|  |  |  |  |
| --- | --- | --- | --- |
| **COMP1843 (2022/23)** | **Principles of Security** | **Faculty Header ID: 11775** | **Contribution: 100% of the course** |
| **Module Leader: Dr Irfan Chishti** | **Risk Assessment (Information Security)** | | **Deadline Date:** |
| This coursework should take an average student who is up-to-date with tutorial work approximately 50 hours  Feedback and grades are normally made available within 15 working days of the coursework deadline | | | |
| **Learning Outcomes:** On completing this course successfully you will be able to: 1. Understand information systems threats, vulnerabilities and risks 2. Understand the management of creating/maintaining a security policy 3. Appraise methods of deployment of security controls/methods/technologies 4. Determine courses of action to solve problems in real-world security scenarios 5. Understand security acts and standards and codes of conduct. | | | |

|  |
| --- |
| **Plagiarism is presenting somebody else's work as your own. It includes: copying information directly from the Web or books without referencing the material; submitting joint coursework as an individual effort; copying another student's coursework; stealing coursework from another student and submitting it as your work.  Suspected plagiarism will be investigated and if found to have occurred will be dealt with according to the procedures set down by the University. Please see your student handbook for further details of what is/isn't plagiarism.** All material copied or amended from any source (e.g. internet, books) must be referenced correctly according to the reference style you are using.  Your work will be submitted for plagiarism checking.  Any attempt to bypass our plagiarism detection systems will be treated as a severe Assessment Offence. |

#### **Coursework Submission Requirements**

* An electronic copy of your work for this coursework must be fully uploaded on the Deadline Date using the link on the coursework Moodle page for COMP1843.
* For this coursework, **you must submit a single PDF document**.  In general, any text in the document must not be an image (i.e. must not be scanned) and would normally be generated from other documents (e.g. MS Office using "Save As .. PDF"). An exception to this is the handwritten mathematical notation, but when scanning does ensure the file size is not excessive.
* There are limits on the file size (see the relevant course Moodle page).
* Make sure that any files you upload are virus-free and not protected by a password or corrupted otherwise they will be treated as null submissions.
* Your work will not be printed in colour. Please ensure that any pages with colour are acceptable when printed in Black and White.
* You **MUST NOT** submit a paper copy of this coursework.
* Coursework must be submitted as above. Under no circumstances can they be accepted by academic staff

The University website has details of the current Coursework Regulations, including details of penalties for late submission, procedures for Extenuating Circumstances, and penalties for Assessment Offences, click the link below for further information

<https://www.gre.ac.uk/policies/undergraduate-and-postgraduate-taught>

#### **Detailed Specification**

**Scenario:**

**LiveWell** provides physiotherapy services to the local community in southeast London and has four clinics. They have recently opened two more clinics aiming to cater for the diverse needs of the community. Their trained staff uses state-of-the-art technology and systems to provide physiotherapy services to local patients. The management has seen a steady influx of new patient enquiries from local medical practices and registrations in the first few months of the opening of new clinics.

**LiveWell** management has invested heavily in their infrastructure including a newly developed web portal and launched marketing campaigns for brand awareness etc. through their web systems and Google adverts to reach out to a wider community, These efforts have resulted in more new patients showing interest from nearby localities. This surge has shown some shortcomings in **LiveWell** operations.

**LiveWell** web portal is interconnected with a few data servers and systems for their clinic's smooth operations, e.g., patients’ referrals, appointments or other related services, and online physiotherapy consultations. The main data server accommodates the current and new patients’ personal and medical data to furnish their needs.

**LiveWell** is a moderate size start-up of 50 staff members and mainly relies on the admin team using the systems for entire patient-facing communication through face-to-face provision within their clinics. Besides, the newly developed resource, i.e., web portal has been added to assist the admin team to direct their patients to it for promotional information. The teams, i.e., admin and physiotherapists, work in shifts with no clear separation of responsibilities concerning communication with the patients, recording patients’ recommendations made to patients, changes made to patients’ dataetc. Furthermore, the influx of new patients and lack of staff training in new systems makes **LiveWell** more susceptible to attacks, and wouldn’t be able to sustain its service levels well.

**LiveWell** has limited security measures implemented for their systems, software and hardware, i.e., log in etc, Due to a lack of information security measures, recently they have been plagued with viruses in their main data server which corrupted their mailing list and sent incorrect information regarding offers and promotions to its registered patients. As a result, to the management’s surprise, patient complaints have risen.

For the sustainable operations and safeguarding information security of their patients’ and organisational data and their specialised services, **LiveWell** would like to call upon your consultancy services seeking guidance and recommendations. They would like you to determine the risks, and their impact on their business presenting them with possible solutions for the risks perceived in the current and near future. However, they feel secure concerning their physical security using locks and alarms.

## Assessment Specifications

This is an individual assessment and the report **word limit is 3000**. The word length includes the title of the report, text, diagrams, charts and tables, as well as footnotes, but does not include appendices and references. Your report should not **exceed** the **maximum word count** and no minimum word count is required but in cases significantly below the suggested word count is unlikely to meet **Pass criteria**. **No penalty** is incurred for **less than 5%** over the word limit. However, **2 marks** will be deducted for **every 5%** over the word limit, **up to a total of 20 marks** (50% of the total word count). After 50% over the word limit, **3 marks** will be deducted for **every 5%**

You are required to perform a risk assessment that should include relevant assumptions, identification and differentiation of threats and vulnerabilities and their impact on the business proposing risk control strategies based on current market research within the healthcare sector achieving assessment outcomes 1, 2, 3, 4 and 5.

**Deliverables**

You **MUST** produce a **report** of **3000** words containing the following:

* A title page and a table of contents mentioning the number of words used.
* A **management summary** of the report including a brief of all the sections and the conclusion.
* A **Risk Identification** section introducing the case supported by your **assumptions** clearly, that further includes the following
  + Critically evaluate the **vulnerabilities** faced by the organisation, based on your assumptions.
  + Critically evaluate **threats** anticipated by the organisation. This should be based on current research on the security trends in the news about SMEs.
* Critically evaluate the **assets** identified with the help of the **weighted factor analysis technique**.
  + Create a **risk register** with **risks prioritised** and provide a critique of the risk probabilities and their impact.
* Suggest suitable **risk control strategies** and provide a critique on how the identified control strategies could help the organisation based on your risk evaluation (score).
* The **conclusion** section should contain the summary of the report along with any further recommendations.
* The report should be supported by appropriate and relevant research documented using the **Harvard style of Referencing (in-text citation)**.

**Marking Scheme**

1. **Report Structure & Layout (5%):**

The report **MUST** be organized with a clear **title page specifying a relevant title of the report, and a table of contents** (using MS Word TOC facility and **NOT** manual) presenting the total number of used The report **MUST** be written in **third person format** supported by **good Grammar and presented professionally.**

1. **Management Summary (10%):** A section synthesizing the key points of the overall report for the management.
2. **Risk identification (20%):** This section should be used to state your **Assumptions** addressing the following
3. Identify the **vulnerabilities** faced by the organisation, based on your assumptions. **(10%).**
4. What kinds of **threats** should **LiveWell** anticipate? This should be based on current research on the security trends of **SME**s **(10%).**
5. **Risk Management (30%):** This section should address the following
6. Identify the assets with the help of the weighted factor analysis technique and critically evaluate them **(15%).**
7. Create a risk register with risks prioritised supported by a discussion highlighting the reasons behind your prioritised list of assets **(15%).**
8. **Risk Control Strategies (20%):** This section should include recommendations of possible controls based on the research to reduce the risks (from risk identification and management sections) involved.
9. **Conclusion (10%):** Summary of main points

**References (5%):** Harvard referencing style **MUST** be applied throughout the report (in-text citation).

**Grading Criteria:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria for Assessment** | **0-29% Fail** | **30-39% Fail** | **40-49% Satisfactory** | **50-59% Good** | **60-69% Very Good** | **70-79% Excellent** | **80-100% Exceptional** |
| **Understanding, Knowledge of IS threats and Controls** | Demonstrated a little or no understanding of one or more of the following; information security. risk identification & management and risk control strategies. There is very little evidence of engagement with the key elements. | Demonstrated a poor understanding of one or more of the following - information security, risk identification & management and risk control strategies. There is insufficient evidence of engagement with the key elements. | Demonstrated a satisfactory level of understanding of IS, risk identification & management and risk control strategies. There are a few notable omissions and limited evidence of engagement with all key elements. | Demonstrated a good level of understanding of information security, risk identification & management and risk control strategies. There is also some good evidence of engagement with most key elements with some omission of detail. | Demonstrated a very good systematic understanding of information security, risk identification & management and risk control strategies. There is very good evidence of engagement with all key elements. | Demonstrated an excellent systematic understanding of information security, risk identification & management and risk control strategies. There is excellent evidence of engagement with all key elements. | Demonstrated an exceptional systematic understanding of information security, risk identification & management and risk control strategies. There is exceptional evidence of engagement with all key elements. |
| **Research & Evaluation** | Demonstrated little or no use of research skills to undertake a critical analysis of infosec with recommendations that are irrelevant, very weak and inadequate. | Demonstrated a little use of research skills to undertake a critical analysis of infosec with recommendations that are mostly irrelevant and lack in detail. | Demonstrated a satisfactory level of research skills to critically analyse some of the infosec issues with a satisfactory level of some mitigating recommendations. | Demonstrated some good use of research skills to critically analyse infosec issues with recommendations to mitigate most of the identified problems. | Demonstrated a very good use of research skills to critically analyse infosec issues with recommendations for mitigating identified problems. | Demonstrated an excellent use of research skills to critically analyse infosec issues with recommendations for mitigating identified problems. | Demonstrated an exceptional use of research skills to critically analyse infosec issues with recommendations for mitigating identified problems. |
| **Communication, Organisation and Presentation** | Demonstrated a very poor use of argument and language to communicate with the target audience. The structure and flow of the report are unacceptable with significant presentation issues. | Demonstrated a poor use of argument and language to communicate with the target audience. The structure and flow of the report are unacceptable with significant presentation issues. | Demonstrated a satisfactory use of argument and language to communicate with the target audience. The structure and flow of the report have some presentation issues | Demonstrated a good use of argument and language to communicate with the target audience. The structure and flow of the report are mostly coherent and the overall quality is good. | Demonstrated a very good use of argument and language to effectively communicate with the target audience. The structure and flow of the report are of a very good quality | Demonstrated an excellent use of argument & language to effectively communicate with the target audience. The structure and flow of the report are of excellent quality. | Demonstrated an exceptional use of argument and language to effectively communicate with the target audience. The structure and flow of the report are of exceptional quality. |
| **Referencing** | Little or no cited work. The references may not be sufficient or appropriate or the most recent. | The references cited using some or no Harvard style reflects a poor understanding of the referenced sources The references may not be sufficient/appropriate/most recent. | Demonstrated a satisfactory use of sources employing an inconsistent Harvard style. Some references may not be the most recent or relevant. | Demonstrated a good use of sources employing Harvard style reflecting a good understanding of the referenced sources. Some references may not be the most recent. | Demonstrated a very good use of a variety of sources employing Harvard style reflecting a very good understanding of cited sources. | Demonstrated an excellent use of a variety of sources employing Harvard style reflecting an excellent understanding of cited sources. | Demonstrated an exceptional use of a variety of sources employing Harvard style reflecting a thorough understanding of cited sources. |
| **Graduate Employability** | There is little or no evidence of the qualities of transferrable skills necessary for employment. | There is little evidence of the qualities of transferrable skills necessary for employment. | There is satisfactory evidence of the qualities of transferrable skills necessary for employment. | There is good evidence of the qualities of transferrable skills necessary for employment. | There is very good evidence of the qualities of transferrable skills necessary for employment such as personal judgement and mostly successful experimentation. | There is excellent evidence of the qualities of transferrable skills necessary for employment such as personal judgement and successful experimentation. | There is exceptional evidence of the qualities of transferrable skills necessary for employment such as personal judgement and successful experimentation. |