Assignment 1

For Assignment 1 you will need to analyse an application scenario and develop a security plan. You must work in a group of 2 - 3 members.

This document includes the instructions and background information:

- Page 2 describes the application scenario, ref. 'Scenario: Online Learning Environment Security'.
- Page 3 is the template for the Security Plan you need to develop, ref. 'IT Security Plan Template'. **You must use this template for your submission.**
- Pages 4-5 provide some ideas to guide you in developing your Security Plan, ref. 'Security Plan Ideas'.

Submission Instructions:

Please read the following instructions carefully:

ONE student in each group must submit **TWO** PDF copies of the report (It does not matter which student of the group uploads the submission):

- One copy **with** the Revision History (using the table below) submitted via the **Assignment 1 Submission** point on Learning@Griffith. This is for INSTRUCTORS to provide official marks and feedback. Enter the names and snumbers of the team members in the submission comments field.
- One copy **without** the Revision History submitted via the **Submission for Peer Review** on Learning@Griffith. This is for your CLASSMATES to conduct a peer review, so please make sure your submission is ANONYMOUS (i.e., the names of the group members are not mentioned).

Revision History

Outline the development history of the plan, including the dates, contributors, and a summary of changes.

Date of Change	Contributor	Summary of Change
11/8/2020	Andy Duong Simon West	Met to plan out assignment task and roles (in-person)
12/8/2020	Simon West	Part of threat identification
12/8/2020	Andy Duong	Introduction
19/8/2020	Simon West	Mitigations and controls part 1
20/8/2020	Andy Duong	Key Asset Identification
21/08/202	Andy Duong, Simon West	Risk Register Table (in-person)
26/8/2020	Simon West	Mitigations and controls part 2
1/9/2020	Andy Duong	Justification for Risk Register part 1
2/9/2020	Simon West	Cost/Benefits
2/9/2020	Andy Duong	Justification for Risk Register part 2
2/9/2020	Andy Duong Simon West	Strategic Strategies Part 1
3/9/2020	Simon West	Strategic Strategies Part 2
3/9/2020	Simon West	Implementation plan part 1
3/9/2020	Andy Duong Simon West	Justification for Risk Register part 3
4/9/2020	Simon West Andy Duong	Implementation plan part 2
5/9/2020	Simon West Andy Duong	Formatting Assignment Page
6/9/2020	Simon West Andy Duong	Proofread and final revision

12/8/2020 - 4/9/2020	Simon West Andy Duong	References

Scenario: Online Learning Environment Security

Remarkable University is developing a new online learning platform. The platform integrates both existing and newly developed systems, and it needs to be developed to ensure that it is fit for purpose as well as secure from identified threats.

The online learning platform includes the following core components:

- a learning management system (LMS) that support online classes and discussions for instructors and students;
- front-end web/application servers which are used by students, academics and administrative staff;
- databases which hold course data, student data, and the digital library;
- network channels and facilities.

The platform will need to be built and managed to ensure that the servers are deployed securely and remain secured against common automated and simple manual attacks. Dedicated, targeted attacks are difficult to protect against, however simple measure can be taken to protect against most automated attacks. Identified threats against the platform include (but not limited to):

- Data hacking/modification, e.g., unauthorized access to personal information.
- Denial of Service (DoS) attacks
- Malicious code such as worms
- Automated scanning and exploit tools
- Phishing attempts

The online learning environment needs to remain secured, use appropriate access controls, enforce least privilege, and ensure that information flowing to and from the platform is protected. New software needs to be developed in a secure manner and be protected against common attacks, and the databases need to be protected against common automated attacks and use appropriate access controls.

IT Security Plan

1. Introduction

Remarkable University is a classified as a low-medium risk organization, and is less likely to be targeted in a cyber-attack. Remarkable University is a currently developing a Learning Management System (LMS), it is required to determine the key IT assets, the threats that is involved, the strategies to implement, and how they will implement the security plan into the LMS. The security policy is rules, and procedure for all users to follow, while on the organization IT network, or while using their assets. This is put in place to define all the risk involved, as well as protect the organization data, and other valuable assets. *The security plan specific the approach, responsibilities, and sources that is applied for an entity to mitigate the risk involved within the different area of the organization. The security plan is used in conjunction with the security policy to take action of cyber threats that may target Remarkable University.*

2. Key IT Assets

A key IT assets, are asset that is critical to the operation of the of the learning management system. These asset collectively provides values to our organization.
Data: student data, course data, digital library Collectively, the 4 domain of asset will be used together to provide the new online learning platform for Remarkable University. Each of these domain plays a crucial role in developing the new LMS. All 4 different domain works together to help facilitates the needs to the student, academics staff, and the administrative staff. The data is the information we access, communication is how we talk between peers, network is allows communication, and sharing resources, software is the program we use, and lastly, hardware is the component involved.

One of the key IT asset's in our Learning Management System (LMS) is data. Data is an asset, as it provides value to an enterprise. Our database will hold a variety of different type of data such as; course data, student data, and a digital library. This database is connected via a network. Through the use of Remarkable software, and hardware, academic staff, student, and administration can have access to this information. ("Data as an asset", 2020)

Communication supports the online classes, as well as helps student, and teachers engages in discussion through the LMS. This is a key asset, as it facilities communication between the different entities of the LMS. Student can use this to communicate with their peers, teachers, the academic staff can use this to communicate with other staff, and student. While administration, can have direct communication to everyone working within the university campus, Communication can be in the form of e-mail service, web-chat, online forum, discussion page, or VOIP.

Network is another important asset for Remarkable University. Due to the nature of Remarkable University, network is an important infrastructure. The network, allows for the academic staff, student, and administration to have access to the software, their personal drive, course data. Networking also support the hardware using the Remarkable University network infrastructure in allowing them to use the network. The Networks and facilities assets include; the firewall, proxy server and server networks.

The software, and web application being used by Remarkable University, allows for the different entity's to have access to the Learning Management System, and the required software supporting their time at university. Through the LMS, the user is able to gain access to database containing information regarding the course, student, staff, and the digital library, from the server linked the network. The software asset is made up of the Learning Management System and the web application that is used by academic staff, and students. ("How Is Computer Software Classified as an Asset?", 2020)

Our hardware, is what runs, and store information on our Learning Management System. This is classified as an asset, as it allows our organization run its course of business. Remarkable University will have 2 main hardware asset; The Database Server, and the Web Application Server. These hardware, help run, and support our database, which hold information such as course data, student data,, and the digital library. Another hardware that is used to access the LMS is University owned and configured workstations and B.Y.O (bring your own) devices owned by student, teacher, and administration. B.Y.O.D is a cost effective system that is smart, practical, and help save IT department money. ("BYOD security: What are the risks and how can they be mitigated?", 2020) These are classified as key asset, as B.Y.O.D and university workstations are the variety of devices being used to access Remarkable University LMS network.

3. Risk Assessment

3.1 Threat Identification

Security Area	Threat	Description
User Authentication and Access Control	Trojan Horse: Corruption	Trojan Horse is a type of malware that disguises itself as a legitimate software. It is designed to damage, disrupt, steal, or inflict damages on the intended user data, or network. It relies on the user downloading, and executing the malicious malware, once installed the Trojan can take control of the user's files.
User Authentication and Access Control	Client Attack	Client-side attack refers to when the user downloads a malicious software. The form of attack is initiated by the user who download the malicious software from the attacker. Client-Side attack is difficult to control for organization allowing its user to have internet access.
User Authentication and Access Control	Eavesdropping	Eavesdropping attack is a form of attack where the attackers sniff or snoop a network with an intent to steal information being transmitted over that network. This type of attack takes advantage of an unsecured network to access the data being sent and receive.
User Authentication and Access Control	Denial of Service	DOS is a form of cyber-attack, with the aim to shut-down the machine/network, making it inaccessible to its users. DOS attack is generally done by taking advantage of vulnerabilities causing the targeted machine is crash by flooding the targeted machine with traffic or sending information that cause it to crash.
User Authentication	Weak User Password	When a user creates a password that is easily guessable, classifying it as a weak password. This can

and Access Control		commonly occur when users do not include capital letters, symbols, numbers and use words related to their name or other generic words making it susceptible to brute force attacks or other password cracking methods.
Web and Network Security	Replay:	Replay is a network-based attacks, it occurs when the attacker eavesdrops on a secure network connection, intercept the information being sent.
Software Security	Worms	Worms is a type of computer malware spread by making replicas and spreading itself. This is done without any human interaction and doesn't require to be triggered by a user action. It's can replicate and propagate independently once it has breached a system. Worms can modify, delete files, and inject malicious code into the user's system.
Software Security	Injection Attack	Injection attack refers the vulnerability, which allows an attacker to supply untrusted input to a program. The interpreter, processed this as part of the command/query, altering how to program is executed.
Software Security	Buffer Overflow	Buffer overflow occurs when a program or process attempts to write more data than what the buffer is allocated to store. This can result in consequences such as data corruption, unexpected transfer of control, execution of malicious code and memory access violations.
Web and Network Security	Third-Party Cookies:	Cookies is data sent between web servers and web browsers and are designed to allow the website to recognize the computer when visiting. Third-party cookies use the same functionality however to an unknown web server, risking user personal data.
Web and Network Security	Browser Attacks	Browser attack incorporates multiple attacks such as man-in-the-browser, keystroke loggers, page-in-the-middle, download substitutes, user-in-the-middle and others. These attacks share a commonality of trying to spy or deceive the user into inputting sensitive information that can be stolen.
Web and Network Security	Email Phishing	Email phishing is when a user receives an email that is designed to look like it's from a reputable company in order to trick the user into clicking a malicious link, responding with personal data, run an executable file on their workstation or all of the above.
Web and Network Security	Unauthorized network scan/access:	An unauthorized network scan/access is when there is external scanning or access to the network to better understand and potentially find vulnerabilities within. These can come in many specific forms, but all involve a level of access to the network.

System and other security	Unauthorized elevated access to operating system	Unauthorized elevated access to OS is when an unauthorized user gains root or admin access to a server or workstation which allows them to execute and create scripts that can be designed to target vulnerabilities.
System and other security	Payload Attack Agent	Payload attack agents are a targeted attack with the intention of taking control of a workstation to then manage and plan network attacks from. Malware is commonly used to gain control initially.
System and other security	Payload Stealth	Payload stealth is when a backdoor or rootkit is exploited in order to expose vulnerabilities within the program secretly and without detection.
System and other security	Payload System Corruption	Payload system corruption is when an effect on the system causes the system to lose functionality and destroy data. This commonly occurs through ransomware and physical damage to hardware or other critical system entities.
User Authentication and Access Control	Unauthorized access of Remarkable University data, by a user	Unintentional access granted is the failure of access control that allows an unauthorized user access to protected data. Depending on the access control strategy, this can occur by mistaken role or attribute assignment.

Data gathered from Norton and Kaspersky

3.2 Threats to Assets

After degerming the key assets within Remarkable University, we need to determine the significant threats to these asset, specify the likely hood, the consequence, the level of risk, and the risk priority in comparison to our other assets.

Hardware

One of the main threats is Physical damage to hardware that causes damage to functionality availability. This can be to a payload system corruption, within the system and other security. This threat generally comes in the form of a ransomware attack, and will lead to physical damage of hardware, as well as corruption, theft, and loss of Remarkable University Data. Due to this, Physical Damage that causes damage to functionality availability likelihood rating was Rare, Consequence was Doomsday, and level of risk is extreme.

Another threat to hardware is a the Integrity of workstation security, and access control. This comes in the form of Payload Attack Agent, where the user workstation is taken over, and is used as a host to plan network control from. This initially happens after a user unknowingly download a malware. This was rated like hood rare, consequence, major, and the level of risk high.

Software

Integrity of Operating System

Trojan horse can cause issues within the OS of the affected user, due to the user downloading a software disguised as a legitimate software. The user may get affected by this if they aren't careful in the program

they download, or don't seek approval from network admin before downloading a software. Once download, this can gain access to the user system, gaining access to the user data. Organization will have policy put into place to protect against the integrity of the operating system. Due to this, the likelihood of this event is unlikely, the consequence moderate, and the level of risk is medium.

Integrity of User Authentication

Integrity of User Authentication can be degraded due to client attack. If a user accidentally downloads a malicious software from the internet, or from an email. Executing this software can allow the attacker to find crucial information about the user, system, and the information about the system, and network information. This is generally hard to control for all organization that relies on a network connection, as it relies on the user being mindful of how they use the internet, and what they download. Due to this reason, the likelihood is rated as unlikely, the consequences as moderate, and level of risk is medium.

Integrity of software, and network security

Eavesdropping plays a role in the integrity of software, and network security. The likelihood of this is rated as unlikely, consequence as moderate, and the level of risk is medium. The reasoning behind this is organization have put into place policies to protect this from happening. Organization will generally implement firewalls, and other security features in the form of anti-virus software from intersecting information transmitted between user of Remarkable University.

Availability, and integrity of network services, and network security.

Denial of Service plays a role in the availability, integrity of network services, and network security, as well as the integrity, and availability of user authentication. If Remarkable University get hits with a DOS cyber-attack, it will make the network services Remarkable University provides, unusable towards the user of the LMS. This can cause slow-downs, disconnection, as well as not being able to reach the LMS services. While DOS may cause a temporary issue with using the LMS. DOS may also cause long lasting damage if the issues isn't resolved in a timely manner. Server that host database, generally has implemented features, and tweak to stop DOS in it tracks, before it can influence the system. Due to this likelihood of this is rated as unlikely, consequences major, and the level of risk as high.

Reliability of software and security

Worms plays a role in the reliability of software, and security. While worms can be easily spread between the user system, and Remarkable network once a file is infected with the worm. Servers, and the user will have software implemented to protect against these threats, in accordance to the policies put into place. Due to this, the likelihood is rare, the consequences are minor, and the level of risk is low.

Buffer Overflow:

Unauthorized takeover of Remarkable University database, software, system and services. If Remarkable University get affected by buffer overflow, this can cause a large amount of damage of its software security, as well as software security. While this have major damages, organization implement polices to protect their services. This will also protect confidential user data involved. Due to this, the likelihood is unlikely, the consequences is catastrophic, and the level of risk is high.

Integrity of OS security

The integrity of OS security can be caused through browser attack, browser attack can cause damages to the user workstation, as well as the data on the machine the user is using. this can have a damaging affecting on the user system; however, OS generally have security measures, and protocol to protect against these cyber threats. Due to this, the likelihood is rated as likely, consequences as insignificant, and the level of risk as medium.

Integrity of software and operating system

Unauthorized elevated access to OS or network and, unauthorized access, and theft of confidential data by staff, and student plays a role in the integrity of software, and operating system. User with privileges beyond what they need can potentially cause issues with the LMS, and the OS. This is due to user being able to change settings within the software, as well as the operating system. This user may be able to access data that also isn't allowed for them to have access to. This can lead onto degrading the LMS integrity of data. Due to this reason, the likelihood is rated as possible, consequence as moderate, and the level of risk as medium. Payload Stealth, and Payload attack has a role in the integrity of software, and operating system.

Ransomware designed to cripple functionality and availability

Payload System Corruption will cripple the functionality, and the availability of Remarkable University services to its student, academic, and administration trying to reach their services, and the digital library. The ransomware can take over the user system requiring them to make a payment in order to regain access. The user data is encrypted by the cyber attacker and is held until the payment is made. This also shows the integrity of user data, where the user data is stolen, and is loss until the ransom is paid. A similar act like this is WannaCry in 2017. Where it taken over user, as well as government organization. ("WannaCry | Kaspersky", 2020) Due to this, the likelihood of this is rated as rare, consequences as doomsday, and the level of risk as extreme.

Integrity of Access Control

A main factor in the integrity of access control is the user-weak password. A weak-user password makes the user more susceptible to their password being crack via brute-force, by dictionary attack, pattern check, wordlist substitution, social engineering, or possibly a combination of multiple different method above. Once the user password is cracked, depending their level of access to the operating system, and network. This can cause a loss, theft, and corruption of Remarkable University Data. This can also create a widespread security issue that spread across the different workstation, and network. (ITPRO, 2020)

Communication

Integrity of user data, and confidentiality of user data

Another factor of communication is integrity of user data, and confidentiality of user data. This is commonly happening due to third-parties cookies implemented onto website the user may use. This stores information, as well as monitor the internet traffic along LMS. A result of this is the third-party cookie provider will have unauthorized access, and monitoring of the data sent over network. This can

result in the theft, corruption, and loss of Remarkable University data, degrading their integrity of user data control. Due to third-parties' cookies are generally used for targeted advertising, by remembering the user internet activity patter. This has been given a likelihood rating of Almost Certain, Consequence of insignificant, and level of risk as medium.

Integrity of operating system, and browser security

Integrity of operating system and browser security is another factor in communication. This is generally done through the means of e-mail phishing, where a widespread email is sent to different user, in hope they open it. Upon opening the program or clicking the link. The user data is than sent to the attacker, gaining access into the user, and the data of the organization. This can lead to data theft, loss, and corruption. Due to this the likelihood is likelihood is likely, the consequence is insignificant, and the level of risk is medium.

Integrity of protected data, and access control

Integrity of protected data and access control is caused due to user given elevated level access of data, and network security. Allowing them to view, edit, and change protected data of another user with Remarkable University. This has been given the likelihood rating of unlikely, consequences of minor, and level of risk as medium.

Integrity of network security and workstations on the network's data

Integrity of network security and workstations on the network's data refers the user's ability to perform unauthorized network scans. This allows the unauthorized user to snoop, and sniff around network traffic going between the LMS sever. Those with unauthorized network scan, will be able to see the data being transmitted, and may risk the loss, corruption, and theft of these data. This has been given the rating of possible, moderate, and high.

Reliability, and integrity of network

The reliability, and integrity of network occurs when a user has an unauthorized elevated of access to operating system, or the network security. When a user is given higher privilege than what is required, this make them susceptible to gain access to confidential data the organization. This can also cause the loss, and theft of student, academics, administration, and the data held by the digital library. Due to this, this has been given the likelihood rating of possible, as procedure are put into place to ensure this doesn't happen, a consequence rating of major, and the level of risk of high.

Data

The second key assets to be concerned about, is the integrity of stored student, academics, administrative, and the digital library data. This could be in the form of a ride variety of attack due to network, software, and communication issues. Due to Remarkable University being a large educational institution, an attack such as, or security flaws:

- Trojan Horse
- Client Attack
- Eavesdropping
- Weak-User Password

- Replay
- Worms Injection Attack
- Buffer Overflow
- Payload Attack Agents
- Payload Stealth
- Payload System Corruption

Each of these attacks, and security flaws, can lead to issues where, students, teacher, administrative, and the digital library data being stolen, corrupted, or loss. However, some of these threats likelihood were rated lower than others. With trojan-horse, client attack, eavesdropping, weak-user password, replay, buffer-overflow being rated unlikely due to security measures already put into place. Trojan horse, client attacks, eavesdropping, weak-user password, replay and worms were all given the consequence rating of moderate, and the level of risk as medium.

Injection attack accounted for roughly 47% of all attacks during the period of January 2016 to June 2017. The most common injection attack were operating system command, and SQL injection. ("Injection Attacks: The Least Glamorous Attack Is One of the Most Threatening", 2020). Due to this, injection attacks has been likelihood rated as a likely. The consequence is rated as major, this is due to the potential loss, corruption, and the theft of Remarkable University data that may be involved in this cyber-attack. The level of risk for injection attack was extreme. An injection attack can also have an effect on the availability, injection of software and systems.

Payload Attack Agents, Payload Stealth, and Payload System Corruption were all given the given the same rating of likelihood of rare, the consequence rating of major, major, and doomsday respectively, and lastly the level of risk rating of high, high, and extreme.

Risk Priority

The risk priority reflects how important the risk is in comparison to the other risk, in our register we have identified the most important risk, and ranked it from most important, to the least important from 1 – 18. This ranking is based on the likelihood, the consequence, and the level of risk to make our choice.

3.3 Risk Register

Likelihood = Almost Certain (5), Likely(4), Possible(3), Unlikely(2), Rare(1)
Consequence = Doomsday, Catastrophic, Major, Moderate, Minor, Insignificant
Level of Risk = Extreme, High, Medium, Low
Risk Priority = 1 - 5

Asset	Threat/ Vulnerability	Likelihood	Consequence	Level of Risk	Risk Priority
Software: Integrity of Operating System	Trojan Horse Attack on the academic staff, student, and administration hardware.	Unlikely	Moderate	Medium	9

Software: Integrity of User Authentication **Data:** Integrity of stored data	Client Attack: Unauthorized access of student, academic staff, and administration data	Unlikely	Moderate	Medium	13
Software: Integrity of software, and network security **Data:** Integrity of stored data	Eavesdropping: Unauthorized use, and theft of student, teacher, and administration file sent over the network	Unlikely	Moderate	Medium	10
Software: Availability, and integrity of network services, and network security. Integrity, and availability of User Authentication	Denial of Service: Disrupting access to server, from hardware used by the students, teacher, and administration	Unlikely	Major	High	7
Communication: Integrity of access control **Data:** Integrity of stored data	Weak User Password: Unauthorized access of teacher, student, administration, and digital library data Theft, corruption of Remarkable University data stored on the network	Possible	Minor	Medium	6
Network: Reliability and integrity of network	Replay: Unauthorized use, and theft of data being sent over the network by users of the LMS	Unlikely	minor	Low	12
Software: *Reliability of software and security* **Data:** Integrity of stored data	Worms. Unauthorized modification of academic staff, students, administration, Remarkable University Data, and software	Rare	Minor	Low	14
Software: Availability and integrity of software and systems **Data:**	Injection Attack: Theft, corruption, and loss of Remarkable University,	Unlikely	Major	Extreme	3

Integrity of stored data	Academic Staff, student data				
Software: Availability and integrity of software and systems **Data:** Integrity of stored data	Buffer Overflow: Unauthorized takeover of Remarkable University database, software, system and services.	Unlikely	Catastrophic	High	7
Communication: Integrity of user data Confidentiality of user data	Third-Party Cookies: Unauthorized access, monitoring and theft of data being sent over the network by users of the LMS	Almost Certain	Insignificant	Medium	8
Software: Integrity of OS security	Browser Attacks: Theft of user information	Likely	Insignificant	Medium	17
Communication: Integrity of OS and browser security	Email Phishing: Unauthorized access to users' information, and data	Likely	Insignificant	Medium	18
Network: Integrity of network security and workstations on the network's data	Unauthorized network scan: Unauthorized use of network traffic within the LMS servers	Possible	Moderate	High	5
Network: Integrity of network security **Software:** Integrity of software and operating system	Unauthorized elevated access to OS or network Unauthorized access, and theft of confidential data by staff, and student	Possible	Moderate	Medium	4
Hardware: Integrity of workstation security and access control **Software:** Integrity of software and operating system	Payload Attack Agent: Unauthorized access of Remarkable University workstation Unauthorized access of Remarkable University software	Rare	Major	High	15
Software: Integrity of workstations and servers **Data:** Integrity of stored data	Payload Stealth Unauthorized access, view, and use of data sent by the user through Remarkable University Software.	Rare	Major	High	16

Hardware: Physical damage to hardware that causes damage to functionality availability **Software:** Ransomware designed to cripple functionality and availability	Payload System Corruption Damage, corruption and theft of Remarkable University data stored on servers.	Rare	Doomsday	Extreme	1
Communication: Integrity of protected data and access control	Unauthorized access of Remarkable University data, by a user	Unlikely	Minor	Medium	11
Data: Integrity of stored data	Unauthorized access of Remarkable University data, by a user	Possible	Major	Extreme	2

4. Security Strategies

4.1 Control Classifications

Security Area	**Control Classification**	**Description**
User Authentication and Access Control	Policy	User Authentication, and Access Control Policy is the process put into place to verify the identity of whomever is accessing the services Remarkable University Provides. There are 4 different means of authenticating a user, this comes in the form of; something the individual knows (password, pins), a processions (token), something unique to the user (biometric identification), or an unique action (dynamic biometric identification) Complex Password Policy forces the user to create a strong password, making the password harder to guess, and brute force. This policy also enforces the password use word that are complex, and hard to guess. The password policy enforces the user to create a password within the password policy parameter; 8 letters, at least 1 uppercase, number, and special symbol. Discretionary Access Control Policy Discretionary Access Control (DAC) refers to restricting the user ability to enable another user to access a resource. Each file has its own attribute to different user. Role-Based Access Control Policy

		A Role-Based Access Control Policy refers to level of access a user may have, based on their role within the organization. A student may only have read access to the course material, and the digital library. A teacher may have elevated access to student data, course data, as well as the digital library based on their role within Remarkable University. Administrative staff will have Cardinality access to student data, teacher data, course data, and the digital library. Attribute-Based Access Control Policy Attribute Based Access Control refers to the level of access based on the user attribute, the environmental attribute, and the resources attribute. Student user attribute will be limited to the current course they are enrolled in, the environmental attribute will be based on the files they can access within the course, and the resources attribute is their access to view their access to the digital library. The teacher will have an elevated level of user attribute; allowing them to edit the content of the course, the environmental attribute, by adjusting the access time for certain files, and document, and resources attribute, allowing them to view all resources contained within their course. Administrative will have cardinality levels of user, environmental, and resource attribute. They can have access to all information regarding the academic staff, the students, and the digital library.
User Authentication and Access Control	User Education/ Awareness	User education and awareness is teaching your users the risks associated with using the system. User education can come in different forms such as from a presentation format to a group of users, documentation of certain procedures and processes, individual communication with users or in the form of organizational policies. The main goal is to develop informed user who can avoid risks by being aware of what their actions can do to the system.
Web and Network Security	Firewall Blacklisting	Firewall blacklisting provides control over what websites can be accessed over the network. Any website is categorized as malicious by the firewall will be blocked and unable to access while on the network.
Web and Network Security	Firewall in/out rules	Firewall rules manage the inbound and outbound traffic between the network and the internet. Inbound rules are set to allow certain data types to travel to their desired location within the network via an allocated port. Outbound rules are set to allow traffic from the network via an allocated port out into the internet.
System and other security	Anti-Virus Software	Anti-virus software is designed to detect, neutralize or eradicate malware detected on the system. Forms of malware that anti-

Software Security		virus commonly detects are viruses, worms, client attacks, eavesdropping, etc. It is installed on workstations and servers and frequently monitors and scans the system to detect real time threats.
Web and Network Security	IDS Software	IDS software monitors network traffic and identifies threats or irregular traffic on the network. This can come in the form of a network IDS to specifically monitor traffic, host IDS to monitor a single host for activity or a hybrid combination of both.
User Authentication and Access Control	Access Control Procedures	Access control procedures are set by the organization and designed to guide the IT department on how access should be granted to users. It is a documented process to ensure that correct access control practices are in place and users only have access to appropriate data.
User Authentication and Access Control System and other security	Least of Privilege rights	Least of privilege rights is the principle that users should only be granted the bare minimum access rights required to operate and use required programs and systems. This is reducing risk within the organization by reducing the number of user accounts with root or administrative access to manipulate vulnerabilities within the system.
System and other security Software Security	Patching	Patching is updating your operating system or software to remove vulnerabilities available in previous versions. Many operating systems and software will become more vulnerable over time due to worms and viruses being created to exploit the vulnerability, by patching regularly it removes reduces the likelihood of an attack through making the software or system more unpredictable to attackers. Patching can come in the form of third-party patching for software (word, adobe, etc.) and operating system patching.
Software Security System and other security	Approved Whitelisted applications	Approved whitelisted application is only allowing IT approved application and its approved version to be to be installed. This helps reduce uncertainties by standardizing the operating environment to allow specific security measures to be implemented without impacting user functionality too much. It also allows consistency in patching and updates.
Web and Network Security System and other security	Log Files	Log files are used to track the actions and change of states within the databases, software, firewall or network. If an issue occurs within the IT environment, the log files of the disruptive system, database, firewall or network can be checked and narrow down or indicate a resolution for the issue via identifying and associated the change of state to the disruption.
System and other security	Backups	Backups of data is a second copy of the data in a safe location to be used in events of disaster recover. Depending on the complexities and size of the data this can be stored on site or in a cloud infrastructure. This data must be accessible within an

		appropriate amount of time to maintain functionality of the system in cases of disaster.
System and other security Web and Network Security	System Testing	System testing is evaluating the system's capabilities against a set of requirements. This is done to ensure that to that newly integrated systems and established existing meet expectations in terms of integrity and available required to perform. Requirements of system testing can be written by the IT department to ensure specific functionality or generic standards based on the system and documentation available
User Authentication and Access Control System and other security Web and Network Security	Comparisons to official IT Standards (ISO)	Official IT security standards are industry standards provided by reputable companies to provide security frameworks to IT departments to help manage their policies, procedures and processes. There are many IT standards that an organization can adopt and are all designed to provide best practices that reduce risk throughout the organization. Currently one of the most common security standards used through IT is ISO/IEC 27001.
Web and Network Security Software Security System and other security	Safe Coding Techniques	Practice safe coding techniques such as: • Limiting user inputs • Assuring each array is within memory capacity • Review out of bounds conditions and ensure they are functional • Use least of privilege for each piece of program code
System and other security	Space Randomization	Space randomization is a security technique used to counter-act buffer overflow by randomizing the location where system executables are loaded into the memory, making it less predictable for attackers to exploit.
System and other security	Guard Pages	Places pages known as "guard pages" between critical points of memory that will abort the process once accessed.
System and other security Web and Network Security	Configuration Revisions	Configuration revisions involves the IT department reviewing their current processes, procedures and policies within the organization to define if improvements can be made or not. This is done to incentivize innovation within the organization and is important to remain current and stay ahead of any possible security attacks.

4.2 Mitigation and Control methods

Level of Risk = Extreme, High, Medium, Low

Risk (Asset/Threat)	**Level of Risk**	**Recommended Controls**	**Selected Controls**

Trojan Horse	Medium	Anti-Virus software: Detect trojan horse threats found on OS User Education/Awareness: Basic understanding of security principles to avoid accidental downloads Approved Whitelisted Applications: Avoid accidently installation of Trojan by only installing approved software Least of Privilege rights: Avoid installation of trojan horses by restricting access/installation rights to approved groups. Log files: System logging of operating systems through windows “Event viewer” (for non-B.Y.O devices) Policy: Security policies based around user education and best practices to induce secure IT environment	Anti-Virus User Education/Awareness Approved Whitelisted Applications Least of Privilege rights Log Files Policy
Client Attack	Medium	Anti-Virus software: Detect any other unmentioned malware threats found on OS User Education/Awareness: Basic understanding of security principles to avoid accidental downloads Approved Whitelisted Applications: Avoid accidently installation of other unmentioned malware by only installing approved software Least of Privilege rights: Avoid installation of other unmentioned malware by restricting access/installation rights to approved groups. Log files: System logging of operating systems through	Anti-Virus User Education/Awareness Approved Whitelisted Applications Least of Privilege rights Log Files Policy

		windows “Event viewer” (for non-B.Y.O devices) Policy: Security policies based around user education and best practices to induce secure IT environment	
Eavesdropping	Medium	Anti-Virus: Detect any eavesdropping software and remove Patching: Ensure software and OS are patched to reduce vulnerabilities Firewall Blacklisting: Ensure firewall filter is active and working to block access from any malicious website Firewall in/out rules: Ensure firewall rules are configured to stop users from viewing information via the network IDS Software: IDS software used to identify irregular traffic on the network	Anti-Virus Patching Firewall Blacklisting Firewall in/out rules IDS Software
Denial of Service	High	Comparisons to official IT Standards: Compare DDOS protection methods to industry standard methods Firewall: Ensure Firewall is appropriately configured to mitigate attacks System Testing: Conduct tests on the system as preparation for the event of an attack Configuration Revision: Conduct revisions on Firewall security to ensure they are up to date and standard	Comparisons to official IT Standards Firewall System Testing Configuration Revision
Weak User Password	Medium	Policy: Password policy enforced on user to follow strict complex	Policy

		password protocol of a minimum of 6 characters, including at least 1 uppercase, 1 special character, and 1 number The user is refrained from using commonly used words, phases, and term. i.e. password Safe Coding Practices: Limit input attempts and lengths to avoid brute force and other password cracking methods	Safe Coding Practices
Replay	Low	Anti-Virus software: Detect replay related software on workstation (for non B.Y.O devices) IDS Software: IDS software used to identify irregular traffic on the network	Anti-Virus Software IDS Software
Worms	Low	Anti-Virus software: Detect worm threats found on OS User Education/Awareness: Basic understanding of security principles to avoid accidental downloads Approved Whitelisted Applications: Avoid accidently installation of Worms by only installing approved software Least of Privilege rights: Avoid installation of trojan horses by restricting access/installation rights to approved groups. Log files: System logging of operating systems through windows “Event viewer” (for non-B.Y.O devices) Policy: Security policies based around user education and best practices including approval prior to any downloads/installation.	Anti-Virus User Education/Awareness Approved Whitelisted Applications Least of Privilege rights Log Files Policy

Injection Attack	Extreme	Least of rights: Avoid malicious code being run on hosts by reducing number of users with admin rights to run. Patching: Ensure patching is regularly conducted on host to patch any vulnerabilities Access Control Procedures: Ensure users with access are appropriately qualified to access the host.	Least of rights Patching Access Control Procedures
Buffer Overflow	High	Safe Coding Practices: Avoid buffer overflow by assuring created application do not exceed the space available Space Randomization: Using space randomization security techniques to reduce predictability of memory loading location Guard Pages: To create gaps in memory that aborts access when accessed to create difficulties for attackers	Safe Coding Practices Space Randomization Guard Pages
Third-Party Cookies	Medium	Firewall Blacklist: Ensure firewall filter is active to block access from malicious websites User education/Awareness: Educate users on third-party cookies and sensitive information	Firewall Blacklist User education/Awarene ss
Browser Attacks	Medium	User education/Awareness: Educating users to common indication of phishing emails Anti-Virus: Anti-virus to block unauthorized installation and activity if user do fall for phishing. Policy: State in policy the certain type of website the user can access while on the organisation network. Firewall Blacklist: Ensure firewall filter is active to block access from any malicious website	User education/Awarene ss Anti-Virus Policy Firewall Blacklisting

Email Phishing	Medium	User education/Awareness: Educating users to common indication of phishing emails Anti-Virus: Anti-virus to block unauthorized installation and activity if user do fall for phishing. Least of Privilege rights: Avoid installation of malware by restricting access/installation rights to approved groups. (for non B.Y.O devices) Policy: State in policy users must report suspicious emails that are sent to their user email User must not open unknown attachment sent via communication software. I.e. e-mail, discussion board, and web-chat services	User education/Awareness Anti-Virus Least of Privilege Policy
Unauthorized network scan	High	IDS Software: IDS software used to identify irregular traffic on the network Policy: Ensure user policy states it is against policy to scan the network Firewall in/out rules: Restrict pings and other communication methods on the network to authorised users Comparisons to IT security standards: Ensure industry standards are met to secure the network System testing: Test the network for vulnerabilities to network scans Firewall in/out rules: Ensure firewall rules are implemented correctly to help categorise traits of irregular traffic practices	IDS Software Policy Firewall in/out rules Comparisons to IT security standards System testing Firewall in/out rules

Unauthorized elevated access to OS or network	Medium	Anti-Virus: To detect any spyware used to steal login details Least of rights: Avoid elevated access to OS by reducing the number of accounts with elevated access Policy: Create policy that account information cannot shared Patching: Ensure regular patching is conducting to patch any vulnerabilities used for elevated access Access Control Procedures: Provide access to data based on the user's role or attribute and have access control procedures to resolve any unauthorized access as soon as possible	Anti-Virus Least of rights Policy Patching Access Control Procedures
Payload Attack Agent	High	Anti-Virus software: Detect malware threats found on OS User Education/Awareness: Basic understanding of security principles to avoid accidental downloads Approved Whitelisted Applications: Avoid accidently installation of malware by only installing approved software Least of Privilege rights: Avoid installation of malware by restricting access/installation rights to approved groups. Log files: System logging of operating systems through windows "Event viewer" (for non-B.Y.O devices) Policy: Security policies based around user education and best practices to induce secure IT environment	Anti-Virus User Education/Awarene ss Approved Whitelisted Applications Least of Privilege rights Log Files Policy IDS Software Firewall in/out rules System Testing

		IDS Software: IDS software used to identify irregular traffic on the network Firewall in/out rules: Ensure firewall rules are implemented correctly to help categorise traits of irregular traffic practices System Testing: Test the system with a mock payload attack to gauge the affect and further insight into control methods	
Payload Stealth	High	Anti-Virus software: Detect malware threats found on OS User Education/Awareness: Basic understanding of security principles to avoid accidental downloads Approved Whitelisted Applications: Avoid accidently installation of malware by only installing approved software Least of Privilege rights: Avoid installation of malware by restricting access/installation rights to approved groups. Log files: System logging of operating systems through windows “Event viewer” (for non-B.Y.O devices) Policy: Security policies based around user education and best practices to induce secure IT environment Configuration Revision: Review configurations frequently to ensure control methods are in place to prevent payload stealth	Anti-Virus software User Education/Awarene ss Approved Whitelisted Applications Least of Privilege rights Log Files Policy Configuration Review
Payload System Corruption	Extreme	Backups: Restore lost data from last successful backup	Backups

		User Education/Awareness: To avoid ransomware attacks, ensure users understand basic security ideologies Least of rights: Avoid ransomware attacks occurring using elevated permissions Comparisons to official IT Standards: Ensure security standards are met to reduce likelihood.	User Education/Awarene ss Least of rights Comparisons to official IT Standards
Unintentional access granted	Medium	Access Control Procedures: Role-based or attribute-based access control is set up, to ensure certain user will have certain privileges based on their role within the organisation. Policy: Policy in place to verify user's authority to need access to data prior to granting	Access Control Procedures Policy

4.3 Cost/Benefits

The university assets is pivotal to the day to day operations of Remarkable University. Proper control methods must be implemented in order to ensure that all assets integrity and availability is upheld, however this must be put into context in terms of the cost Remarkable University will pay to implement these controls. The cost to the university can take different forms such as physical resources, money, skills and time.

It is for that reason that the above controls must be contextualized by understanding what controls can appropriately be implemented to protect the Remarkable University assets in terms of the cost of implementation and the security provided.

The hardware within the organization and the associated threats are listed in **section 3.2.** The most pivotal pieces of hardware within Remarkable University are the **database and web application host**. Due to the significance of the database and web application to the operational procedures of the university all above technical controls must be implemented as the benefit far outweighs the cost. Practical aspects of hardware must be used such as:

- **User Education/Awareness**: Ensure hardware location and number is documented and accessible
- **Policy**: Assign responsibility of hardware physical safekeeping in policy

The database and web application host must be configured correctly in terms of software security. Controls and mitigations for software security are listed under software.

Mitigation procedures must also be used to initially avoid threats to hardware:

- **Comparisons to official IT Standard:** Ensure security meets industry standards for databases and web applications
- **Policy:** To discourage user behaviour that can cause threats

Mitigation procedures main expense is time, if the technical controls are in place, mitigation procedures can reduce in frequency to equalize the cost/benefit.

Other hardware assets are B.Y.O.D and University owned workstations. B.Y.O.D are not within Remarkable Universities control and will only be influenced by such mitigation controls listed in software.

University owned workstation must have the above mitigation controls along with software configurations listed in software.

Firewall must be purchased, is integral to system security and has a significant benefit to the university.

The software within the organization and the associated threats are listed in **section 3.2.** The software that the university manages are the LMS and Web App. The LMS and Web App are the most important assets due to the LMS being the key communication and data sharing tool for the university, the LMS depends on the Web App so they both must be secure since the benefit outweighs the cost. In order to secure the database and web applications from the mentioned threats, we must technical controls such as:

- **Backups**: In case of deletion or corruption of data
- **Log Files**: To supply traceability to problems
- **Safe Coding Practices:** Ensure minimal vulnerabilities in code
- **Space Randomization:** Avoid buffer overload
- **Guard Pages:** Avoid buffer overload
- **Patching**: Patch vulnerabilities in OS and software
- **Configuration Reviews**: To remain innovative with controls
- **Least of rights:** Reduce number of possible accounts with access

Mitigation for the LMS and Web App are:

- **Policy**: Assign responsibility of software security management policy
- **User Education/Awareness**: Educate users on safe practices

B.Y.O.D devices are not under Remarkable University responsibility however can still pose a threat since they will be connected to the network. Mitigation of risk used for these devices are:

- **User Education/Awareness:** Safe practices while using the university network
- **Policy:** Prohibit dangerous activity

In order to cater for students accessing university owned systems these must be implemented as a precaution.

University owned workstation must be configured correctly in order to make the operationally safe for use. Software security controls such are:

- **Anti-Virus:** First line of defence against malware
- **Patching**: Patch vulnerabilities in OS and software
- **Least of Rights**: Limit access rights to workstation
- **Approved whitelisted applications**: Only approved applications installed

These are very cheap and sustainable control methods that must be applied in order provide access to workstations with minimal risk to the university.

The communication assets within the organization and the associated threats are listed in **section 3.2.** The communication assets within the university depend on the LMS being functional. The LMS provides communication tools such as email, web chat, discussion boards and VOIP. However since this is a client facing asset (unlike the LMS software back end) different controls must be implemented such as:

- **Policy**: Assign responsibility of software security management policy
- **User Education/Awareness**: Educate users on safe practices
- **Anti-Virus**: Installed on University workstations, encourage for B.Y.O.D

These controls must be implemented in order to maintain the integrity of the LMS in order to allow students and staff work on the system safely.

Communication is heavily dependent on the integrity of the network. Without the network's functionality LMS communication cannot exist. This means in order to control and mitigate risks to the communication assets you must ensure the network is operational.

The network assets within the organization and the associated threats are listed in **section 3.2.** The key network assets the organization is responsible for are the firewall, proxy and server networks. This network assets are key to the smooth communication of the LMS and the transmission of data through the network. Without proper control and mitigation methods, the university runs a risk of communication and data errors. Technical controls consist of:

- **Firewall in/out rules**: Manage traffic throughout the network and block threats
- **Firewall Blacklisting**: Blacklisting threats
- **System Testing:** Testing system security to indicate vulnerabilities to patch
- **Patching**: Keeping Firewall firmware up to date
- **IDS Software**: Software to detect irregular traffic on the network

Mitigation controls can be applied to manage the security of the network through regular:

- **Comparisons to official IT Standards (ISO):** Regularly comparing practices to industry standards
- **Configuration Revisions:** Regularly revising configuration for improvements
- **Log Files:** To provide traceability to events

Initial cost of firewall hardware is significant; however, the benefit outweighs the cost. The controls and mitigation are time consuming tasks but in order to provide security to all systems they must be implemented and frequently kept track of.

The data assets within the organization and the associated threats are listed in **section 3.2.** Data is a key asset that must be protected within the university. The university has a responsibility to the students and staff to not only keep their student and course data safe but also to provide consistent and reliable access to their data. Technical controls for managing data are heavily related to the hardware and software used. Since users must have access to their data, user education and awareness is pivotal to empower the user to be safe and secure with their own data. Mitigation controls for this are:

- **Policy:** Ensure safe user practices are compulsory within policy
- **User Education/Awareness**: Of how to keep data safe

The majority of this education comes in the form of 2 factor authentication and secure password policies. The user authentication via password means that users must understand the significance of keeping their password safe and secure. In order to provide them ease of access to their data they must agree within policy to follow safe practices when using the system.

Data libraries used by the university must also be kept secure through software security methods and the safe practices of the IT staff maintaining the asset.

5. Implementation

Despite all steps of mitigation and control taken, eliminating risk from the project entirely is unrealistic, there for residual risks are still attached to each asset and must be accounted for to ensure integrity and availability for the system. Each asset will be discussed and recommended maintenance and training will be outlined to mitigate the remaining residual risks involved.

Hardware will have many procedures and processes based around the maintaining the database and web app host server. All servers must remain secure because of the sensitive information and operational information that is stored within. In order to maintain the integrity of the servers Remarkable University must:

- Ensure the university hires the required skills to maintain
- Responsibility of maintaining is assigned to an individual
- Documented processes are created to help guide different circumstances

It is crucial for the organization to hire the appropriately skilled technicians, placing the integrity of the hardware in the hands of an inexperienced technician runs the risk of oversight, lack of innovation and mistakes. The university cannot afford these mistakes due to how much depends on the availability and integrity of the servers.

Software is another crucial asset that must be held to a high standard. The software is dependent on the hardware, while the communication and data is dependent on the software. Communication and data are core functions that must be maintained, meaning procedures and processes providing insight into the software designs must be documented or at the very least shared throughout IT to ensure understanding of how functionality is provided throughout the system. Failure to document or share knowledge can lead to:

- Slow response times to problems
- Lack of innovation

- Potential overlooked vulnerabilities

When new developers are hired, development knowledge must be shared to reduce the need for specific individuals and provide more versatility in the long term of the university.

Communication is crucial for front facing functionality of the system. If communication methods are down, the day to day operations of the University will be slowed. The maintenance of communication related assets pivots on the integrity of the software, hardware and network. There for residual risk related to communication relates back to the user's actions and the safe practices they use on the system. In order to incentivize safe practices the university must:

- Policies be accessible to users
- Brief understandable documentation is used
- IT Support is accessible
- Support contacts are advertised

Communication issues can range from technical issues to user errors, there for it is more difficult control as it is heavily based on the user understanding. There for training and awareness of what to do, and if that fails or to contact is important for communication functionality.

Network residual risks share the same nature as hardware risks, practical and consistent steps must be undertaken to ensure the integrity and availability of the system. Once the network is setup maintenance processes must be documented and shared throughout IT. Similarly to hardware:

- Ensure the university hires the required skills to maintain
- Responsibility of maintaining is assigned to an individual
- **Documented** processes are created to help guide different circumstances

Network environment are often very unique to the organization as different network architectures are designed for different objectives. Making the need for a skilled network engineer a must to develop a critical understanding of the network that can be leveraged for different issues. Knowledge that the engineer finds ideally should be documented and shared to add more versatility to IT.

Lastly, availability of **data** comes with its own residual risks. It is important to the users to access data when they need, but with ease of accessibility comes with less security. The key to keeping data secure is the access control methods and user authentication. In order to keep user authentication secure, users need:

- Access to IT support services
- Documentation on how to change password and other crucial procedures
- Policies banning sharing of data/passwords

The best way to reduce residual risk of data is through user education. The LMS system to access data must provide ease of access, this ease of access becomes a double edge sword as if their authentication details are revealed, unauthorized users can do the same. IT themselves must create processes and procedures to deal with the event of unauthorized access and ensure the knowledge is shared.

6. References

[1] Griffith Online: https://www.griffith.edu.au/life-at-griffith/online

[2] Griffith Information Security Policy: http://policies.griffith.edu.au/pdf/Information Security Policy.pdf

[2] Griffith Information Security Procedure: https://policies.griffith.edu.au/pdf/Information Security Procedure.pdf

ITPRO: Password Cracking, from https://www.itpro.co.uk/security/34616/the-top-password-cracking-techniques-used-by-hackers

BYOD security: What are the risks and how can they be mitigated?. (2020)., from https://www.comparitech.com/blog/information-security/byod-security-risks/

Computer Security Products for Home Users | Kaspersky. (2020). , from https://www.kaspersky.com.au/home-security

Data as an asset. (2020). , from https://www2.deloitte.com/us/en/insights/industry/public-sector/chief-data-officer-government-playbook/data-as-an-asset.html

How Is Computer Software Classified as an Asset?. (2020)., from https://www.investopedia.com/ask/answers/09/computer-software-intangible-asset.asp

Injection Attacks: The Least Glamorous Attack Is One of the Most Threatening. (2020). Retrieved 4 September 2020, from https://securityintelligence.com/injection-attacks-the-least-glamorous-attack-is-one-of-the-most-threatening/

Official Site | Norton™ - Antivirus & Anti-Malware Software. (2020). , from https://au.norton.com/