ASSESSMENT 2 BRIEF

Subject Code and Title	SBD403 Security by Design
Assessment	Case Study
Individual/Group	Individual
Length	3,000 Words +/- 10%
Learning Outcomes	The Subject Learning Outcomes demonstrated by successful completion of the task below include: b) Administer implementation of security controls, security risk mitigation approaches, and secure design architecture principles. c) Explain Secure Development Lifecycle models and identify an appropriate model for a given situation. e) Apply security by Design industry standard principles in systems development.
Submission	Due by 11:55pm AEST/AEDT Sunday end of Module 8.
Weighting	35%
Total Marks	100 marks

Assessment Task

Create a document that advises on how to create a complete cyber security environment in an enterprise. Criticially analyse the basic requirements in conjunction with available technical and organizational cyber security methods and align them with adequate user experience. This has to be aligned with relevant industry or international standards, such as OWASP or ISO270xx.

Please refer to the Instructions for details on how to complete this task.

Context

Security (and the maintenance of security) is an issue that many companies have to consider in order to protect both corporate and user data, assets, and other general information. Breaches of this security have happened in the past, at many different levels. A breach often has many effects, affecting both the consumer and the company.

The report you produce will assess your understanding and ability to create a secure IT environment that is manageable and provides the actual users with as less burden as possible while maintaining the highest security standard possible.

Scenario

Consider you being the member of the CISO-Team (Chief Information Security Officer Team) of an enterprise with approx. 300 employees. The business of this company is

- performing data analysis for hospitals (i.e. how many diagnosises of what type)
- performing data analysis for retailers (i.e. how many products of what type). This data contains no personal data from shoppers such as credit cards.

In both instances the data is provided by the respective client. All clients and all client data is from Australia only.

Because of the sensitive nature of the hospital data, the data is stored on premise while the retail data, because of sheer size, is stored in a cloud storage. The cloud provider fulfills all necessary security standards and resides in Australia.

About 100 staff is working with the hospital data, this group is called “Doctors” and 200 with the retail data, group called “Retailers”.

Every group is organised into a “support”-team, consisting of personal assistants, group head and group vice head and then the analysts. Every 20 analysts work on the same client, there is no one working on two or more clients’ data.

The software that is being used for both groups is capable of having individual usernames and group roles. Access control for data can be set by username, group or both.

The executives of the company (CEO, CFO and CMO) as well as their PA should not have any access to the data, the IT staff only when required for troubleshooting the application or storage.

Instructions

You will be asked to write a design guide how to create a secure environment for the enterprise since the client demand information about the safety of their data. This includes addressing the following topics:

- What kind of user training is required and explain why this suggested training is required to achieve a better cyber security?
- Perform a risk assessment to identify at least 5 major risks?
- What technical and/or organisational methods can be deployed to mitigate assessed risks? Name at least four technical and two organisational methods and indicate on how to deploy them. Describe the impact on the users ability to work for each method.
- If applicable identify mandatory methods out of the list created.
- Describe if user groups and user rights need to be implemented in the
  - analysis application and
  - the basic IT system (E-Mail, PC-Login etc.)
- Create an appropriate password rule for user accounts both in the application and for general IT and administration accounts (administrator, root, etc.). Explain why you chose this rule or those rules and align that with current standards (such as NIST)
- Define the required security measures for the storage and align them with current standards
- A recommendation for a plan of action for creating and maintaining proper information security.
- A recommendation for a plan to sustain business availabilities.
- A reference to relevant security and governance standards.
- A brief discussion on service quality vs security assurance trade-off (less than 500 words).

You will be assessed on the justification and understanding of security methods, as well as how well your recommendations follow Secure by Design principles, and how well they are argued. The quality of your research will also be assessed, you may include references relating to the case, as well as non-academic references. You need to follow the relevant standards and reference them. If you chose to not follow a standard a detailed explanation of why not is required.

The content of the outlined chapters/books and discussion with the lecturer in the modules 1 – 12 should be reviewed. Further search in the library and/or internet about the relevant topic is requested as well.

Referencing

Referencing is essential for this assessment. A minimum of one reference for each topic is required for this, including at least 8 academic sources or relevant standards.

(An academic source is one that has been peer-reviewed).

Your references will be evaluated for their relevance to the case study. Remember you must ensure that your arguments and justifications are based on sound reasoning and clear relevance.

Ensure that you reference according to the appropriate APA style, for citing and referencing information, as well as all appropriate research sources.

Please see more information on referencing here: http://library.laureate.net.au/research_skills/referencing

Submission Instructions

Submit your **Assessment 2 Report** via the **Assessment** link in the main navigation menu in SBD403 Secure By Design. Please name your file in the following format: Lastname_First initial_course code_assessment number, e.g., Smith_A_SBD403_A2. The Learning Facilitator will provide feedback via the Grade Centre in the LMS portal. Feedback can be viewed in My Grades.

Academic Integrity

All students are responsible for ensuring that all work submitted is their own and is appropriately referenced and academically written according to the Academic Writing Guide. Students also need to have read and be aware of Torrens University Australia Academic Integrity Policy and Procedure and subsequent penalties for academic misconduct. These are viewable online.

Students also must keep a copy of all submitted material and any assessment drafts.

Special Consideration

To apply for special consideration for a modification to an assessment or exam due to unexpected or extenuating circumstances, please consult the Assessment Policy for Higher Education Coursework and ELICOS and, if applicable to your circumstance, submit a completed Application for Assessment Special Consideration Form to your Learning Facilitator

Assessment Rubric

Assessment Attributes	Fail (Yet to achieve minimum standard) 0-49%	Pass (Functional) 50-64%	Credit (Proficient) 65-74%	Distinction (Advanced) 75-84%	High Distinction (Exceptional) 85-100%
Knowledge and understanding of risk assessment The student must explain why a risk assessment is essential and who is responsible for that assessment.	Demonstrates a limited or no knowledge of cyber security design by: · providing not more than one risk in the risk assessment · Discussion of one or no	Demonstrates a functional knowledge of cyber security design by: · only provide two risk in the risk assessment. · Discussion of more than one but less	Demonstrates proficient knowledge of cyber security design by: · provide no more than three risks in the risk assessment · Discussion of more than three but	Demonstrates advanced knowledge of cyber security design by: · provide no more than four risks in the risk assessment · Discussion of five or more cyber	Demonstrates exceptional knowledge of cyber security design by: · provide at least five risks in the risk assessmen t · giving more than

Percentage for this criterion = 25%	cyber security methods.	than four cyber security methods.	less than five cyber security methods.	security methods.	the required six cyber security methods (the minimum number for each category still applies).
Understanding correlation between cyber security methods and user impact The list of methods (4 and 2 as chosen by the student)	Limited analysis capability • 0-2 methods mentioned and limited discussion about the user impact for each of them.	Demonstrated analysis capability • 2-3 methods mentioned and discussion about the user impact for all of	Well-developed analysis capability • 4-6 methods mentioned and discussion about the user impact for all of	Thorough analysis capability • All required method numbers mentioned and discussion about the	Highly sophisticated and creative analysis capability • mentioning more than the required number

must be evaluated about which of those are mandatory and which are not. The methods must have a description on the user impact, i.e. how much is the user affected by that method. i.e. a firewall does not restrict normal user work, a strict password regime and/or rights management does. Percentage for this criterion = 30%		them.	them.	user impact for all of them.	and extensive discussion about the user impact.
Understanding of overall ISMS	No mentioning of proper ISMS application	Mentioning primary risk assessment implementation	Mentioning risk assessment, method testing as	ISMS methods according to ISO but not implementing/for	Full ISMS cycle implemented

Percentage for this criterion =20 %		as ongoing process	ongoing process	getting one of the five stages	
Detailed knowledge about user rights management and password regimes Percentage for this criterion = 20 %	No mention of either rights management or password rules for application and IT Limited or no discussion about the reason of choosing this specific rule.	Mentioning of either rights management or password rules but not both. Limited discussion about the reason of choosing this specific rule.	Mentioning of both rights management and password rule but failing to reason for more than one.	Mentioning of both rights management and password rule with basic reasoning about the specific choice.	Mentioning of both rules with extensive reasoning on why those rules were chosen.
Correct citation of key resources, standards and evidence	Limited or no use of credible and relevant resources to support and develop ideas.	Demonstrates use of credible and relevant resources to support and develop ideas, but	Demonstrates use of credible resources to support and develop ideas.	Demonstrates use of good quality, credible and relevant resources to support and	Demonstrates use of high-quality, credible and relevant resources to support and

Percentage for this criterion = 5%	Referencing does not resemble APA, or has frequent or repeated errors.	these are not always explicit or well developed. Referencing resembles APA, with frequent or repeated errors.	Referencing resembles APA, with occasional errors.	develop arguments and statements. Shows evidence of wide scope within the organisation for sourcing evidence. APA referencing is free from errors.	develop arguments and position statements. Shows evidence of wide scope within and without the organisation for sourcing evidence. APA referencing is free from errors.

The following Subject Learning Outcomes are addressed in this assessment	
SLO b)	Administer implementation of security controls, security risk mitigation approaches, and secure design architecture principles.
SLO c)	Explain Secure Development Lifecycle models and identify an appropriate model for a given situation.
SLO e)	Apply security by Design industry standard principles in systems development.