=9581&displayformat=dictionary) on how to access your feedback.  All marks are provisional and are subject to [quality assurance processes](https://outlookuwicac.sharepoint.com/:b:/s/QED/Ec3kYQQeEHdKrCbo_tJnr2kBomIiiLINmPebUgvTUljq9Q?e=a0G2z5) and confirmation at the programme Examination Board. | | |

# Assessment Criteria

|  |
| --- |
| Learning outcomes assessed |
| |  | | --- | | **Learning Outcomes** | | [LO1] Appraise and apply fundamentals of information security including CIA triad.  [LO2] Evaluate and apply risk assessment and management principles.  [LO3] Analyse business continuity, incident response and recovery planning  [LO4] Demonstrate an understanding of laws, regulations.  [LO5] Apply privacy and online rights in different contexts.  [LO6] Demonstrate an understanding of the importance of human centred security requirements.  [LO7] Reflect on their own personal development within the module. |  |  |  | | --- | --- | | **Assessment Criteria** | **100%** | | Individual Report (The breakdown of the allocated marks on each task are detailed above) - (**LO1, LO6, LO7)** | 100% | | **Total** | 100% | |
| Other skills/attributes developed  This includes elements of the Cardiff Met EDGE (Ethical, Digital, Global and Entrepreneurial skills) and other attributes developed in students through the completion of the module and assessment. These will also be highlighted in the module guidance, which should be read by all students completing the module. Assessments are not just a way of auditing student knowledge. They are a process which provides additional learning and development through the preparation for and completion of the assessment. |
| |  |  |  |  | | --- | --- | --- | --- | | Ethical | Students will be taught the ethics of cyber security, existing laws, the guiding principles, and standards. | Students will be taught the ethics of Forensics and the guiding principles of NIST digital forensics process. | … | | Digital | The teaching will be conducted using the state-of-the-art tools in cyber security, and their implementations. | The usage of state-of-the-art in Forensics Science will be taught and implemented. | … | | Global | The tools to be used in teaching and learning and workshop practises are the universally tested and accepted tools in cyber security. | The tools to be used in teaching and learning and workshop practises are the universally tested and accepted tools in Forensic Science. | … | | Entrepreneurial | The teaching, learning and demonstration of how cyber security can be achieved in an industry will be carried out and hands-on practises will follow industry standards. This will provide the student employability skills as well as the capability of solving problems that could lead to a commercial spin-out. | The teaching, learning and demonstration of how forensic investigations are carried out and hands-on practises will follow industry standards. This will provide the student employability skills as well as the capability of solving problems that could lead to a commercial spin-out. | … | |

|  |
| --- |
| Marking/Assessment Criteria |
| |  |  | | --- | --- | | **Mark Classification** | **Criteria** | | **70 – 100%**  **(1st)** | The ability to demonstrate excellent knowledge of CIA triad and their different phases of implementation on human centred security. | | **60-69%**  **(2:1)** | The ability to provide good report on CIA triad and their different phases of implementation on human centred security. | | **50-59%**  **(2:2)** | Fair report on CIA triad and their different phases of implementation on human centred security. | | **40-49%**  **(3rd)** | Limited report on CIA triad and their different phases of implementation on human centred security. | | **<40%**  **(Fail)** | Poor report on CIA triad and their different phases of implementation on human centred security. | |
| Further Information on assessment, referencing and grading can be found in the Module Handbook (on Moodle) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **WRIT 1 Main** | | | | | |
| **Part 1: Confidentiality**  **File formatting information:**  Font face: Times New Roman  Size: 12  Justification: Full  Any Figure/Table used should be labelled appropriately and referenced in the body of the text.  All secondary information used must be cited and referenced. All files must be submitted using the specified file format and naming convention. | (Fail <40) There is an attempt at providing report on the knowledge of confidentiality and the implementation on human centred security.  0-19 points | (40-49) Providing limited information on the knowledge of confidentiality and the implementation on human centred security.  20-24 points | (50-59) Providing fair information on confidentiality and the implementation on human centred security.  25-29 points | (60-69) Providing good and complete information on confidentiality and the implementation on human centred security.  30-34 points | (70-100) Providing excellent and complete information on confidentiality and the implementation on human centred security.  35-50 points |
| **Part 2:**  **Integrity**  **File formatting information:**  Font face: Times New Roman  Size: 12  Justification: Full  Any Figure/Table used should be labelled appropriately and referenced in the body of the text.  All secondary information used must be cited and referenced. All files must be submitted using the specified file format and naming convention. | (Fail <40) There is an attempt at providing requisite information on how to ensure the integrity of an information received and the implementation on human centred security.  0-11 points | (40-49) The student provided limited information on how to ensure the integrity of an information received and the implementation on human centred security.  12-14 points | (50-59) The student provided fair information on how to ensure the integrity of an information received and the implementation on human centred security.  15-17 points | (60-69) The student provided good and comprehensive information on how to ensure the integrity of an information received and the implementation on human centred security.  18-20 points | (70-100) The student provided excellent, comprehensive, and easy to follow information on how to ensure the integrity of an information received and the implementation on human centred security.  21-30 points |
| **Part 3: Availability**  **File formatting information:**  Font face: Times New Roman  Size: 12  Justification: Full  Any Figure/Table used should be labelled appropriately and referenced in the body of the text.  All secondary information used must be cited and referenced. All files must be submitted using the specified file format and naming convention. | (Fail <40) There is an attempt at providing requisite information on how to ensure the availability of an information system and the implementation on human centred security.  0-7 points | (40-49) The student provided limited information on how to ensure the availability of an information system and the implementation on human centred security.  8-9 points | (50-59) The student provided fair information on how to ensure the availability of an information system and the implementation on human centred security.  10-11 points | (60-69) The student provided good and comprehensive information on how to ensure the availability of an information system and the implementation on human centred security.  12-13 points | (70-100) The student provided excellent, comprehensive, and easy to follow information on how to ensure the availability of an information system and the implementation on human centred security.  14-20 points |
| Very poor = a report that failed at providing requisite information, full of errors and failed to follow nearly all the instructions. Limited = Report contains fewer requisite information and has some errors as well as missed out majority of the instructions. Fair = A report that contains an average level of information, has some minor errors, and missed out on some instructions. Good = a report that contains majority of the information needed, has little or no errors and followed nearly all the instructions. Excellent = Report followed all the instructions and contains all the required information. | | | | | |

A picture containing text, electronics, circuit

Description automatically generated