**Cyber Security Assessment 2**

*Risk Assessment Scenario Description for Learning Management System (LMS)*

1. **Scope and Focus of the Risk Assessment**

In the evolving digital education world, Universities have taken up the new method of providing learning for students through Learning Management Systems (LMS). These management systems provide Universities with better methods for delivering, managing, monitoring and providing students with their studies. Due to an increased reliance on these systems, Universities can face increased risk to cyber threats. Using the CORAS method, we will systematically identify, evaluate, and treat security risks affecting the LMS. The CORAS process is a model-based risk analysis method which is used throughout cybersecurity to visualise assets, threats and treatments clearly though diagrams.

The scope of this risk assessment includes:

* The student portal, where students submit assignments, view grades and can access course materials.
* The instructor portal which is responsible for assignment grading, student performance analysis and course creation.
* Administrator backend which handles user management, provides data analytics and allows for course approval.
* Third party tool integrations including cloud storage services, external educational resources and video conferencing.
* Authentication server which manages user access, interfacing with both student and instructor portals for ensuring secure logins.
* The local database that supports the LMS, storing courses, user information and system data for retrieval and analysis.

The focus of this risk assessment includes:

* Confidentiality- ensuring that sensitive data such as student personal information, student grades and examination records are only accessible to the correctly authorised parties.
* Integrity- ensuring that data is safeguarded and processed against unauthorised modification including grade tampering or malicious content being injected.
* Availability- Uninterrupted and reliable access to the system is maintained, especially during critical periods such as examination periods and releasing of grade periods.
* Authentication and Non-repudiation- Verifying user identities and ensuring actions taken within the system can be reliably traced back to the source of it.
* Privacy Compliance- Meeting data obligations under cyber law, especially when dealing with student records and third party data processes.

1. **Target of the Risk Assessment**

The main target of this risk assessment for the party is the operations of the Learning Management System (LMS) and how it plays a central role for the university in delivering educational services, management of academic operations and the achievement of institutional outcomes. Why the LMS is the main target for this risk assessment is because it is the primary channel which the university delivers teaching and manages the engagement with students and staff members, so security is extremely important from the perspective of the university.

1. **Asset Diagram**

**A diagram of a diagram of money

AI-generated content may be incorrect.**

Within this CORAS diagram, we identify the key party being the University Analysis Client as shown within the Asset diagram. We further categorise direct and indirect assets based on their proximity and control within the LMS.

The direct assets represent the components and subsystems owned and operated by the university and include the student and instructor portals, authentication server, administration backend local database and the web server. These assets are the most central to the LMS system operations and the main focus of internal security controls

The indirect assets are cloud storage, video conferencing, student/teacher devices, internet infrastructure and the external learning API. These are services which are expanded from the LMS functionality but also introduce additional threat surfaces and reliability risks. These external systems are critical to the specified services that the university delivers through their LMS, which includes them in the focus of the risk assessment.

The asset diagram also shows interactions between assets, such as: the student portal uploads/downloads to the cloud storage, the auth server verifies login for the student portal and instructor portal, the admin backend validates roles through the auth server and the web server passes read/writes on data to the local database. Showing the interconnection and communication between assets allows us to identify the risk exposure landscape.

1. **Analysis of Unwanted Risks**

The LMS must uphold strong security to protect both the educational outcomes and institutional integrity. Based on the systems architecture and the universities stated security requirements, this risk assessment will focus on the confidentiality, integrity, availability mainly but also we will focus on the privacy, authentication and non-repudiation. These requirements are focused on especially in the context of high-stakes academic activities like online exams and grading.

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Threat** | **Unwanted Incident** | **Damaged Asset** |
| 1 | External Attacker | SQL injection attack modifies grade records | Local Database |
| 2 | External Attacker | DoS attack causes login failure during peak usage | Authentication Server |
| 3 | Insider | Privileged admin accesses and exports student data | Administrative Backend |
| 4 | External Attacker | Phishing email leads to stolen student credentials | Student Portal/Auth System |
| 5 | Third-Party Failure | Unauthenticated user hijacks online exam session | Video Conferencing Service |

1. A malicious external actor can insert a specific value into an input field on the LMS which launches an SQL injection. They can do this by manipulating the query structure and this can give them access or modify the grade records of multiple students. This unwanted incident highlights the critical need for input validation, parameterised queries and strict database access controls to maintain strong backend security.
   1. **Confidentiality-** At very high risk as the academic data and potential personal information can be uncovered.
   2. **Integrity**- Severely impacted as grades can be altered which undermines the trust in academic records.
   3. **Availability**- Possibly impacted if database data corruption causes system errors or outages.

*\*\*\*\*apply the confidentiality, integrity and availability to this assignment*

*Confidentiality- encryption- if this is broken then can get sued etc*

*Increase in one can bring down another one- so important to weigh up what the asset is to determine which one gets most etc*

Step1- identify what the digital assets you are going to protect

* Student data
* Student ID data- name, address, personal information
* Course information
* Staff personal information
* Student fees
* School information
* Contractual documents
* Financial assets
* Web server information
* If LMS is down then students cannot be taught (loss of business and money)

*Using the CIA triad, will need to identify of these which will require which resources eg the student personal information will require more confidentiality than the course information*

**Things like more availability means public looking which means confidentiality goes down and integrity has more risk because public infmration.**

**If more confidentiality then less availability because information is hidden- integrity is balanced**

* Some government regulations have to abide by othersise business cannot run (privatised informration of students) – university policy document (maybe in assignment?)- things like 2FA, MFA- dunno if actually part of the assignment, then just make suggestion why it should be implemented if no policy

**Terminology**

* **Asset- digital information**
* **Vulnerability (weakness a threat can exploit)- bugs in code, no 2FA/MFA, sanitization error, Web server installed on server machines so hosting the website on that web server available for people- apache, nginx, tomki (if webserver outdated its vulnerability)- something you exploit**
* **Threat(actor looking for weakness )- hacker, system downtime, malware, virus. Phishing (use symbols in diagram)- potential cause of unwanted incident**
* **Threat scenario- series of events that is initiated by a threat adnd may lead to unwanted incident**
* **Unwanted incident- event that harms or reduces the value of an asset**
* **Risk- likelihood of unwanted incident and its conseuquence for a specific asset**
* **Consequence- loss of CIA triad, reputation of business ruined, loss revenue**
* **Likelihood- frequency of probability of something to occur**
* **Party- organisation, company, person, group or other body on whose behalf a risk analysis is conducted**
* **Treatment- appropriate measure to reduce risk level- mitigates the risk- treatment to the vulnerability**

create security mechanisms to mitigate these vulnerabilities

if mitigating anything look for the treatment symbol

the risk assessment- need to use the ISO 310000 risk management process- look at CORAS->Coras process in notes- has the process in a diagram

don’t think these indented below are important, just telling us

every stage is consulting with management to discuss what you have identified

approval of management to accept the risk or not

SURVEY AND EVALUATE are for management

always a cost with mitigating a risk

**POWER POINT SLIDE GOOD EXAMPLES OF THE DIAGRAMS**

**HOW TO USE CORAS**

When making diagram

Define scope- must do this first to identify the assets before making diagram

List down all the assets

Identiofy the threats- non human can be bots, natural distasiters (disaster recovery plan)- describe the threat

Identify the threat scenario (how can this threat compromise the asset)- things like unwanted incident

Layer the diagrams so its broken down

*NEED TO MAKE 5 diagrams-*  in notes- Risk Management -> CORAS Risk Management Phases

Diagrams will have report explaining as well

- \*\*Asset Diagram\*\*- 1. Identifying and Documenting assets

**Have two asset diagrams, one for indirect assets and one for direct assets**

Majority of assets listed below are direct- eg the contracts, services, information etc

Indirect is like the reputation which is key for Universities

Maybe have like 3-4 assets and have more detail in the explanation

- devsribe the focus of the analysis

- asj question “What are we protecting?” What is most impotant product to protect?

- identify the system, environment, like web server and database server.

- identify assets- information, contracts, services, uptime, look at indirecit and direct assets (thinks like reputation can be an asset if you are a bank or uni etc

- security concerns with these assets? Compare with CIA triad

- \*\*Threat Diagrams\*\*- describe scenarios that may cause harm to the assets 2. **Identifying and Documenting Threats and Unwanted Incidents in the Threat Diagram**

**LOOK AT THE CORAS SEMANTICS AND DIAGRAMS diagram from notes**

Can have one to many of threat actor to asset (a hacker can cause harm to multiple threats)

Showing in the diagram the threat, vulnerability, threat scenario, unwanted incident, asset and treatments (can have multiple types of treatments for each step)

Can have multiple treatments for the same thing- eg to protect a burglar getting on premise is (guard dog, electric fences, security guards)- but be realistic with costs etc

* Need to have the probability of threats etc using **WEIGHTED FACTOR ANALYSIS**
* Scenario analysis is important to identify so can prioritise the threat importance
* Calculating a realistic assumption (WRITTEN IN THE SCENARIO)

Have to create a table with the Threat, Unwanted incident and asset damaged to summarise and then write the description in the report with more explanation.

Write your threat scenario as the diagram in the picture- adjust to why it is, a threat can have multiple impacts

- \*\*Risk Diagrams\*\*- summarise the risks presented in the threat diagrams- 3. **Identifying and Documenting Likelihoods and Consequences**

- summarises the risks presented in threat diagrams

- make sure explanation of the priority list of risks and explain why

- shouldn’t intoruce new risks if NOT intrduced in threat diagrams

4. **Documenting Risks**

- important to give the numbers of risk to track down which risk and which asset considering- Risk1, Risk2 from the main diagram

5. **Identifying and Documenting Risk Treatments**

- using those identified risks its easier to identify

- CAN FIND WEBSITE INFORMATION FOR THE SOLUTION??? OR SOMETHING like upgrading outdated software

- same risk type can impact different assets

- acceptable and unacceptable risks are documented to determine the appropriate risk treatments

- need to justify why making that assessment for an asset has a risk based on a vulnerability etc

- **HAVE TO DO RISK METRICS- 5x5 metrics**

**- must give the analysis based on the 5x5 metrics for the risk assessment, probability and impact- to prioritise which vulnerability needs to be priority**

- \*\*Treatment Diagrams\*\*- add proposed treatments to the threat diagrams

- \*\*Treatment Overview Diagrams\*\*- add the proposed treatments to the risk diagrams

Have to make a threat scenario diagram for each threat to a specific asset, an asset could have multiple threats and therefore many threat scenarios. Could be More than one vulnerability and more than one vulnerability diagram could also mean more than one treatment diagram- all of these are diagrams