IS Audit Report

Important note:

- This is an <u>individual</u> assignment. You <u>must</u> complete the task <u>independently</u>. If you submit a report that is similar to any of your classmate's reports it will be considered academic misconduct.
- Refer to the Macquarie University Academic Integrity Policy and associated documents.

Estimated student workload: 30 hours

Task

Many organisations have recently suffered from data breaches that resulted in exposure of confidential customer data. A breach of such sensitive data hurts the organisation's reputation and causes significant financial losses.

In this assignment, you will write a report on a data breach that took place no more than 5 years ago. Your report should reference articles on the data breach incident in addition to other reliable sources.

Your role is an IS auditor. Therefore, your report should highlight the main risks that should be addressed by the management of the organisation and the controls that would have mitigated the risks.

The report should include the following:

1) Executive Summary
You will need to prepare an executive summary document (0.5-page maximum) to the Board of Directors.

2) Background to the Case
Provide the background to the organisation's business and technology environment. This is to demonstrate your understanding of the organisation's business and IS environment.

3) Problem Identification
Identify how the breach occurred, the stakeholders and the impact to the organisation

4) Audit Approach and Potential Solution
This section explains the role of the auditor in auditing the data breach. It contains the following subsections:

 I. **IS Risks**
  Identify IS risks from the data breach in the case study, including analysing the likelihood, level of risks and implications to the business.

 II. **Audit Plan, Objectives and Procedures**

Prepare an audit plan outlining the areas that you propose to audit. In addition, you will need to include audit objectives and audit procedures for each of the area(s) that you plan to audit.

III. Audit Questions and Documents

For each of the audit objectives, provide at least three examples of interview questions that you will use to gather evidence from the organisation, including naming relevant documents that you may want to obtain for the audit.

IV. Control Recommendations

Provide a set of recommendations of control mechanism(s) to mitigate for each of the IS risks. Identify the benefits of your recommendations to the organisation.

5) Conclusion

Summarise main points in the report and provide a synthesis of the key findings. Furthermore, add your reflection on whether the recommended controls could have avoided the data breach

Required

Write a report that addresses all of the above sections.

- Format requirements: "Times New Roman" size 12 with 1.5 line spacing, approximately 1500-2000 words in total (not including references). You must include the total of words used in your report. The report should have appropriate headings and subheadings (including an introduction and conclusion).
- You must acknowledge the use of the work of others (e.g. the academic journal articles on which your report is based) using the Harvard referencing style (see http://www.lib.mq.edu.au/research/referencing.html). Any ideas or quotations must be correctly cited in the body of your report and a reference list must be provided at the end of your report.
- Once you have submitted your report, check the originality report in turn-it-in and ensure similarity with other sources is referenced. You can resubmit your report until the due date.
- Please note that the originality report for a resubmission takes 24 hours to be produced. Please ensure that you allow adequate time, if you are considering resubmission.
- Review the marking rubric on the following page so that you understand the expected standards and how you will receive feedback.

Submission

- Students will need to upload their assignment to http://ilearn.mq.edu.au (Turn-it-in) by 11:59 pm of Friday 24th April (week 7). Otherwise your assignment will be considered late.
- Late assignment will also be submitted via Turn-it-in.

Penalties

- **Extension** • No extensions will be granted. Students who have not submitted the task prior to the deadline will be awarded a mark of 0 for the task, except for cases in which an application for special consideration is made and approved. Please refer to https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policiesand-procedures/policies/special-consideration

- **Late Penalty** • Late tasks will be accepted up to 72* hours after the submission deadline. There will be a deduction of 20%* of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late (for example, 25 hours late in submission – 40% penalty). This penalty does not apply for cases in which an application for special consideration is made and approved.

Marking Criteria

The following criteria are how IS audit report will be marked.

	Not attempted	Fail	Pass	Credit	Distinction	High Distinction
1) Selection of the case study and risk analysis (30%)	No attempt. or The answer is copied or substantially copied from materials or other sources.	Poor selection of the case study. Report indicates poor or no understanding of the case study and its associated risks.	Good selection of the case study. Report indicates some understanding of the case study and its associated risks.	Good selection of the case study. Report indicates good understanding of the case study and its associated risks.	Good selection of the case study. Report indicates high level of understanding of the case study and its associated risks.	Good selection of the case study. Report indicates in-depth understanding of the case study and comprehensive risk analysis.
2) Critical analysis of the case, quality of audit plan and recommendation to target audience. (50%)	No attempt. or The answer is copied or substantially copied from materials or other sources.	Report indicates poor or no understanding of audit plan and inappropriate recommendation to target audience.	Report indicates some understanding of audit plan and able to provide an appropriate recommendation to target audience.	Report indicates good understanding of audit plan and able to provide multiple appropriate recommendations to target audience.	Report indicates high level understanding of audit plan and able to provide many appropriate recommendations to target audience.	Report indicates advanced understanding of audit plan and able to provide appropriate recommendations for all risks identified to target audience.
3) Structure of the text (10%)	No attempt, or The answer is copied or substantially copied from materials or other sources	Report does not follow the structure given and information is not generally clearly organised within each section.	Report mostly follows the structure given and information is generally clearly organised within each section.	Report follows the structure given and information is generally clearly organised within each section.	Report follows the structure given and information in each section is organised in a clear and logical way.	Report follows the structure given and information in each section is presented in a clear logical way that supports the overall point /argument of that section.
4) Professional presentation including formatting, spelling, grammar, referencing (10%)	No attempt, or The answer is copied or substantially copied from materials or other sources	Presentation is of a very poor standard, with numerous errors / inconsistencies.	Presentation is of a basic standard, with some formatting, spelling, grammar, referencing errors / inconsistencies	Presentation is of a good standard, with infrequent formatting, spelling, grammar, referencing errors/ inconsistencies.	Presentation is of a very good standard, with little or no formatting, spelling, grammar, referencing errors/ inconsistencies.	Presentation is of a professional standard, with little or no formatting, spelling, grammar, referencing errors/ inconsistencies.