UWE Bristol University of the West of England

Computer Science and Creative Technologies

Coursework Specification

Module Details

Module Code	UFCFWN-15-M
Module Title	Information Risk Management
Module Leader	Tom Barnes
Module Tutors	Tom Barnes, Ahsan Ikram, Eirini Kalaitzopoulou
Year	2020-21
Component/Element Number	CW1/2
Total number of assessments for this module	1 coursework + 1 Presentation
Weighting	100%
Total Assignment Time	25 hours
Element Description	Written Report (3000 words) Weighting - 75% 10 Minute PowerPoint Presentation (videoed) – Weighting 25%

Dates

Date issued to students	9 June 2021
Date to be returned to students	CW1 Report 2 September 2021 CW2 Presentation 20 September 2021
Submission Date	CW1 Report 5 August 2021 CW2 Presentation 19 August 2021
Submission Place	Blackboard
Submission Time	14:00
Submission Notes	

Feedback

Feedback provision will be	Written feedback via Blackboard / MyUWE

Due Date: Thursday 5th August 2021 (report) & Thursday 19th August 2021 (presentation)

UWE Bristol University of the West of England

Contents

Section 1: Overview of Assessment

This assignment assesses the following module learning outcomes:

1. To form a deep and systematic understanding of why cyber security matters, both in terms of the importance on business operations and on our modern society.
2. To apply relevant techniques such as ISMS and FAIR, to formulate effective solutions for Risk Management.
3. To analyse a broad range of real-world security issues that face commercial organisations and other institutions.
4. To identify the shortcomings of real-world security incidents and evaluate and critique how ISMS and FAIR can be utilised to help better inform decisions and mitigate risks.
5. To develop critical reflection skills and analyse of self in the context of proposing suitable ISMS strategy, and to further independent learning ability required for continuing professional development.

The assignment is worth ***100%*** of the overall mark for the module.

Broadly speaking, the assignment requires you to produce a 3000-word report that provides a critical reflection on a real-world security incident, with evidence of risk assessment using suitable methodologies, and how this can inform mitigation of future incidents. The assignment also requires the delivery of a 10-minute presentation to disseminate the findings reported in your journal article, to address the role of Information Risk Management to the wider organisation.

The assignment is described in more detail in section 2. This is an individual assignment.

Working on this assignment will help you to develop your knowledge and understanding of applying risk methodologies to resolve real-world security incidents. It will also help to develop your critical thinking skills for identifying appropriate mitigation strategies to avoid future security incidents. If you have questions about this assignment, please post them to the discussion board “Information Risk Management Assignment” on Blackboard.

Section 2: Task Specification

Part 1 (worth 75% towards the final grade):
Produce a 3000-word report to address a case study of information risk management, informed by a real-world security incident and demonstrating concepts of IRM.

For this assignment, you are expected to present a case study for a chosen organisation, informed by a real-world security incident, and provide a narrative that presents a risk assessment and a critical reflection in the form of a journal article. The article will need to address the following aspects:

- Description of the chosen industry and why IRM is important in the given context. This should be justified based on evidence from other related real-world security incidents, with discussion as to why these are significant risk indicators.
- Identification of key assets and personnel within the organisation, with discussion on information asset valuation and relevant risk methodologies (ISMS and FAIR).
- Examples of risk analysis using appropriate methodology to illustrate the potential impact on the chosen organisation. You will need to justify how you derive quantitative and qualitative values for risk assessment.
- Critical reflection on appropriate treatment strategies that address the identified risks, with strong justification for the decisions taken.

You are expected to draw on both ISO27000 and FAIR as discussed within the module to justify your analytical approach in assessing the security incident. You will need to conduct further research into both of these methodologies, beyond the provided lecture material. Your critical reflection should also reflect on your choice of risk methodology, and their relative strengths and limitations.

The report should be written as a journal article for a professional audience using the IEEE template, provided on Blackboard. The article is expected to be no more than 3000 words, please refer to the UWE word count policy: *http://www1.uwe.ac.uk/aboutus/policies.aspx*

Part 2 (worth 25% towards the final grade):
Prepare an individual videoed PowerPoint presentation for a CEO pitch that reports your findings

The presentation should be considered as a pitch to the CEO to impress the importance and relevance of information risk management for the chosen organisation. You should draw on real-world security incidents in the context of your chosen organisation. You should expand beyond what is included in the report to provide greater detail if deemed necessary. The presentation should be delivered as a videoed PowerPoint presentation. The presentation should be designed so that it can be delivered within a time of **10 minutes**. This contributes towards 25% of the module’s assessment.

Section 3: Deliverables

Part 1: A written report is to be submitted via Blackboard by Thursday 5th August 2021 in either DOC or PDF format.

Part 2: A **10-minute** videoed PowerPoint presentation is to be prepared. This should be submitted via Blackboard by Thursday 19th August 2021.

Section 4: Marking Criteria

The marking criteria for both the journal article and the report can be found on the next page:

Due Date: Thursday 5th August 2021 (report) & Thursday 19th August 2021 (presentation)

Part 1: Report (Contribution of each marking component is shown)

	0-29	30-39	40-49	50-59	60-69	70-84	85-100	Mark & Feedback
Description of organisation, importance of IRM, and analysis of real- world security incident (20%)	Little or no evidence of research related to a real-world security incident or why IRM is important for the chosen organisation	Some evidence of research related to a real-world security incident and why IRM is important for the chosen organisation, however lacking significant details	A real-world security incident has been identified with key details being discussed. IRM is discussed for the chosen organisation	A real-world security incident has been identified, with some discussion on why the incident occurred. IRM is discussed for the chosen organisation	A well-detailed real-world security incident has been identified, with some discussion on why the incident occurred and how this could have been mitigated. IRM is well-justified for the chosen organisation	A well-detailed real-world security incident has been identified, with good discussion on why the incident occurred and how this could have been mitigated IRM is well-justified for the chosen organisation	A well-detailed real-world security incident has been identified, with excellent discussion on why the incident occurred and justification of how this could have been mitigated. Excellent justification for IRM for the chosen organisation	
Application of ISMS AND FAIR in context of the organisation (20%)	Little or no discussion on the use of an ISMS and FAIR	Some discussion on the use of an ISMS and FAIR, however lacking in details	Discussion on the use of an ISMS and FAIR, however little application to organisation	Discussion on the use of an ISMS and FAIR with application to the organisation, but at a fairly basic level.	Discussion on the use of an ISMS and FAIR with a good discussion on the application to the organisation.	Good discussion on the use of an ISMS and FAIR with the justification of how this can apply to the organisation.	Excellent discussion on the use of an ISMS and FAIR with the strong justification of how this can apply to the organisation.	
Analysis of Identified Risks, and proposal of treatment strategies (30%)	No attempt at identifying or analysing risks	Identification of some risks, with limited analysis.	Identification of some risks, with some basic analysis and treatment strategies	Identification of a variety of risks, with analysis and detail of treatment strategies	Identification of a variety of risks, with clear analysis and good detail of treatment strategies	Identification of a broad variety of risks, with clear analysis and good detail of treatment strategies	Identification of a broad variety of risks, with excellent analysis and strong justification of treatment strategies choices	
Critical reflection of appropriate security controls and legislation (20%)	No evidence of critical reflection on security controls and legislation	Limited evidence of critical reflection on security controls and legislation	Some discussion about the choice of security controls and legislation	Discussion about the choice of security controls and relevant legislation, with some evidence of critique	Good discussion about the choice of security controls and relevant legislation, with some evidence of critique	Good discussion about the choice of security controls and relevant legislation, with strong evidence of critique	Excellent discussion about the choice of security controls and relevant legislation, with strong evidence and justification of critique	
Report Presentation (10%)	Poor presentation	Weak presentation	Fair presentation	Good presentation but with some grammatical errors	Good presentation with minor errors	Excellent presentation but with minor errors	Excellent presentation	

Part 2: Presentation (Contribution of each marking component is shown)

	0-29	30-39	40-49	50-59	60-69	70-84	85-100	Mark & Feedback
Demonstration of knowledge and understanding of the real-world security incident (30%)	Little or no discussion on a real-world security incident	Limited discussion on a real-world security incident	Some discussion on a real-world security incident	Discussion on a real-world security incident with some detail regarding threats, vulnerabilities, risks, and impact	Discussion on a real-world security incident with good detail regarding threats, vulnerabilities, risks, and impact, and CIA principles	Discussion on a real-world security incident with excellent detail regarding threats, vulnerabilities, risks, and impact, and CIA principles	Discussion on a real-world security incident with excellent detail regarding threats, vulnerabilities, risks, and impact, and CIA principles	
Demonstration of knowledge and understanding of information risk management (30%)	Little or no discussion on IRM	Limited discussion on IRM	Some discussion on IRM	Some discussion on IRM, making clear the stages of implementing an IRM	Discussion on IRM, making clear the stages of implementing an IRM, and application of this to the chosen organisation	Discussion on IRM, making clear the stages of implementing an IRM, and good application of this to the chosen organisation	Discussion on IRM, making clear the stages of implementing an IRM, an excellent application of this to the chosen organisation	
Extension of the material presented in the report **(30%)**	Presentation contains no extension to the report	Presentation contains limited extension to the report	Presentation contains some extension to the report	Presentation is appropriately pitched at audience with some evidence of extending the report	Presentation is appropriately pitched at audience with evidence of extending the report	Presentation is appropriately pitched at audience with good choices of how to extend the original report	Presentation is appropriately pitched at audience with excellent choices of how to extend the original report	
Presentation clarity, timing, and delivery including the use of Presenter Notes **(10%)**	Presentation is poorly delivered and lacks in clarity	Presentation is weak but lacks in clarity	Presentation is fair and some clarity	Presentation is fair but clarity of content is clear	Presentation is good and clarity of content is clear	Presentation is excellent and clarity of content is good	Presentation is excellent and clarity of content is excellent	