Scenario: Online Learning Environment Security

IT Security Plan

1. Introduction

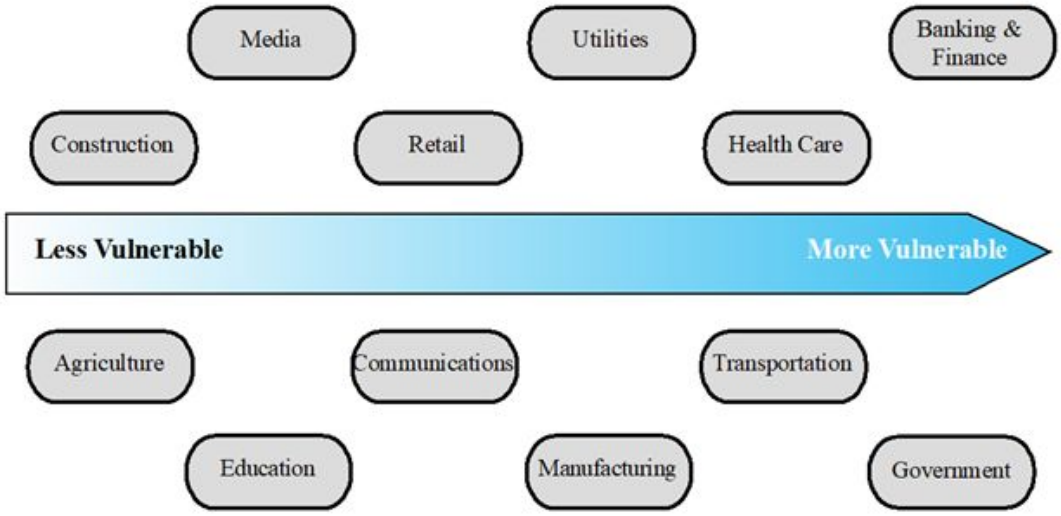
As most organisations have many assets involving valuable information, security plans are often initiated to enhance and maintain the level of security in organisations' assets and to better secure organisational assets from potential threats and risks.

It is important to note that different security plans are initiated based on different organisational context and policies. Before initiating a security plan one organisation's risk profile must be examined to obtain information about their organisational context and policies.

To assess one organisation's risk profile, one must:

1. Identify one organisation's general level of risk
2. Analyse the likelihood of identified risks
3. Examine one organisation's security policy and procedure.
4. Determine boundaries for risk assessment

For this online learning platform scenario, Remarkable University's organisational risk profile will be examined in detail followed by the four-step process mentioned above.



Step 1: From the figure above (Wang, 2020), it is depicted that educational-based organisations are leaning more towards the less vulnerable and less risky spectrum in general.

Step 2: Being placed at the less vulnerable and less risky spectrum in general meaning that Remarkable University is less likely to be specifically targeted. However, the risk will be major if student and staffs' data is thefted or corrupted, and leaked to the public. Thus, in general, only moderate or lower level of risks should be accepted.

Step 3: Since Remarkable University is a fictional educational institution, it is unknown the details to its security policy and procedures. However as Griffith University and Remarkable University are organisations of the same type, Griffith University's security policy and procedure will be closely examined to form base knowledge for Remarkable University's security policy and procedure. By examining Griffith University's security policy and procedure, it is confirmed that Griffith University is obliged to legal requirements for asset security standards such as the ISO/IEC 27001 standard (Information Security Policy, 2020), and Information Privacy Act 2009. Hence, it can be safely assumed that since Remarkable University is also an educational-organisation, it is as well subjected to comply with such legal requirements.

- ISO/IEC 27001 standard sets rules and governs for information security.
- Information Privacy Act 2009 is an enforced law that aims to maintain data integrity and confidentiality of students and academics, and strictly prohibited any unauthorised access to student's and employee's data (Griffith University Procedure, 2020).

Step 4: The boundaries for Remarkable University's risk assessment were specified to include only the systems under the direct control of the internal operations, and its private networks such as the organisation's intranet, focusing on protecting shared content and internal information flow accessed by members within Remarkable University, and aiming to block all external users' access to any of these protected content and information. This excluded the organization's internet gateway, any information flow and shared content outside Remarkable University's intranet will not be protected (Moss, 2020).

2. Key IT Assets

In this section, a broad range of relevant assets in the new online learning platform will be identified and classified into four categories: hardware, software, data, or communication facilities and networks. Among all identified and classified relevant assets, key assets that will seriously impact organisational operations are then being recognised and justified.

Relevant IT assets:

Common hardware of a online learning system will include:

- Database server facilitates Oracle software that stores students' and staff' data.
- Web server stores students' and staff' user authentication cookies and third-party tracking cookies for which records the visiting information of users on LMS.
- Email server is responsible for email exchange between students and staff.
- Digital library server stores book data which would be available to students for consumption.
- Course and enrolment server manages correspondingly the course information and students' enrollment details.
- Personal machine/computer that belongs to or is in utilisation of students and staff allows them to run LMS and possess access to relevant components that their roles enable.

Common software of a online learning system will include:

- Oracle Database Software is an application that supports the Database Management System where students' and staff' data are stored, and reasonable changes to the data can be performed through Oracle.
- LMS is the online learning platform where daily teaching and study runs on.
- Operating systems act as the interface between the user and the computer hardware, it is a paramount component for personal machines/computers to have in order for its users to carry out communication among software and hardware.
- Remarkable University's web server is hosted by Apache Tomcat HTTP Server.
- Remarkable University's application server is hosted by Oracle WebLogic.
- Remarkable University's email server is hosted by Microsoft Outlook.

Data exist in Remarkable University's online learning platform:

- Students' personal information including their first name, last name, age, date of birth, phone number, gender, enrolment details and grade are stored in the database server using oracle software, by staff of administrative level.
- Staffs' personal information including their first name, last name, age, date of birth, phone number, gender and salary are stored in the database server using oracle software, by staff of administrative level.
- Digital books' information is stored in the digital book server and is made accessible for students and staff.
- Communication is facilitated between students and staff, the consequent transmitted email data are stored in the email server.
- Course details are entered by admins upon academics' requests and enrolment details are updated aligning to students' academic decisions and status, regardless, all the data is stored in the course and enrolment server, and is managed by administrators.

Common communication facilities and networks:

- Remarkable University's firewall determines and controls online traffic flow for their online learning platform. Firewall allows in only the students and internal staff and blocks external users from entering the online learning platform.
- Email server and web server are placed under Demilitarised Zone (DMZ) network, DMZ separates Remarkable University's email server and web server from other untrusted networks.
- Hypertext Transfer Protocol Secure (HTTPS) connection protects the integrity and confidentiality of data transmission process between students' and staff' computers and the online learning platform.

Key assets are recognised from the identified relevant assets:

As Remarkable University is an educational organisation, it is required to comply with the two enforced laws, ISO/IEC 27001, and Information Privacy Act 2009 to ensure that no unauthorised access to student and staff's data is permitted. Also, both integrity and confidentiality in students and academics' data should remain uncorrupted and unleaked. In other words, the main focus of an educational organisation such as Remarkable University is to protect student and staff's data privacy from risks and threats, any failure to preserve data privacy would expose Remarkable University to fines and other legal sanctions, and could impact Remarkable University's reputation. Hence, Remarkable University needs to maintain student and staff's data privacy. Though Remarkable University's main organisational focus is on data integrity and confidentiality, however, it is important to note that quick accessibility on data should also be made available to enable for effective and efficient administrative and online learning operations.

The reliability of software such as Oracle Database Software, Apache Tomcat Server, Oracle Weblogic, Microsoft Outlook, LMS and Authentication Server are strongly emphasised. These six software are extra critical to efficient daily administrative and effective online learning operations. Any compromise in the confidentiality, integrity and availability of these physical servers would impact not only the performance in Remarkable University's daily administrative and online learning operations, but will also endanger students' and staff' data privacy and integrity. Hence, these five software are identified as first key assets.

Next, the four physical in-house servers, database, web, and email servers are identified as second key assets. As each particular physical server is hosted by, and stores data for specific software, physical servers are closely linked to the first key assets - software. Therefore, physical servers need to be closely monitored to secure data privacy and to ensure speedy processing of students' and staff' data:

- The database server is hosted by Oracle Database Software.
- The web server is hosted by Apache Tomcat Server.
- The application server is hosted by Oracle Weblogic.
- The email server is hosted by Microsoft Outlook.

Availability and confidentiality of students' and staff' data must not be compromised. Any compromise in data's confidentiality and availability will result in data leakage and denying service. All of which will impact Remarkable University's daily operations.

To better protect the first identified key assets - software, the firewall is deemed essential, as it controls online traffic within Remarkable University, and blocks external users from accessing Remarkable University's data. A failure in blocking any external user’s entrance could lead to potential data modification, data theft, or data deletion by external users, and result in compromising student and staff’ data confidentiality, integrity, and availability, which then further affect Remarkable University’s day-to-day operations. Hence, this is a third key asset.

It is identified that a large amount of crucial data for students and staff are stored on various physical servers and software, and is indicated by Remarkable University the importance in preserving these data’s confidentiality, integrity, and availability. As negligence in maintaining these data’s confidentiality, integrity and availability could bring Remarkable University undesirable scandals. This is a key asset of fourth importance because if the first three key assets are cautiously protected, the fourth key asset - student and staff data should be as well secured.

Lastly, email is identified as the fifth key asset, since the new online learning platform is based online it is presumed that a mass of communication and correspondence between staff and students is predominantly through LMS as well as in the form of emails. Aside from student-staff communication, there are occasional events where staff would need to communicate with head office, as well with other administrative and IT units, and to conduct a large amount of internal correspondence. Email is given greater importance than usual due to the remote location of the learning institution. Hence the collective availability, integrity, and confidentiality of mail services were listed as a key asset.

Relevant assets are summarised into a table as follows, and key assets are bolded:

HARDWARE (In-house servers)	SOFTWARE	DATA	COMMUNICATION FACILITIES AND NETWORKS
Database server	**Oracle Database Software**	**Student's personal information**	**Firewall**
Web server	**Learning Management System (LMS)**	**Personal information of staff**	Demilitarised Zone (DMZ) network
Application server	**Apache Tomcat HTTP Server**	**Email**	Hypertext Transfer Protocol Secure (HTTPS) connections
Email server	**Oracle WebLogic**	Course and enrolment details	
Course and enrolment server	**Microsoft Outlook**	Digital book	
Digital library server	**Authentication server**		
Personal Machine/computer	Operating system		

3. Risk Assessment

These identified key assets are organised into four clustered security areas, user authentication and access control, software security, web and network security, and system and other security for risk assessment purposes.

To assess the risks of key assets:

- the threat/vulnerability, existing controls to these key assets are identified.
- the likelihood and consequence of these identified threat/vulnerability are specified.
- The level of risk in these assets are determined by the likelihood and consequences to identified threat/vulnerability.
- Based on each asset's level of risk, their risk priority is then rated.

3.1 User Authentication and Access Control

3.1.1 Confidentiality and Integrity of Learning Management System (LMS), Authentication Server, Oracle Database, and Oracle Weblogic Software, Microsoft Outlook

Currently, Remarkable University adopts only baseline controls.

Vulnerability in vertical access control: Vertical access controls categorise users into different types of groups, and access to sensitive functionality is granted based on the type of group. With vertical access controls, administrators can modify or delete any user's account, while a general user has no access to these actions (Portswigger, 2020). This difference in accessing power could trigger both internal and external users to conduct malicious activities surrounding the act to seize unauthorised privileges to administrator-level of which allow them to access data of higher critical-value. To gain such access to Remarkable University's application such as Learning Management System (LMS), Authentication Server, Oracle Database, and Oracle Weblogic Software, Microsoft Outlook, it is possible the third-party contractors and other internal users of higher authority could make inappropriate changes to the level of application and database access control, database programs, structures or security configurations. At the same time, other external users have the potential to hijack an admin's account, and from then perhaps escalate privileges to their convenience. From Common Weakness Enumeration(CWE)'s records, the risk associated with improper privilege management

scores ‘Medium’ for likelihood of exploitation. (CWE, 2006) In fact, 58% of organisations found over 1,000 folders associated with inconsistent permissions, and 53% of companies found an excessive number of over 1,000 sensitive files accessible to every employee (Varonis, 2019). Looking at a bigger scope, there’s data targeting companies with over 1 million folders, and within them found that there’s a huge proportion, precisely 80% found over 50,000 folders open to every employee (Varonis, 2019). Furthermore, from the same study of Varonis, in 2019, indicates that on average every employee had access to 17 million files and 1.21 million folders, which can be seen as an aftermath of users making inappropriate changes to level of application and database access control, database programs, structures or security configurations and unauthorized privilege escalation.(Varonis, 2019) Hence, a likelihood of **Likely**, accompanied by a consequence of **Major** is given. The consequence is given a Major because if administrators’ account is hacked, then whoever successfully hacked gains the privileges to modify and delete any information stored on the servers. In point of fact, research directed by Cert has found the most probable class to inflict cyberattacks are system administrators or other employees working in the IT sector with privileged system access. (Whittle, 2008) Regardless, the effect is scoping the whole system of the organisation, let alone the intruder is capable of escalating privilege to their conspirator, which would arouse a chain of subsequent undesirable events harming Integrity and Confidentiality of the assets defined. The judgement is consolidated by CWE’s compiled top 25 most dangerous vulnerabilities, which improper privilege management placed 22. (CWE, 2020) Combining the likelihood rating of unlikely and consequence rating of major, a risk level of **Extreme** is determined, and *3.1.1.b - Internal users made inappropriate changes to level of application and database access control, database programs, structures or security configurations* and *3.1.1.c - Unauthorized privilege escalation performed by external users* is given a first and second risk priority respectively.

Vulnerability in authentication: As 90% of user-generated passwords are considered weak, most are considered easily vulnerable to hacking (Swoop, 2020). One concern with the Authentication Server asset is unauthorised users accessing student and staff’ Remarkable University accounts by using simple manual attacks such as brute-force attacks. Given the commonality and simplicity in conducting a brute-force attack, a likelihood rating **Likely** is given to the risk *3.1.1.a - External users inappropriately accessing students and staff’ sensitive data*. Since brute-force attacks are normally targeting a specific person or group of users, the consequences on the university as a whole are not significant. Still, a specific person or group of Learning Management System (LMS), Oracles software and Microsoft Outlook users' passwords or privacy could be modified and leaked to the public, violating both Confidentiality as well as

Integrity measures. Hence, a consequence rating of **Moderate** is given. Combining the likelihood rating of likely and consequence rating of moderate, the risk level of **High** is then defined, and *3.1.1.a - External users inappropriately accessing students and staff' sensitive data* is given a third risk priority.

Vulnerability in sessional management: Sessional management for web application and server is performed by session cookies, which contain identification for users and this contained identification is maintained and used until that particular session ends, however, one problem with session cookies is that they are not encrypted and is transmitted in clear text if without secure attributes enabled, and external users could take advantage of this vulnerability and execute unsecured session cookie attack (WhiteHat Security, 2020). At this moment, Remarkable University has not enabled secure attributes on their session cookies, raising the possibility for external users sniffing on Remarkable University user's information. If the data sniffing does occur, then the user's information might be observed by external users, which again violates Confidentiality measures. Hence, a likelihood rating of **Likely** is given, and a consequence rating of **Minor** is given. Combining the likelihood rating of likely and the consequence rating of moderate, a risk level of **High** is determined, and *3.1.1.d - Failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack* is given a fourth risk priority.

In the security area of User Authentication and Access Control, half of the identified risks are of extreme level, and the rest are high, which are way above the acceptable minimum management specified as tolerable (moderate or lower risk level). Hence treatment is required.

Asset	**Threat/ Vulnerability**	**Existing Controls** (Baseline Approach)	**Likelihood**	**Consequence**	**Level of Risk**	**Risk Priority**
3.1.1 Confidentiality and Integrity of Learning Management System (LMS), Authentication Server, Oracle Database, and Oracle Weblogic Software, Microsoft Outlook	a. External users inappropriately accessing students and staff' sensitive data.	● Password-based encryption ● Use authentication to verify the person accessing the data.	Likely	Moderate	High	3
	b. Internal users made inappropriate changes to level of application and database access control, database programs, structures or security configurations.	● Vertical access controls	Likely	Major	Extreme	1
	c. Unauthorized privilege escalation performed by external users.	● Vertical access controls	Likely	Major	Extreme	2
	d. Failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack.	-	Likely	Minor	High	4

3.2 Software Security

3.2.1 Availability of Learning Management System (LMS), Oracle database software, Oracle webLogic, Apache Tomcat Server, and Microsoft Outlook

Vulnerability in Anti-virus software: Nothing is 100% secured in this digital world. The world is ever evolving and so are viruses. This is said in view of the number of said new occurring malware variants detected in the year of 2019, as identified by SonicWall, there are 439,854 new malware variants (Cook, 2020). Consequently, anti-virus software can provide brief improvement, but definitely should not be relied on as a standalone protection against malwares. Also, based on reports by Malwarebytes Labs, indicates institutions within the education sector are of weak security posture, and are most likely to fall a prey into intruder's trap. This year, 2020, the education industry has already been hit with a sum of 159,846 reported detections of malware attacks (Malwarebytes Labs, 2020). In perspective of the likelihood of *3.2.1.c - Malware Infections* on Learning Management System (LMS), Oracle Database Software, Oracle WebLogic, Apache Tomcat Server, and Microsoft Outlook, a rating of **Likely** is given. From the 2019 Internet Security Threat Report (ISTR) issued by Symantec Corporation, one of the most reputable cyber security companies in the world, the account has shown a ratio of 1:10 targeted attack groups use malware to either sabotage or disrupt business operations (Symantec, 2019). To assess the consequence level of the risk, the average economic toll of a ransomware attack is taken into account. According to statistics, it is $133,000 for retrieving the locked data (Bera, 2019). At the risk of losing all data, paying $133,000 isn't too bad, however just as the consequences associated with the risk of *3.2.1.b - Inadvertent and intentional unauthorized changes to software's code,* by encounter malware infection, the whole network system is to experience downtime from an attack and the effect can freeze the system, which would infringe the Availability of the software. Thus, a consequence rating of **Major** is provided. Combining the likelihood rating of likely and consequence rating of major, the risk level of **Extreme** is then determined, and *3.2.1.c - Malware infections* is given a first risk priority.

Vulnerability in backed up software code: Though having backups of code that is before corrupted, the network administrator needs time to pull it back up for the public after unauthorized changes have been made to software's code. To gain an insight into how likely it is to experience downtime from an attack, a survey conducted by Mimecast suggests a high mark of 82% out of 1025 IT decision makers have experienced downtime from an attack (Mimecast, 2020). The effect can be large, causing the system to crash, which influences the Availability of the software. Be it inadvertent or intentional, all would inevitably lead to undesirable outcomes, which result in loss financially and also taint the university's reputation. Tracing back to the financial loss,

there is a study from Stripe and Harris Poll calculated the opportunity cost of bad code comes to $85 billion annually (Gaybrick, 2018). Considering above findings, a consequence rating of **Major** is provided. Regarding the likelihood of happening, a rating of **Possible** is given judging based on the aforementioned study. It is discovered in the study that the average programmer spends almost half, precisely 42% of their time handling design or code debt to the software and relevant maintenance issues, in which 3.8 hours are spent purely on troubleshooting badly-written code, or code of poor quality that's difficult to maintain (Avery, 2018). Combining the likelihood rating of possible and consequence rating of major, the risk level of **Extreme** is then defined, and *3.2.1.b - inadvertent and intentional unauthorized changes to software's code* is given a second risk priority.

Vulnerability in organisation's external firewall: It is of no secret that these days the attacks inflicted by hackers are too strong that the external firewall alone would be of not much use to resist an attack. To exacerbate the problem, developers of a software leave flaws that can put software under threats of software exploitation attack, which could foster unwanted system behaviors such as buffer overflow causing the system to crash. From there, the software is more vulnerable to any intruders, creating various security vulnerabilities such as performance degradation, and attacks on other systems. Taking into account that these mistakes are especially problematic with software developed in C/C++ as according to CWE, which does not have built-in protection against buffer overflows (CWE, 2006). In this case, for software used by Remarkable University such as Learning Management System (LMS), Oracle WebLogic, Apache Tomcat Server, and Microsoft Outlook, the chance will not be high to encounter such attacks thus a likelihood rating of **Unlikely** is given to *3.2.1.a - Exploitation on Design flaws and programming bugs* and *3.2.1.d - Buffer Overflow Attacks*, however the chance of Oracle database software, suffering one is still relevant, and this might engender all dependent systems to be of a not-in-working-order state. Considering that the affected area is excessively large, it is foreseeable the Availability of the systems will be impacted, and how much inconveniences would bring to its system users and all end users using Remarkable University's LMS that its interface relies on the unserviceable system. Therefore, it is determined a consequence rating of **Major** is provided. Combining the likelihood rating of unlikely and consequence rating of major, the risk level of **High** is then defined, and *3.2.1.a - Exploitation on Design flaws and programming bugs* and *3.2.1.d - Buffer Overflow Attacks* is given a third and forth risk priority respectively.

Asset	**Threat/ Vulnerability**	**Existing Controls** (Baseline Approach)	**Likelihood**	**Consequence**	**Level of Risk**	**Risk Priority**
3.2.1 Availability of Learning Management System (LMS), Oracle database software, Oracle webLogic, Apache Tomcat Server, and Microsoft Outlook	a. Exploitation on Design flaws and programming bugs	● ISO/IEC 27001 standard sets rules and governs for information security ● Shielded by the organisation's external firewall	Unlikely	Major	High	3
	b. Both inadvertent and intentional unauthorized changes to software's code	● Backed up software code	Possible	Major	Extreme	2
	c. Malware infections	● Anti-virus software	Likely	Major	Extreme	1
	d. Buffer Overflow Attacks	● Shielded by the organisation's external firewall	Unlikely	Major	High	4

3.3 Web and Network Security

3.3.1 Confidentiality, Integrity, and Availability of Firewalls

Vulnerability in only apply security updates for firewalls: Exactly as mentioned earlier in section 3.2.1 about vulnerability in anti-virus software, the same theory holds true for firewalls in that there isn't such a thing as being 100% secure in the digital world, and unfortunately there are times when the fault lies within the people in the organisation itself. As an example, the firewall's misconfiguration can lead to a loss of performance on a company's network in some cases, and a firewall outright failing to provide protection in others, which violates Accessibility of the CIA triad. Further, less advanced firewalls can be easily spoofed by hackers to trick network's firewalls and get in the system to carry out unethical actions thus hurting firewall's Confidentiality and Integrity. More specifically, according to a 2019 cyber criminal case *United States of America v Paige* (2019), "...because[the criminal] involves similar unusual communication through the misconfigured firewall...that the data of approximately 120,000 SSNs and approximately 77,000 bank account numbers have been stolen." Unfortunately, this happens all the time. Gartner noted in one of their 2019 research notes that there was an estimate of 99% of firewall breaches caused by firewall misconfigurations, not firewall flaws (Whitney, 2019). Having no firewalls in this digital age is the same as going in a gunfight barehanded. One CAIDA study concluded that there were almost 30,000 spoofing attacks each day, and within the investigation period spanning from March 1, 2015 and Feb. 28, 2017 alone, there's a total of 21 million attacks on about 6.3 million unique internet protocol addresses (Jonker et al., 2017). Based on the findings, a rating of **Likely** and a consequence rating of **Catastrophic** is decided. Combining the likelihood rating of likely and consequence level of catastrophic, the risk level of **Extreme** is then justified, and *3.3.1.a - Firewall Misconfiguration* and *3.3.1.b - IP Spoofing attacks* is given a first and second risk priority respectively. The majority of risk levels assigned to risks in this section is extreme, *3.3.1.a - Firewall Misconfiguration* is topping the list as a determinative factor for which determines how likely all of the subsequent events will happen upon firewall misconfiguration.

3.3.2. Confidentiality, Integrity, and Availability of Web Server

Vulnerability in Employed SSL/TLS and Same Origin Policy for server: Encryption of the data traffic passed between the parties by using SSL/TLS and same origin policy does prevent the majority of sniffing-style attacks. However, it could still be possible to perform some other kind of session hijack. Cross site scripting (XSS) is a very common web application vulnerability used by attackers to inflict assaults from hijack user accounts, to distribute malware, then to control user's computer remotely and exploit user's applications, as well as seeking capability to bypass access controls such as the same origin policy, as reported by ethical hacker Deepak, there are multiple XSS in HTC website that allow an attacker to inject malicious scripts (Wang, 2012). Moreover, another vulnerability, cookies Handling makes it even easier for an intruder to hijack accounts on the web platform, for example of HTC users (Wang, 2012). For proof of concept, Deepak has demonstrated how he imported the cookie fetched from his created account and logged in without password authentication (Wang, 2012). Aside from the incident with HTC, many websites including enterprises like Microsoft services use cookies to store the session information in the user's web browser. XSS is one of the most well-known web attacks, not only because of its severity upon triggers, but its number of occurrences. According to OWASP, one out of every five tested applications contain vulnerabilities allowing the hackers to attack a user session and perform Cross-Site Scripting (XSS) in order to capture the user's session identifier. Thus, a likelihood rating of **Almost Certain** is given based on the findings. The vulnerability, described by the CWE as "Improper neutralization of input during web page generation", was given a threat score of 46.82, topped the 2020 list of the 25 Most Dangerous Software Weaknesses collated by the Common Weakness Enumeration (CWE, 2020). Further, from OWASP's Top Ten 2017 report, it is found XSS is placed at 7th and its exploitability is scored a 3 out of 3 (OWASP, 2017). In view of this, XSS is deemed to happen, and is not hard to imagine how havoc will be for Remarkable University that intruders compromising Confidentiality and Integrity of web server through cookies can cause students and staff' sensitive information leaked to external users online, and cause irrevocable outcomes for both the victims of data loss and the university to suffer financially. Therefore, a consequence level of **Major** is being decided. Combining the likelihood rating of likely and consequence level of catastrophic, the risk level of **Extreme** is then justified, and *3.3.2.a - Failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack* and *3.2.2.b - Cross-site scripting(XSS) attacks* is given a third and forth risk priority respectively.

Vulnerability in an organisation's external firewall: As mentioned in section 3.2.1, simply relying on firewall to provide protections to systems and files is futile. Aside from XSS attacks, DoS is another common attack of which can impact Web Server's operating speed and can render Web Server unavailable. DoS attacks are often executed with an aim to flood one targeted server, and can be performed using a single computer and a single IP address to attack one specific target (Weisman, 2020), DoS attack is deemed to be a simple but an effective attack, a successful DoS attack can cause significant financial and time ramifications (Keary, 2020). Statistically speaking, 51% of businesses experienced DoS attacks in 2018 (Milkovich, 2020). To be more specific, 20% of companies with 50 or more employees admitted to at least one DoS attack, as extracted from Kaspersky's examination. That proportion however, varies among industries, with telecommunications companies on a mark of 24% being the highest chances of getting hit with DoS attack and 9% of professional services have suffered from an attack. Educational institutions are at 15%, which are situated in the mid-tier of the range (Kaspersky Lab, 2018). While in the balance of determining the likelihood rating for the risk as possible, it is found in Kaspersky's study also, they have raised a point where DoS is frequently used as a decoy to distract IT staff from an intrusion taking place at the same time, which means the actual statistics of DoS attack could be lower than provided. Taking all factors in, it is decided a likelihood rating of **Unlikely** for the risk *3.3.2.c - DoS attacks inflicted by intruders*, and a consequence rating of **Catastrophic** is given. The consequence rating is given with contemplation of the effect on Remarkable University. If hackers inflict Flood-attacks and Crash attacks (DoS attacks) it stops legitimate users from accessing online services, and can make the system eventually crash, which prohibits Availability of the web server (CISA, 2019). Monetarily speaking, on the authority of Bulletproof's 2019 Annual Cyber Security Report, it indicates that a DoS attack could cost up to $120,000 for a small company or considering Remarkable University's scale, that will be more than $2 million out of their pocket for an enterprise organization (Bulletproof, 2019). That also equates to a great deal of apologies to students and staff for data and reputation loss. Combining the likelihood rating of unlikely and consequence level of catastrophic, the risk level of **Extreme** is then justified, and *3.3.2.c - DoS attacks inflicted by intruders* is given a third priority.

3.3.3 Confidentiality and Accessibility of Mail Server

Vulnerability in SMTP authentication and DNSBL servers: Have in place the SMTP authentication and DNS-based blacklists (DNSBL) helps increase security of users' accounts while preventing open relay and abuse of the mail server itself. However, the intruder can impersonate a person of a legitimate account and circumvent, turning the utilisation of SMTP and DNSBL to no effect. Worse yet, there is little effort and attention paid to examine the content of an incoming email sent to the users. As of concern, there should be measures established in the prevention of the malicious content, especially malware that might embed in the email to harm users in any way. To assess the likelihood of one MITM attack, it is necessary to look at some figures. From statistics, it is found by Memecast that on average, there are 9 web or email spoofing attacks per organization each year, and that's just what they know about. From the same group, there are 49% of 1025 respondents anticipating an increase in web or email spoofing in 2020, and the 84% are concerned about email domain spoofing attacks (Mimecast, 2020). Inferring from that, it is believed the likelihood ranking of the risk is **Likely**. Moving to view and assess the consequence ranking of the risk, it is discovered that 90% of malware comes from emails (Dark Reading, 2018), and nearly one in ten targeted attack groups use malware to destroy or disrupt business operations (Symantec, 2019). Indeed, the result of a MITM attack in the form of email hijacking can be severe, it is expected once the Man-in-the-middle spoof one email communication, they are able to send their own instructions and malicious attachment to the victim email owners as the counterpart, which could leak user's personal details, or crash their computer system and led to financial loss. All of which taints Confidentiality and Accessibility of mail server. On this point, 96% of 1025 respondents of Memecast have confessed that during usage of Microsoft 365 for email delivery, the impact to their organizations following an outage or other security event created a lasting impression of the need to build in greater resilience with components like email security (Mimecast, 2020). In this framework, it is reviewed that a consequence level of **Catastrophic** should be given. Combining the likelihood rating of likely and consequence level of catastrophic, the risk level of **Extreme** is then accounted for, and *3.3.3.a - MITM attack in the form of email hijacking* is given a third priority.

Asset	**Threat/ Vulnerability**	**Existing Controls** (Baseline Approach)	**Likelihood**	**Consequence**	**Level of Risk**	**Risk Priority**
3.3.1 Confidentiality and Availability of Firewalls	a. Firewall misconfiguration	● Ensured to apply security updates for firewall software as soon as possible	Likely	Catastrophic	Extreme	1
	b. IP Spoofing attacks	● Ensured to apply security updates for firewall software as soon as possible	Likely	Catastrophic	Extreme	2
3.3.2. Confidentiality, Integrity, and Availability of Web Server	a. Failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack	● Cookie is HttpOnly so it is not accessible to JavaScript. ● Employed SSL/TLS for server ● Multiple instances of a web application not sharing a Wildcard certificate so the principle of least privilege is not violated.	Almost Certain	Major	Extreme	6

		• Same origin policy				
	b. Cross-site scripting(XSS) attacks	• Employed SSL/TLS for server	Almost Certain	Major	Extreme	5
	c. DoS attacks inflicted by intruders	• Firewall	Unlikely	Catastrophic	Extreme	4
3.3.3 Confidentiality, Integrity and Accessibility of Mail Server	a. MITM attack in the form of email hijacking	• Have Setted up SMTP authentication to control user access • Use DNSBL servers to fight spammers	Likely	Catastrophic	Extreme	3

3.4 System and Other Security

3.4.1 Confidentiality and Availability of Database server

There are no existing controls to govern the possible risks of *3.4.1.a - Age of the equipment and overheat of database hardware* and *3.4.1.b - Probable damage on database server hardware by unpredictable natural disasters*. Naturally, when parts or all components of the database server hardware need to be replaced, the Oracle database it serves will be inaccessible and causing inconvenience for users. There are researches that examine the failure rates of servers in correlation of the age of the equipment, that have found that a four year-old server has an 11% annual failure frequency, accounting for a 6% increase compared to the rate of failure in a server's first year sits at 5% (Statista, 2014). Despite the seemingly trivial effect of annual failure frequency, consequences could be significant if hardware affected are impossible to restore after a natural deterioration or disasters, for such would include thunderstorms and floods etcetera. Regarding the likelihood of such risks occurring, there are numbers indicated that 35% of outages are caused by natural disasters (Datacore, 2018). Moreover, studies have been undertaken by analyst group Dynamic Technologies to

unveil that hardware failures are responsible for causing 45% of total unplanned downtime (Dynamic Technologies, 2017). Above findings suggests that the likelihood rating of the risk is not too likely, but **Possible**. The consequences in which the Remarkable University will embroil is out of question, the Confidentiality and Availability of servers is violated. When it comes to the costs of the risk, which in this case is data loss and monetary value. Direct costs for equipment can be computed according to research firm Gartner, that can be summarised to the average cost of downtime around $5,600 per minute, equivalent to $300,000 an hour. There is also data providing an estimate of how many hours an organisation needs to recover from a natural disaster, and it turns out that 56% would need more than 8 hours to restore 100% of data (Datacore, 2018). While $300,000 per hour is a fortune to pay, what's more devastating for Remarkable University is the risk can be damaging for organizations when it could be possible they are forced to shut down due to a drop in students' and employees' trust (Lerner, 2014). To indicate the graveness of the risk, there is data highlighting an alarming percentage of 93% of companies without Disaster Recovery who suffer a major data disaster are out of business within one year. In this context, the consequence level of *3.4.1.a - Age of the equipment and overheat of database hardware* and *3.4.1.b - Probable damage on database server hardware by unpredictable natural disasters* is selected as **Major** and **Catastrophic** respectively. Both combining the likelihood rating and consequence level of (possible, catastrophic) and (major, catastrophic), a risk level of **Extreme** is determined for both. *3.4.1.a - Age of the equipment and overheat of database hardware* and *3.4.1.b - Probable damage on database server hardware by unpredictable natural disasters* is given a sixth and first risk priority respectively.

Vulnerability in CCTV monitors: CCTV monitors are good tools for direct employee monitoring. However, there could even be down time for CCTV monitors, taking this into account only pinpoints the need for additional controls on the matter of employee monitoring. It is paramount for more secure servers and therein the network system and data. There is an Insider Threat Report from CA Technologies, which has declared databases topping the list of most vulnerable IT assets. In fact, half of cybersecurity professionals have chosen databases as their most vulnerable asset (Observe IT, 2019). The need for a more sophisticated control for supervising employees is conspicuous in view of more research performed by the US Computer Emergency Response Team, and as stated, 40% of IT security breaches are approximated to be perpetrated by insiders of the organisation (Whittle, 2008). To complement the studies, there is data surrounding the group that's likely to undertake criminal attacks out of all committed crimes, which is estimated at a shocking 90% attempted by employees of the company attacked (Whittle, 2008). A likelihood rating of possible was to be given after

averaging the numbers indicated in the statistics, however judging by the surveillance of CCTV, it is contemplated that an **Unlikely** is supplied to the risk *3.4.1.c - Insider attack on physical server machine*. The consequence level of the risk sits **Catastrophic**. The consequence level was determined upon the severity of interruption of business if an insider attack on the physical server were to occur, tainting Accessibility of the server. Borrowing words from Wyss, who states “An [insider] attacker gains physical access to a physical asset in the infrastructure system in order to damage it, disable it, steal it, or use it in an undesirable way” (Wyss et al., 2007). If that is true by Wyss, and like pointed out by Resolver, that ‘An attacker breaks into a server room and installs rogue devices to capture confidential data’ among some other common examples of how physical threat vectors can compromise digital security (Resolver, 2018), then it is frightfully how it is going to influence Remarkable University. It is foreseeable there would be an eviatible financial loss and serious legal consequences if personal information of staff or students were disclosed to the public or if important process information about the organisation were lost. As such, the likelihood rating of possible and consequence level of catastrophic was considered, the risk level of **Extreme** is then accounted for, and *3.4.1.c - Insider attack on physical server machine* is given a second priority. It needs higher priority, just below *3.4.1.b - Probable damage on database server hardware by unpredictable natural disasters***.** Most of the insider attacks are with malicious intent, their actions are unpredictable and need to be dealt with quickly before mishap happens.

3.4.2 Confidentiality, Integrity and Availability of stored file and database information

Vulnerability in having only general policies and abiding only Privacy Acts:

It is pronounced that the Remarkable University is exercising the government legislation and regulation, for such Privacy Act 1988 and Information Privacy Act 2009 is to be abide to maintain data Confidentiality and Integrity of students and academics, and strictly prohibited any unauthorised access to student’s and employee’s data (Griffith University Procedure, 2020). Furthermore, associates of Remarkable University are expected to follow university-established data breach management policies that’s inaugurated to be obeyed to ensure data breaches are appropriately managed. The company also has policies on the input and handling of a range of data, especially that required for audit purposes. However, it raises concern when there are only policies, and no actual documents or records to monitor who have touched the data, and the inadequacy of physical security protection such as lack of access control or data encryption used to govern the data security of students’ or staff’ data. The deficiency

can make Remarkable University's data vulnerable to anyone external, but what's more agitating for the organisation is if there were any insiders waiting to snatch the valuable data away from the university's database. In the concrete, according to Verizon, there are 34% of data breaches in 2018 involving internal actors (Verizon, 2018). To validate the point, the IT, telecoms and technology sector reports that 70% have been hit by malicious activity spread amongst employees (Mimecast, 2020). As raised in *3.4.1.c - Insider attack on physical server machine,* attacks initiated by insiders are indeed one of the most crucial yet the easiest to overlook. Nevertheless, it is not always the malicious insider, sometimes the careless insider that intends no harm but does harm to the organisation that leads to data leakage. As one study found human error is the number one cause of security and data breaches, responsible for 52 percent of incidents (Greenberg, 2015). A likelihood rating of **Possible** has been decided upon analysis of the context. A consequence level is decided following the read of Ponemon's post regarding the average cost of a data breach, which suggested by Ponemon is $3.92 million as of 2019 (Ponemon, 2019). A substantial amount of financial loss is definite if a data breach is to happen and serious legal consequences are possible if personal information were disclosed or if important process information about the organisation were lost. Further, since in this case concerns the internal actors of the organisation, in most cases insiders will have more access to databases, therefore the scale of releasing or modification of data can be large, which would be violating Confidentiality and Integrity respectively. In event of deletion of data would affect Availability of stored file and database information of students' and staff' personal information.
However, data theft or leakage wouldn't cause any network system to go down or corrupt entirely, which isn't as critical compared to the risks given catastrophic consequence level - Remarkable University is still capable of business operating. In view of the effect, a consequence level of **Major** is given. Combining the likelihood rating of possible and consequence level of major, the risk level of **Extreme** is then determined, and *3.4.2.a - Insider attack on data stored on computers* and *3.4.2.c - Unintentional deletion, modification, or disclosure of information Insider attack on data stored on computers* is given a third priority and fifth priority respectively. *3.4.2.a - Insider attack on data stored on computers* is of similar level of priority to *3.4.1.c - Insider attack on physical server machine*, for the same reason that the insider attacks are unpredictable and usually destructive to an extent, so need to be dealt with quickly.

There are no existing controls to govern the possible risks of *3.4.2.c - SQL Injection.* However, care and attention should be given to address the risk of *3.4.2.c - SQL Injection*. SQL injection, its operation is relatively easy to implement in comparison to the dozens of much more complicated attacks such as botnet attacks, this simplicity in implementation made it another of the most common cyberattack on web platforms.

SQL injections can be extremely destructive in that it can be utilized to modify SQL database query logic to circumvent security checks, or to insert additional statements that would execute and cause irrevocable data-loss or other assaults to the back-end database, possibly including execution of system commands. For example, on the LMS platform where users can input substances of code, possibly in discussion or comment sections of the LMS component, the malicious user can provide a SQL command that if triggers would display error message box printing a specific student's personal detail etcetera. Once again, if the data has been deleted or modified or leaked without data owner's authorisation would breach Availability of users' data, as well as its Integrity and Confidentiality correspondingly. The likelihood of the risk associated with SQL injections is assessed based on Akamai's 'State of the Internet' report and their observation on credential abuse attacks across their customer base. On the authority of Akamai, SQL Injection (SQLi) accounted for more than 72% of all attacks when looking at all verticals, that comprised 7,957,307,672 subjects of interest (Akamai, 2020). With large sample sizes give more reliable results with greater precision and power, it assists in assuring a **Likely** likelihood rating. The vulnerability, described by the CWE as "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')" was given a threat score of 20.69, situated itself a 6th place on the 2020 list of the 25 Most Dangerous Software Weaknesses collated by the Common Weakness Enumeration (CWE, 2020). After having examined the outcomes of SQL injection, while taking into account the relevant CWE rating, a consequence level of **Major** is decided. As such, the likelihood rating of likely and consequence level of major was considered, the risk level of **Extreme** is then accounted for, and *3.4.2.c - SQL Injection* is given a fourth priority.

Asset	**Threat/ Vulnerability**	**Existing Controls** (Baseline Approach)	**Likelihood**	**Consequence**	**Level of Risk**	**Risk Priority**
3.4.1 Confidentiality, Availability of Database server	a. Age of the equipment and overheat of database hardware	-	Possible	Major	Extreme	6
	b. Probable damage on database server hardware by unpredictable natural disasters	-	Possible	Catastrophic	Extreme	1
	c. Insider attack on physical server machine	● CCTV monitors	Unlikely	Catastrophic	Extreme	2
3.4.2 Confidentiality and Integrity of stored file and database information	a. Insider attack on data stored on computers	● Privacy Act 1988 ● Information Privacy Act 2009 ● General data breach management policies ● Policies on the input and handling of a range of data	Possible	Major	Extreme	3

	b. SQL Injection	-	Likely	Major	Extreme	4
	c. Unintentional deletion, modification, or disclosure of information	● Privacy Act 1988 ● Information Privacy Act 2009 ● General data breach management policies ● Policies on the input and handling of a range of data	Possible	Major	Extreme	5

4. Security Strategies

Given the outcome of the risk assessment for Remarkable University, the next stage in the security management process is to select the most appropriate controls among recommended controls based on the result of the cost and benefit analysis conducted on the recommended controls. Management must decide which amount of residual risk is acceptable for the organization and select the appropriate controls based on this decision.

4.1 User Authentication and Access Control

4.1.1 Cost and Benefit analysis on Recommended Controls for risk 3.1.1.a

For risk 3.1.1.a, external users inappropriately accessing students and staff' sensitive data. The selected controls are control 1, and control 2, but not control 3.

- Control 1: Enforce organisational policies such as separation of duties and least privilege.
- Control 2: Conduct regular scans using monitoring tools to expose suspicious activity and unauthorized attempts to access data, and flag them in audit logs that can be scanned for suspicious behavior.
- Control 3: Make sure sensitive data can be accessed only by authorized employees who have a legitimate reason to access it.

Most unauthorised access is allowed in because of one organisation's lack of thorough scanning and regular monitoring in network traffic. To reduce risk 3.1.1.a, Remarkable University will need controls that support scanning, monitoring and regulating the network traffic. Hence, Control 2 is selected as the primary treatment for this risk.

However, with only Control 2 alone does not reduce the risk sufficiently. Normally, most scanning and monitoring can prevent only simple, common, and known attacks from getting inside one organisation's Authentication Server, meaning that it cannot fully resist difficult attacks such as DDoS from getting inside the organisation's Authentication Server. Hence, instead of just having Control 2, Control 1 which enforces organisational policies such as separation of duties and least privilege will also be selected to provide further control to reduce risk 3.1.1.a. With Control 1, external users who gained access to Authentication Server can perform only limited tasks because

they are given only a limited amount of privileges. Control 3 is not selected, since Control 1 provides similar control and better protection compared to Control 3 in this case.

To implement Control 1 and Control 2, cyber threat defense senior manager (Griffith University, 2020) will need 7 days to write and enforce organisational policies for separation of duties and least privilege, and it will take 3 days for identity management administrators (Griffith University, 2020) to verify and change monitoring tools to adapt for regular scanning on Authentication Server. Identity management administrators need to perform day-to-day security administration, they should monitor and flag any suspicious activities and unauthorised access in audit logs. Lastly, 1 day for educating and training all internal users is needed to help ensure that these policies are strictly followed.

4.1.2 Cost and Benefit analysis on Recommended Controls for risk 3.1.1.b

To reduce risk 3.1.1.b, internal users made inappropriate changes to level of application and database access control, database programs, structures or security configurations. Control 1 and 2 are both selected.

- Control 1: Enforce privilege escalation monitoring and role management.
- Control 2: Regularly review administrative accounts and revoke them if access is no longer needed.

To prevent internal users from making inappropriate changes to the level of application and database access control, database programs, structure or security configurations, it would be best to monitor the internal user's privilege escalation activities, and to make privilege escalation option available only to Remarkable University's database administrators, and not to staff and students (Griffith University, 2020). To achieve this, privilege escalation monitoring and role management needs to be enforced, hence Control 1 is selected. With the adoption of Control 1, it is made difficult for ungranted internal users to gain privileged access to database and security configures.

Though using solely Control 1 will be enough if the risk is lower, however due to the extreme risk level of 3.1.1.b, further control such as regular review of administrative accounts and internal user's privilege access needs to be managed by database administrators. Hence, Control 2 is selected as well as Control 1.

To enforce Control 1 and Control 2, cyber network administrators will need 5 days to configure for privilege escalation monitoring and role management. Database administrators are required to perform day-day database administration, this includes daily privilege escalation monitoring, regular review of administrative accounts and revoke them if access is no longer needed.

4.1.3 Cost and Benefit analysis on Recommended Controls for risk 3.1.1.c

To reduce risk 3.1.1.c, unauthorized privilege escalation performed by external users. Both Control 1 and Control 2 are selected.

- Control 1: Permissions should come with strict limitations on the length of time for when internal users are using their account.
- Control 2: Limit the type of permissions internal users can simply request themselves.

Due to the reason being attackers from external environments often take over an existing account, for example the student account in this case, with an intention to gain more privileged access. Currently, Remarkable University has some existing controls such as vertical access control in place to protect against administrative privilege being unauthorisedly escalated by external users (Cynet, 2020). Vertical privilege escalation can help prevent this, but that is only when vertical privilege escalation is properly structured. If the vertical access control allows student accounts to have more privileges than they actually need, such as updating to a staff account. Then, Remarkable University is risking its vertical access control model to be compromised by external attackers. Hence, both Control 1 and 2 are in need to prevent this by setting limitations on internal user's account restrictions, and limiting internal users' privilege access. Having a minimum privilege set for internal users significantly decreases the amount of activities that is available for hackers to perform, hence consequently reducing the risk 3.1.1.c.

To implement Control 1 and 2 for risk 3.1.1.c, identity management administrators will need 1 day to set limitations on the length of time on internal users' login sessions, and 2 days are required for database administrators to limit internal users privilege to have only general access.

4.1.4 Cost and Benefit analysis on Recommended Controls for risk 3.1.1.d

To reduce risk 3.1.1.d, failure in session management, cookie information stolen and sniffed by external users using unencrypted session cookie attack. Both Control 1 and 2 are implemented.

- Control 1: Set HttpOnly flag of session cookies to disable its accessibility to JavaScript's Document.cookie.
- Control 2: Set Secure flag of session cookies to enable encrypted connections.

Currently, Remarkable University has not changed the setting of session cookies, the attributes of session cookies are on default. By default, the HttpOnly and Secure attributes of session cookies are disabled. A session cookie without HttpOnly enabled is readable from the front-end JavaScript code, and a session cookie with Secure attributes disabled will be sent as plaintext through an unencrypted connection. With these attributes unset, Remarkable University's session cookies can be easily targeted by malicious users online. To reduce the risks of being targeted by malicious users, session cookies need to be properly secured. Hence to sufficiently reduce risk 3.1.1.d, Control 1 is selected to set the HttpOnly flag of session cookies and to disable its accessibility to JavaScript's Document.cookie. Control 2 is selected to set the Secure flag of session cookies and to enable session cookies to traverse on encrypted connections. With these attributes set, the likelihood of a successful attack can be sufficiently reduced.

To implement Control 1 and 2, cyber network administrators will need 0.5 day to set HttpOnly and Secure flags for session cookies. Though the priority of risk 3.1.1.d is lower than risk 3.1.1.a, 3.1.1.b, and 3.1.1.c, however since only 0.5 days is required for network administrators to implement Control 1 and 2, this should be completed as soon as possible.

Risk (Asset/Threat)	**Level of Risk**	**Recommended Controls**	**Selected Controls**	**Required Resources**
External users inappropriately accessing students and staff' sensitive data. (refer to 3.1.1.a)	High	Control 1: Enforce organisational policies such as separation of duties and least privilege. Control 2: Conduct regular scans using monitoring tools to expose suspicious activity and unauthorized attempts to access data, and flag them in audit logs that can be scanned for suspicious behavior. Control 3: Make sure sensitive data can be accessed only by authorized employees who have a legitimate reason to access it.	Control 1 and 2	7 days for cyber threat defense senior managers to write policies. 3 days for identity management administrators to verify and change monitoring tools to adapt for regular scanning on Authentication Server. Identity management administrators performing day-to-day security administration. 1 day for educating and training all internal users is needed to help ensure that these policies are strictly followed.
Internal users made inappropriate changes to level of application and database access control, database programs, structures or security configurations. (refer to 3.1.1.b)	Extreme	Control 1: Enforce privilege escalation monitoring and role management. Control 2: Regularly review administrative accounts and revoke them if access is no longer needed.	Control 1 and 2	5 days for cyber network administrators to configure for privilege escalation monitoring and role management. On a daily basis, database administrators should review administrative accounts, and manage access revocation on accounts.
Unauthorized privilege escalation	Extreme	Control 1: Permissions should come with strict limitations on the length of time for when internal users are using their account.	Control 1 and 2	1 day for identity management administrators to set limitations

performed by external users. (refer to 3.1.1.c)		Control 2: Limit the type of permissions internal users can simply request themselves.		on the length of time on internal users' login sessions. 2 days for database administrators to limit internal users privilege to have only general access.
Failure in session management, cookie information stolen and sniffed by external users using unencrypted session cookie attack. (refer to 3.1.1.d)	High	Control 1: Set HttpOnly flag of session cookies to disable its accessibility to JavaScript's Document.cookie. Control 2: Set Secure flag of session cookies to enable encrypted connections.	Control 1 and 2	0.5 day for cyber network administrators to set HttpOnly and Secure flags for session cookies.

4.2 Software Security

4.2.1 Cost and Benefit analysis on Recommended Controls for risk 3.2.1.a

To reduce risk 3.2.1.a, exploitation on Design flaws and programming bugs. Control 1 and 2 are selected, but not Control 3.

- Control 1: Adapt to proper software quality assurance activities such as code review.
- Control 2: Use of Static Application Security Testing (SAST)
- Control 3: Use formal methods hackers often adopt such as Dynamic Application Security Testing (DAST) to detect design flaws before a hacker does in a given running application.

It is known that most exploitation on software results from exploitation of design flaws and programming bugs, and most design flaws and programming bugs are generated because of programmer's 'tired eyes'. It is difficult for programmers themselves to spot design flaws and programming bugs in their own software they code, because they have stared at the same code for too long, their eyes are already adapted to the code. Hence, to reduce the amount of design flaws and programming bugs in software, code reviews are essential, programmers should ask their fellow-programmers who have 'fresher eyes' than themselves to review their code for them. However, solely human error detection is not sufficient to reduce the risk 3.2.1.a, as there might still be some detailed errors human eyes cannot catch, and because of such reason, tools such as Static Application Security Testing (SAST) are highly recommended to use (Koussa, 2018). Hence Control 1 and 2 are selected.

The combination usage of Control 1 and 2 sufficiently reduces the risk 3.2.1.a, hence Control 3 is not adopted. Control 3 might be used if the risk level of 3.2.1.a is extreme, however considering its current risk level of being high, and since Dynamic Application Security Testing (DAST) is more expensive to conduct compared to SAST, Control 3 will not be adopted to address the current level of risk 3.2.1.a.

To implement Control 1 and 2, the quality assurance team will need 1 day of educating on good coding practices, and 2 days to train quality assurance teams to use SAST.

4.2.2 Cost and Benefit analysis on Recommended Controls for risk 3.2.1.b

To reduce risk 3.2.1.b, both inadvertent and intentional unauthorised changes to software's code. Control 1 and 2 are selected.

- Control 1: Use version control features of the repository to track all changes made to code with accountability to the individual developer account.
- Control 2: Monitor files and folder for change in real-time

Due to the advance of technology, hackers' technological skill advances too, they conduct inadvertent and intentional unauthorised changes to software code and make public the software's source code, causing information leakage to organisations. Information leakage will do no good to any organisations including Remarkable University. Hence, to prevent this from happening, any changes to software should be tracked using version control tools such as Git, and changes to files and folders should be monitored.

The adoption of version control tools, and files and folders monitoring can help to spot suspicious activities efficiently and immediately. Nowadays, many programmers spend more time on fixing maintenance issues rather than developing new software. These adoptions can reduce the amount of maintenance issues and decrease the amount of time invested in troubleshooting for maintenance issues, as well as decreasing the chance for information leakage of software's source code to occur. Hence, Control 1 and 2 are selected.

To implement Control 1 and 2, 1 day educating and training for the software configuration management team on using version control tools such as Git is required. Also, cyber network administrators should monitor files and folders on a daily basis to look out for inadvertent and intentional unauthorised changes made to software's code.

4.2.3 Cost and Benefit analysis on Recommended Controls for risk 3.2.1.c

To reduce risk 3.2.1.c, malware infections. Control 1, 2, and 3 are selected.

- Control 1: Back up important files and folders regularly.
- Control 2: Update security software frequently and patches required.
- Control 3: Train internal users basic ransomware attack prevention.

Ransomware attacks are attacks that encrypt one organisation's file and folders including all important documents and threaten one organisation for the exchange of financial resources, and they are one major type of the malware attacks that are commonly-encountered by educational institutions. With all important documents locked, one organisation might face unavailability in systems and daily operations. Hence, Remarkable University needs protection against such attacks.

Control 1 is selected to prevent ransomware attacks, Remarkable University will need to back up their important files and folders regularly. As there will be no need to unlock encrypted important files and folders, and Remarkable University does not need to pay to unlock their files and folders if they have another copy of that files and folders. The problem with this approach is the concern of attackers behind the ransomware spreading unlocked files and folders' information to the public as the attackers have not received payment from Remarkable University. Therefore, using merely Control 1 does not sufficiently reduce risk. To sufficiently reduce risk 3.2.1.c, Remarkable University should not only be backing up their important files and folders, but also updating their security software and patches, and training their internal users' ways to prevent against basic ransomware attacks. Hence, Control 1, 2, and 3 are all selected.

To implement Control 1, 2, and 3, daily back up should be performed by cyber network administrators. Cyber security network administrators check for updates daily, and need to apply patches monthly. 1 day is required for cyber network administrators to test out patches on test environments, and 3 days are needed for training internal users basic ransomware attack prevention. Training should provide internal users insights of not to click on untrusted links, and not to give personal information to untrusted websites (Norton, 2020).

4.2.4 Cost and Benefit analysis on Recommended Controls for risk 3.2.1.d

To reduce risk 3.2.1.d, buffer overflow attacks. Control 1, 2, and 3 are selected.

- Control 1: Adopt Address Space Layout Randomization (ASLR)
- Control 2: Use Data Execution Prevention (DEP)

Insufficient memory checking and management could lead to potential buffer overflows, and buffer overflows often are vulnerable to exploitation by attackers. Mostly, attackers use this vulnerability to overwrite the memory of organisations' software, damage important files and folders of organisations, causing system unavailability and private information leakage. All of which are events organisations want to eliminate. To reduce buffer overflow attacks, and to sufficiently check and manage memory, Control 1 and 2 are selected and used cohesively.

Typically, buffer overflow attacks rely heavily on the static location of executable code, hence Control 1, ASLR is selected, as it randomly moves around the address space locations of memory regions, which makes buffer overflow attacks difficult to be conducted. Additionally, Control 2 is also selected, as the amount of buffer overflow attacks can be reduced by using DEP. DEP flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region. The cohesive use of Control 1 and 2 can reduce the amount of risk 3.2.1.d on Remarkable University, preserve system’s availability, and keep information private and unleaked.

To implement Control 1 and 2, database administrators will need 7 days to implement ASLR and DEP.

Risk (Asset/Threat)	**Level of Risk**	**Recommended Controls**	**Selected Controls**	**Required Resources**
Exploitation on Design flaws and programming bugs (refer to 3.2.1.a)	High	Control 1: Adapt to proper software quality assurance activities such as code review. Control 2: Use of Static Application Security Testing (SAST) Control 3: Use formal methods hackers often adopt such as Dynamic Application Security Testing (DAST) to detect design flaws before a hacker does in a given running application.	Control 1 and 2	1 day educating and training for the quality assurance team on good coding practices. 2 days for educating and training quality assurance teams to use SAST.
Both inadvertent and intentional unauthorized changes to software's code (refer to 3.2.1.b)	Extreme	Control 1: Use version control features of the repository to track all changes made to code with accountability to the individual developer account. Control 2: Monitor files and folder for change in real-time	Control 1 and 2	1 day educating and training for the software configuration management team on using version control tools such as Git. Cyber network administrators should monitor files and folders on a day-to-day basis.
Malware infections (refer to 3.2.1.c)	Extreme	Control 1: Back up important files and folders regularly. Control 2: Update security software frequently and patches required. Control 3: Train internal user basic ransomware attack prevention.	Control 1, 2 and 3	Daily back up should be performed by cyber network administrators. Cyber security network administrators check for updates daily. Cyber network administrators apply patches monthly. 1 day for cyber network administrators to test out patches on test environments.

				3 days of training internal users basic ransomware attack prevention.
Buffer overflow attacks (refer to 3.2.1.d)	High	Control 1: Adopt Address Space Layout Randomization (ASLR) Control 2: Use Data Execution Prevention (DEP)		7 days for database administrators to implement ASLR and DEP.

4.3 Web and Network Security

4.3.1 Cost and Benefit analysis on Recommended Controls for risk 3.3.1.a

For risk 3.3.1.a, firewalls are not correctly configured. Both Control 1 and 2 are selected as effective controls.

- Control 1: Need to disable dynamic routing so it won't result in a loss of control that reduces security, and creates a vulnerability in firewall protection.
- Control 2: Automating firewall configuration capable of maximizing efficiency while reducing the expenditures on operational and security and reducing human error by eliminating misconfigurations that could otherwise increase the attack surface.

The company is so vulnerable to cyber attacks, while there are many causes to this, one of the prominent factors is the loss of control that reduces security, and creates a vulnerability in firewalls. To completely remove the risk or at least minimize the effect of the risk accompanying risk 3.3.1.a, Remarkable University has two options: Control 1 for simple fix which would improve slightly the functions of current misconfigured firewalls with no cost. Conversely, there is Control 2, for which would require a lot of effort, knowledge and time to establish a new method in managing the firewall, that is automation. However, the outcome of having configured the firewalls is fruitful with optimal controls.

Control 2 is selected in this case as the main control, and Control 1 is the backup plan to follow if Control 2 appears to not suit, as usually it is hard to implement in the sense of time and monetary resources contributed to the process of automate implementation. In some unfortunate cases, they even collapse all together, forcing the people to return to their original manual processes they were on before seeking to automate. However, that is what happens when executing the process without a plan, and for an organisation of a scale like Remarkable University consisting of so much critical data relevant to the organisation and its people is even more so important, since the firewall is going to take effect on a bigger scope covering staff and students.

The steps to implement Control 2, an automation of firewall, is well documented in Algosec's Automating Firewall Change Management Plan, which can be used as reference for an insight into the process of performing and bringing to life a firewall automation. On that note, the process was simplified for this case and is summarised down to 1. get proper authorization from Manager Cyber Threat Defence for the change

to opt to firewall automation, 2. backup existing configurations, 3. audit and govern the change process, and 4. recertify policies (Algosec, 2018).

Fully automating firewall configuration will be capable of maximizing efficiency while reducing the expenditures on operational and security. There are also benefits of it reducing human errors by eliminating misconfigurations that would otherwise increase the attack surface. Effectively, there would be less worry for spoof attacks or DoS by hackers to trick network's firewalls and get in the system to carry out unethical actions.

Nevertheless, as of Control 1, it will be used to replace Control 2 if Remarkable University decides the effort and time is too much to afford. Regardless, in both cases, there is a need for the Manager Cyber Threat Defence to establish and implement standards and related procedures for access to information systems belonging to the University. Control 1 only constitutes a minor change, which would require 1 day for modifying the standards. However, Control 2 would tolerate calculations in months, it is approximated at least 3 months for new standards and procedure development in review of the Cyber Security Risk Register and selecting, implementing and administering controls and procedures to manage information security risks, in order to develop automation and better controls for firewalls (Griffith University, 2020).

4.3.2 Cost and Benefit analysis on Recommended Controls for risk 3.3.1.b

For risk 3.3.1.b, IP Spoofing attacks are used on systems with flaws open to exploitation.

- Control 1: Have internal firewalls on top of perimeter firewalls to help partition individual assets on the network.
- Control 2: VPN protection strategies against IP spoofing attacks, using key-based encryption to create a subnet for secure communication.

IP spoofing attack was one of the attacks suffered by the Remarkable University due to their weak security posture. IP spoofing is distinctive to have a modified source IP address in order to either hide the identity of the offender, or to impersonate another legitimate user from the university. That fraudulent identity will then be used to communicate with the sufferer of this attack, and will result in the loss of users' personal information such as the revelation of password to the students' or staff' account to the LMS as well as their personal information that should remain secret however being eavesdropped or spied on by a malicious attacker.

To prevent such a miserable event, there are 2 controls to be implemented. Currently, the Remarkable University only has an external firewall. However with a resolve to improve the overall security, it is decided to have a control, which is Control 1, that there are needs for an internal firewalls to help partition individual assets on the network so attackers have to work harder to move from one system to another one. This helps increase the attacker's breakout time so system admin have more time to respond to the attack. This is one solution to provide to staff or students who are comfortable with only traditional controls. Another way, as specified in Control 2, is by the use of VPN protection strategies, using key-based encryption to create a subnet for secure communication. What this means is that, even if an attacker gains access to Remarkable University's user data, they would not be able to read nor can they modify it, and so they will not be able to start an attack.

Again, like there is a need for the Manager Cyber Threat Defence to establish and implement standards and related procedures for implementing an automation on firewalls, there's need to consult Manager Cyber Threat Defence for permission on the addition of internal firewall as well as VPN. Control 1 would require 14 days for modifications made to the existing standards. Similarly for Control 2, it is approximated 14 days for new standards and procedure development to take place (Griffith University, 2020). However, Control 2 would require additional training to be provided to the students and staff on the usage of VPN. For this, it is predicted to be long-term training for 3 months. Control 2 also needs to check if VPN is in adherence with the University security policy, and make sure VPN password must be changed every six months and must comply with University standards for composition and strength (Griffith University, 2020).

4.3.3 Cost and Benefit analysis on Recommended Controls for risk 3.3.2.a

For risk 3.3.2.a, DoS attacks inflicted by intruders are used on systems with flaws open to exploitation.

- Control 1: Use an access list (ACL) to block the IP address of the hacker.
- Control 2: Server request rate limiting

An risk that was brought up was that there are consistent DoS attacks inflicted by offenders. The risk deserves to be addressed, as if not it would definitely cause packet loss and extreme inconveniences to the university's staff and students who need to access the resources; access to their emails, files, or online accounts. As well for users, it would also cause disruptions for internal admins who need to perform tasks on the system as DoS attacks will crash systems at its worst.

To address this risk, there should be restrictions, which specified in Control 2 to pose around the number of requests a server will accept over a certain time window to mitigate DoS attacks. While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be insufficient to handle a DoS attack effectively. Ergo, Control 1, using an access list (ACL) can be helpful to support server request rate limiting in the mission of providing protection to Remarkable University's security systems as well as software and servers against DoS. ACL will tackle the root cause by blocking the IP address of the hacker who executes DoS attacks in an attempt to put down a network and consequently the web server.

The controls are easy to implement however effective and efficient enough to address the DoS attack. The only required resources will be for the users of university devices or on their network to abide by the Internet and Network Access Security Standards set out by Remarkable University. In particular, the users need to ensure packet filtering will be used with rules which keep the security risk to a minimum, and all Internet/Web servers will be configured to allow access to and use of services to be controlled, which include Access Control Lists (Griffith University, 2020).

4.3.4 Cost and Benefit analysis on Recommended Controls for risk 3.3.2.b

For risk 3.3.2.b, failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack.

- Control 1: Disable Compression
- Control 2: Prevent Caching of Sensitive Data

The failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack is by no accident due to the trust they have with TLS protocol fosters the lack of care paid to the user cookies. However, having only TLS is not enough to protect the cookies from being stolen. The security can be improved to have controls such as identified by Control 1. First of all, Remarkable University should start making a change to the TLS compression, which should be disabled in order to protect against a vulnerability which could potentially allow sensitive information such as session cookies to be recovered by an attacker.

While this is a good improvement, Control 1 can be better accompanied by Control 2, which also concerns the TLS protocol the university has in place currently. Albeit TLS provides protection of data while it is in transit, Control 2 is suggested noting the fact TLS does not provide any protection for data once it has reached the requesting system. As such, this information may be stored in the cache of the user's browser, or by any intercepting proxies which are configured to perform TLS decryption. It is of critical importance that HTTP headers should be used to instruct the browser not to cache the sensitive data that is returned in responses to prevent it being sent to the other users who may be someone that’s of malicious intent to tamper your data (Lingappa, 2018).

The required resource needed for the 2 controls to be implemented required Web-based administration must be via secure HTTP (HTTPS), at the same time are required to utilise a valid SSL certificate of not less than 2048 bits issued by a University certificate authority (Griffith University, 2020).

4.3.5 Cost and Benefit analysis on Recommended Controls for risk 3.3.2.c

For risk 3.3.2.c, Cross-site scripting (XSS) attacks inflicted by intruders are used on systems with flaws open to exploitation.

- Control 1: install an anti-XSS plugin
- Control 2: Add code snippets as extra measures to validate and sanitize user inputs.

Cross site scripting (XSS) is a very common web application vulnerability used by attackers to inflict assaults from hijack user accounts, to distribute malware, then to control user's computer remotely and exploit user applications. It is known how most of the XSS attacks are launched, and that is by exploiting user inputs. Knowing the root cause to the problem, then it is easier to tackle. If intruders are leveraging the use of input fields, then simply block their source of usage. One way to do this, is by adding to the LMS or any other server or software conditional statements as measures to filter users' inputs, while also letting in users with good intent. However, there is an alternative to Control 2, which is by installing an anti-XSS plugin. Control 1 works without the need of writing any extra code, and manages its own prevention parameters that are powerful enough to shelter Remarkable University's data from XSS attacks. Specifically, what Control 1 does is it can secure user input fields, instances can include comment fields, search bars etcetera. and effectively prevent most of the XSS attacks from even executing. However, using Control 1 would provide more freedom in defining the type of conditions against specific cyber attacks, not subjected to only XSS attacks.

For Control 1, it is required that all systems and software, which would include the anti-XSS plugin in the university's network environment must have patches applied at the earliest opportunity as per an established patch management regime, and that critical patches must be deployed within one month of the patch's release (Griffith University, 2020). While Control 2 needs to conduct sophisticated boundary test cases before the code can be committed and merged to the existing code for the LMS.

4.3.6 Cost and Benefit analysis on Recommended Controls for risk 3.3.3.a

For risk 3.3.3.a, MITM attack in the form of email hijacking and malware attached.

- Control 1: Use a robust encryption protocol on networks: WPA2 alongside AES.
- Control 2: Enable Spam URI Real-time Block Lists (SURBL) to verify message content
- Control 3: Only open or download attachment from known sender or expected email.

It is hard to be able to identify a phishing email these days, let alone an attack that's so sophisticated where an attacker hides their identity by impersonating as a user's acquaintance. MITM attacks are quite hard to address, but still, there are controls which can help. Control 1 is suggested which provides the highest levels of protection. WPA2 with AES are a combination which forms a strong encryption that makes it much more difficult for an attacker to gain access to the network by just being nearby. However, these days, one can never guarantee a 100% security of the network. Besides, the mail can still be sent with malicious mail with malware without attacker spoofing on one's internet. Therefore, measures need to be established to verify the content of the message, and that is what Control 2 does. Control 2 enables Spam URI Real-time Block Lists, abbreviated SURBL, which can detect suspicious email based on malicious links within a message. Having a SURBL filter helps to protect users from malware (OWASP Cheat Sheet Series, 2020). However, like said, the digital world is kept on evolving and so does everything else, including viruses and malware. Hence, the last control, Control 3 asks to only open or download attachments from known senders or expected email, with the intention to avoid Malware. However, Control 3 could unfortunately cause the user to miss out on an important email from an actual legitimate friend. Thus, it is Control 1 and Control 2 as the selected controls.

The controls have to be practised while ensuring if devices identified probable to cause malicious network activity such as virus infection, ransomware, unauthorised access or data exfiltration will be subject to immediate disconnection or isolation by delegated authority of the Chief Digital Officer (Griffith University, 2020).

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Selected Controls	Required Resources
Firewalls not correctly configured. (refer to 3.3.1.a)		Control 1: Need to disable dynamic routing so it won't result in a loss of control that reduces security, and creates a vulnerability in firewall protection. Control 2: Automating firewall configuration capable of maximizing efficiency while reducing the expenditures on operational and security and reducing human error by eliminating misconfigurations that could otherwise increase the attack surface.	Control 1 Control 2	1 day for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls. (Control 1) 3 months for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls. (Control 2) Get Proper authorization for the change to opt to firewall automation. Backup existing configurations Audit and govern the change process Recertify policies
IP Spoofing attacks (refer to 3.3.1.b)		Control 1: Have internal firewalls on top of perimeter firewalls to help partition individual assets on the network. Control 2: VPN protection strategies against IP spoofing attacks, using key-based encryption to create a subnet for secure communication.	Control 1 Control 2	2 weeks for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls. 3 months training to use VPN Check if VPN is in adherence with the University security policy. VPN password must be changed every six months and must comply with University standards for composition and strength.

DoS attacks inflicted by intruders (refer to 3.3.2.a)		Control 1: Use an access list (ACL) to block the IP address of the hacker. Control 2: Server request rate limiting	Control 1 Control 2	Packet filtering will be used with rules which keep the security risk to a minimum. All Internet/Web servers will be configured to allow access to and use of services to be controlled (e.g. Access Control Lists, TCP Wrappers).
Failure in sessional management, cookie information stolen and sniffed by external users using unencrypted session cookie attack. (refer to 3.3.2.b)		Control 1: Disable Compression Control 2: Prevent Caching of Sensitive Data	Control 1 Control 2	Web-based administration must be via secure HTTP (HTTPS) and utilise a valid SSL certificate of not less than 2048 bits issued by a University certificate authority.
Cross-site scripting (XSS) attacks (refer to 3.3.2.c)		Control 1: install an anti-XSS plugin Control 2: Add code snippets as extra measures to validate and sanitize user inputs.	Control 1 Control 2	All systems in the University's network environment must have patches applied at the earliest opportunity as per an established patch management regime. Critical patches must be deployed within one month of the patch's release. Need conduct boundary test cases.
MITM attack in the form of email hijacking		Control 1: Use a robust encryption protocol on networks: WPA2 alongside AES.	Control 1	Ensure devices identified probable to cause malicious network activity such as virus

and malware attached. (refer to 3.3.3.a)		Control 2: Enable Spam URI Real-time Block Lists (SURBL) to verify message content Control 3: Only open or download attachment from known sender or expected email.	Control 2	infection, ransomware, unauthorised access or data exfiltration will be subject to immediate disconnection or isolation by delegated authority of the Chief Digital Officer.

4.4 System and Other Security

4.4.1 Cost and Benefit analysis on Recommended Controls for risk 3.4.1.a

To reduce risk 3.4.1.a, age of the equipment and overheat of database hardware. Control 1 and 2 are selected.

- Control 1: Carry out daily physical maintenance to ascertain servers are regularly dusted and cleaned and not overheated.
- Control 2: Network admins monitoring the lifespan and condition of the hardware, and report to Senior Manager Risk and Compliance for preemptive plans.

Database hardware is directly linked to Oracle Database Software, it stores student and staff data for Oracle Database Software, which means that any malfunction in database server can render Oracle Database Software unavailable, and can cause data loss. Hence, maintenance of the database server needs to be properly handled, Remarkable University will suffer a significant financial cost if otherwise.

Ways to care for a database server is different from maintaining a software. Many problems with physical database servers have occurred because of machine overheating caused by lack of regular dusting, and the overlooked aging condition with the physical database server. Therefore, Control 1 and 2 are selected to resolve these issues.

To implement Control 1 and 2, server maintenance staff should dust the physical database server daily, and check that there is no dust clogged in gaps of the physical database server to ensure the factors that can cause machine overheating are all eliminated. Server maintenance staff should also monitor the lifespan and condition of the database server on a day-to-day basis to make sure that the database server is still

operating properly and is not passing its usable lifespan. Any issues found for the database server should be immediately reported to senior manager risk and compliance for preemptive plans. If there are no issues found for the database server, then a report on database server inspection should be made to senior manager risk and compliance fortnightly.

4.4.2 Cost and Benefit analysis on Recommended Controls for risk 3.4.1.b

To reduce risk 3.4.1.b, probable damage on database server hardware by unpredictable natural disasters. Control 1 and 2 are selected, but not Control 3.

- Control 1: 24/7 uninterrupted power supply with backup power so that your servers can continue to operate if there is a power outage or natural disaster.
- Control 2: Keep backup of the critical business data to an offsite location for protection in case of a data erasing event.
- Control 3: Ensure to have backup machinery in hand.

Oftenly, it is easier to protect against one person's misdoing than the misdoing of the climate, this is because natural disasters often are unpredictable. One main problem with natural disasters is that it normally cuts off power supply of physical database servers which it essentially needs to be able to perform daily operations 24/7. Many organisations have suffered unexpected cut offs in power supply, and have lost millions of financial resources, as a cut off in power supply, meaning a loss of availability in services and a loss of data.

Seeing this, Remarkable University adopts Control 1 to ensure that a 24/7 uninterrupted power supply with backup power is in place so that the database servers can continue to operate if there is a power outage or natural disaster. Doing this, can help preserve the availability of service, as well as the completeness of data.

However, due to the extreme level of risk, having only backup power cannot sufficiently reduce the risk 3.4.1.b, hence Control 2 is also selected to complement Control 1. As physical database servers are prone to suffocate from natural disasters, a better plan will be to move backup of the data to an offsite location for protection. With implementation of both Control 1 and 2, it is guaranteed that risk 3.4.1.b will be significantly reduced. Judging by the current level of risk being extreme, Control 3 will not be implemented as backup machineries can be costly to implement, Control 3 could be implemented if the level of risk is catastrophic.

To implement Control 1, and 2, server maintenance staff monitors the machine's power supplyance on a daily basis to ensure proper daily operations. Server maintenance staff backups critical data to an offsite location for protection in case of a data erasing event.

4.4.3 Cost and Benefit analysis on Recommended Controls for risk 3.4.1.c

To reduce risk 3.4.1.c, insider attack on physical server machine. Control 1 and 2 are selected.

- Control 1: Enforces a two-factor authentication that includes biometric scanning, making it far more difficult for someone to steal or copy access credentials.
- Control 2: The administrator should ensure that the inbuilt database server system monitoring utilities are appropriately installed and configured, and review servers' performance and any potential security risks as well as backup protocols.

Misdoing conducted by people from within remarkable University is harder to detect than an attack from outside. Most organisations do know that they need to enforce protections against outsiders, but not all organisations enforce protections against insiders, this is because of trust. People tend to trust people within the organisations, and this trust within an organisation often creates vulnerabilities for insider attacks.

To prevent this, monitoring of physical machines, and two-factor authentication such as biometric scanning should be implemented to make it far more difficult for insiders to steal or copy access credentials. Hence, Control 1 and 2 are selected.

To implement Control 1 and 2, 1 month is required for engineers to implement a two-factor authentication that includes biometric scanning. 14 days are needed for network engineers to install and configure monitoring utilities for the database server system, and network security administrators needs to review servers' performance and any potential security risks as well as backup protocols to ensure that no insider attacks are conducted.

4.4.4 Cost and Benefit analysis on Recommended Controls for risk 3.4.2.a

To reduce risk 3.4.2.a, insider attack on data. Control 1, 2 and 3 are selected.

- Control 1: Encrypt data that is critical to organisation so insiders could not interpret and therein expose.
- Control 2: Keep a log and monitor who have touched the data.
- Control 3: Maintaining a data breach incident register to record key information in relation to identified data breaches incidents.

Many organisations assume their insiders will post no danger to their organisational assets, hence, many organisations store data in unencrypted form. However, unencrypted data is insecure, because it can be read and understood by anyone. Insiders with ill intentions could use this vulnerability, steal this information and potentially cause data leakage.

To prevent this from happening, data will need to be encrypted, logged, and carefully monitored using Control 1, 2 and 3. If any data breaches from insiders are detected, then a data breach incident will need to be recorded and maintained in the data breach incident register. Proper usage of Control 1, 2 and 3 will put the organisation in good condition.

To implement Control 1, 2, and 3, 3 days are required for network security administrators to encrypt data, and it is essential for identity management administrators to monitor, record, log, and maintain data breach incidents on a daily basis.

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Selected Controls	Required Resources
Age of the equipment and overheat of database hardware. (refer to 3.4.1.a)	Extreme	Control 1: Carry out daily physical maintenance to ascertain servers are regularly dusted and cleaned and not overheated. Control 2: Network administrators monitoring the lifespan and condition of the hardware, and report to Senior Manager Risk and Compliance for preemptive plans.	Control 1 and 2	Server maintenance staff dust the physical database server on a daily basis. Server maintenance staff monitors the lifespan and condition of the database server on a day-to-day basis. Report to senior manager risk and compliance for preemptive plans fortnightly.
Probable damage on database server hardware by unpredictable natural disasters. (refer to 3.4.1.b)	Extreme	Control 1: 24/7 uninterrupted power supply with backup power so that your servers can continue to operate if there is a power outage or natural disaster. Control 2: Keep backup of the critical data to an offsite location for protection in case of a data erasing event. Control 3: Ensure to have backup machinery in hand	Control 1 and 2	Server maintenance staff monitors the machine's power supplyance on a daily basis. Server maintenance staff backups critical data to an offsite location for protection.
Insider attack on physical server machine. (refer to 3.4.1.c)	Extreme	Control 1: Enforces a two-factor authentication that includes biometric scanning to prevent someone to steal or copy access credentials. Control 2: Ensure that the inbuilt database server system monitoring utilities are installed and configured appropriately, and review servers' performance and any potential	Control 1 and 2	1 month for engineers to implement a two-factor authentication that includes biometric scanning. 14 days for network engineers to install and configure monitoring utilities for the database server system.

		security risks as well as backup protocols.		Network security administrators review servers' performance and any potential security risks as well as backup protocols.
Insider attack on data (refer to 3.4.2.a)	Extreme	Control 1: Encrypt data that is critical to organisation so insiders could not interpret and therein expose. Control 2: Keep a log and monitor who have touched the data. Control 3: Maintaining a data breach incident register to record key information in relation to identified data breaches incidents.	Control 1, 2 and 3	3 days for network security administrators to encrypt data. Identity management administrators monitor, record, log, and maintain data breach incidents on a daily basis.
SQL Injection (refer to 3.4.2.b)		Control 1: Validate All Input. Eg. Reject input that contains ';' or '--'. Control 2: Use appropriate privileges		
Unintentional deletion, modification, or disclosure of information (refer to 3.4.2.c)		Control 1: Policies governing specifications for critical documents. Control 2: Appropriate education and training on handling data to ensure policies to be followed. Control 3: Always ensure to follow schedules to backup the system containing the critical data.		

5. Implementation

To reduce risks for assets, simple measures are implemented, access controls are appropriately managed, least privileges are enforced, and information flow is monitored and encrypted.

After all possible cost and benefit analysis, there are still residual risks, because no controls that will give 100% protections on organisational assets. Since Remarkable University asks only to protect its online learning platform against common automated and simple manual attacks, recommended controls are selected based on this criteria. Hence, if there are dedicated, and targeted attacks conducted on the online learning platform, there is a bigger chance for the attacks to be successful. A successful attack can cause corruption, leakage, and unavailability in Remarkable University's servers, online learning environment, software, and data.

Recommended maintenance of the security mechanism and training for the relevant personnel

- Cyber threat defense senior manager (Griffith University, 2020) will need 7 days to write and enforce organisational policies for separation of duties and least privilege.
- 3 days for identity management administrators (Griffith University, 2020) to verify and change monitoring tools to adapt for regular scanning on Authentication Server.
- Identity management administrators need to perform day-to-day security administration, they should monitor and flag any suspicious activities and unauthorised access in audit logs.
- 1 day for educating and training all internal users is needed to help ensure that these policies are strictly followed.
- Cyber network administrators will need 5 days to configure for privilege escalation monitoring and role management.
- Database administrators are required to perform day-day database administration, this includes daily privilege escalation monitoring, regular review of administrative accounts and revoke them if access is no longer needed.
- Identity management administrators will need 1 day to set limitations on the length of time on internal users' login sessions,
- 2 days are required for database administrators to limit internal user privilege to have only general access.
- Cyber network administrators will need 0.5 day to set HttpOnly and Secure flags for session cookies.
- 1 day educating and training for the software configuration management team on using version control tools such as Git is required.
- Cyber network administrators should monitor files and folders on a daily basis to look out for inadvertent and intentional unauthorised changes made to software's code.

- 1 day educating and training for the software configuration management team on using version control tools such as Git.
- Cyber network administrators should monitor files and folders on a day-to-day basis.
- Daily back up should be performed by cyber network administrators.
- Cyber security network administrators check for updates daily, and need to apply patches monthly.
- 1 day is required for cyber network administrators to test out patches on test environments.
- 3 days are needed for training internal users basic ransomware attack prevention. Training should provide internal users insights of not to click on untrusted links, and not to give personal information to untrusted websites (Norton, 2020).
- 7 days for database administrators to implement ASLR and DEP.
- 1 day for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls.
- 3 months for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls.
- Get Proper authorization for the change to opt to firewall automation.
- Backup existing configurations
- Audit and govern the change process
- Recertify policies.
- 2 weeks for the Manager Cyber Threat Defence to modify the existing standards and policy to govern firewalls.
- 3 months training to use VPN.
- Check if VPN is in adherence with the University security policy.
- VPN password must be changed every six months and must comply with University standards for composition and strength.
- Packet filtering will be used with rules which keep the security risk to a minimum.
- All Internet/Web servers will be configured to allow access to and use of services to be controlled (e.g. Access Control Lists, TCP Wrappers).
- Web-based administration must be via secure HTTP (HTTPS) and utilise a valid SSL certificate of not less than 2048 bits issued by a University certificate authority.
- All systems in the University's network environment must have patches applied at the earliest opportunity as per an established patch management regime.
- Critical patches must be deployed within one month of the patch's release.
- Server maintenance staff should dust the physical database server daily, and check that there is no dust clogged in gaps of the physical database server to ensure the factors that can cause machine overheating are all eliminated.
- Server maintenance staff should also monitor the lifespan and condition of the database server on a day-to-day basis to make sure that the database server is still operating properly and is not passing its usable lifespan.
- Any issues found for the database server should be immediately reported to senior manager risk and compliance for preemptive plans. If there are no issues found for the

database server, then a report on database server inspection should be made to senior manager risk and compliance fortnightly.

- Server maintenance staff monitors the machine’s power supplyance on a daily basis to ensure proper daily operations.
- Server maintenance staff backups critical data to an offsite location for protection in case of a data erasing event.
- 1 month is required for engineers to implement a two-factor authentication that includes biometric scanning.
- 14 days are needed for network engineers to install and configure monitoring utilities for the database server system
- Network security administrators need to review servers' performance and any potential security risks as well as backup protocols to ensure that no insider attacks are conducted.
- 3 days for network security administrators to encrypt data.
- Identity management administrators monitor, record, log, and maintain data breach incidents on a daily basis.

REFERENCE (APA 7)

Akamai. (2020). *Executive Summary: [state of the internet] / security. (Volume 6, Issue 1).* https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-executive-summary-2020.pdf

Algosec. (2018). *AUTOMATING FIREWALL CHANGE MANAGEMENT.* https://www.algosec.com/wp-content/uploads/2018/12/18271_Auto_FW_Chg_Mgm_WP_EN-1.pdf

Avery, L. (2018). *The $85 Billion Cost of Bad Code.* Retrieved September 4, 2020 from https://www.pullrequest.com/blog/cost-of-bad-code/

Bera, A. (2019). *Ransomware Statistics.* Retrieved September 4, 2020 from https://safeatlast.co/blog/ransomware-statistics/

Bulletproof. (2019). *BULLETPROOF ANNUAL CYBER SECURITY REPORT 2019.* *https://www.bulletproof.co.uk/industry-reports/2019.pdf*

CISA. (2019). *Security Tip (ST04-015): Understanding Denial-of-Service Attacks.* Retrieved September 5, 2020 from https://us-cert.cisa.gov/ncas/tips/ST04-015

Cook, S. (2020). *Malware statistics and facts for 2020.* Retrieved September 4, 2020 from https://www.comparitech.com/antivirus/malware-statistics-facts/

CWE. (2006). *CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.* Retrieved September 4, 2020 from https://cwe.mitre.org/data/definitions/119.html

CWE. (2006). *CWE-269: Improper Privilege Management.* Retrieved September 2, 2020 from https://cwe.mitre.org/data/definitions/269.html

CWE. (2020). *2020 CWE Top 25 Most Dangerous Software Weaknesses.* Retrieved September 2, 2020 from https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Cynet. (2020). *Understanding Privilege Escalation and 5 Common Attack Techniques.* Retrieved September 1, 2020 from https://www.cynet.com/network-attacks/privilege-escalation/

Dark Reading. (2018). *Most Malware Arrives Via Email.* Retrieved September 5, 2020 from https://www.darkreading.com/attacks-breaches/most-malware-arrives-via-email/d/d-id/1333023

Datacore. (2018). *17 Shocking Statistics about Disaster Recovery and Business Resiliency—Where Does Your Organization Stand?: Part.* Retrieved September 5, 2020 from https://www.datacore.com/blog/17-shocking-statistics-about-disaster-recovery-and-business-resiliency-where-does-your-organization-stand-part-1/

Dynamic Technologies. (2017). *7 Backup & Disaster Recovery Statistics to Know for 2018.* Retrieved September 5, 2020 from https://dbtechnologies.com.au/7-backup-disaster-recovery-statistics/

Resolver. (2018). *Physical and Cybersecurity Defense: How Hybrid Attacks are Raising the Stakes.* Retrieved September 5, 2020 from https://www.resolver.com/resource/physical-and-cybersecurity-defense-how-hybrid-attacks-are-raising-the-stakes/

Lerner, A. (2014). *The Cost of Downtime.* Retrieved September 5, 2020 from https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

Lingappa, R. (2018). *What is session hijacking and how you can stop it.* Retrieved September 2, 2020 from https://www.freecodecamp.org/news/session-hijacking-and-how-to-stop-it-711e3683d1ac/

Gaybrick, W. (2018). *Tech's ultimate success: Software developers are now more valuable to companies than money.* Retrieved September 3, 2020 from https://www.cnbc.com/2018/09/06/companies-worry-more-about-access-to-software-developers-than-capital.html

Greenberg, A. (2015). *Human error cited as leading contributor to breaches, study shows.* Retrieved September 3, 2020 from

https://www.scmagazine.com/home/security-news/human-error-cited-as-leading-contributor-to-breaches-study-shows/

Griffith University. (2020). *Information Security Procedure* (2020/0000032). Griffith University. https://policies.griffith.edu.au/pdf/Information%20Security%20Procedure.pdf

Wyss, Gregory Dane, Sholander, Peter E., Darby, John L., & Phelan, James M. (2007). *Identifying and Defeating Blended Cyber-Physical Security Threats*. United States. https://www.osti.gov/servlets/purl/1427000

Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A., & Dainotti, A. (2017). *Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem.* CAIDA *https://www.caida.org/publications/papers/2017/millions_targets_under_attack/millions_targets_under_attack.pdf*

Kaspersky Lab. (2018). *DENIAL OF SERVICE: HOW BUSINESSES EVALUATE THE THREAT OF DDOS ATTACKS IT SECURITY RISKS SPECIAL REPORT SERIES.* https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf

Koussa, S. (2018). WHAT DO SAST, DAST, IAST AND RASP MEAN TO DEVELOPERS? Retrieved September 6, 2020 from https://www.softwaresecured.com/what-do-sast-dast-iast-and-rasp-mean-to-developers/

Malwarebytes Labs. (2020, February). *2020 State of Malware Report.* https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

Mimecast. (2020). *The State of Email Security 2020: Email security insights at your email perimeter, inside your organization, and beyond.* https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf?utm_source=pr&utm_medium=pr&utm_campaign=7013l000001N4dRAAS

Milkovich, D. (2020). *15 Alarming Cyber Security Facts and Stats.* Retrieved September 5, 2020 from https://www.cybintsolutions.com/cyber-security-facts-stats/

Moss, H. (2020). *Difference Between Internet, Intranet and Extranet.* Retrieved 28 August, 2020 from https://www.difference.wiki/internet-vs-intranet-vs-extranet/

Norton. (2020). *7 tips to prevent ransomware.* Retrieved September 1, 2020 from https://us.norton.com/internetsecurity-malware-7-tips-to-prevent-ransomware.html

Observe IT. (2019). *How to Protect Databases from Insider Threats.* Retrieved September 5, 2020 from https://www.observeit.com/blog/how-to-protect-databases-from-insider-threats/

OWASP. (2017). *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks.* https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

OWASP Cheat Sheet Series. (2020). *Transport Layer Protection Cheat Sheet.* Retrieved September 2, 2020 from https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Ponemon, L. (2019). *What's New in the 2019 Cost of a Data Breach Report.* Retrieved September 5, 2020 from https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Portswigger. (2020). *Access control vulnerabilities and privilege escalation.* Retrieved September 1, 2020 from https://portswigger.net/web-security/access-control

Statista. (2014). *Frequency of server failure based on the age of the server (per year).* Retrieved September 5, 2020 from https://www.statista.com/statistics/430769/annual-failure-rates-of-servers/

Swoop. (2020). *Password Authentication: Avoiding 4 Common Vulnerabilities.* Retrieved September 1, 2020 from https://swoopnow.com/password-authentication/#:~:text=How%20do%20user%2Dgenerated%20credentials,and%20easily%20vulnerable%20to%20hacking

Symantec. (2019). *Executive Summary: 2019 Internet Security Threat Report (Volume 24).* https://docs.broadcom.com/doc/istr-24-executive-summary-en

United States of America v Paige (2019) MJ19-0344

Varonis. (2019). *2019 GLOBAL DATA RISK REPORT FROM THE VARONIS DATA LAB.* Retrieved September 4, 2020 from https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

Verizon. (2018). *2018 Data Breach Investigations Report (11th edition).* https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

Wang, W. (2012). *Vulnerability in HTC website allow attacker to hijack accounts.* Retrieved September 5, 2020 from https://thehackernews.com/2012/12/vulnerability-in-htc-website-allow_28.html

Wang, Z. (2020). *Lec3-Risk-Assessment-OL: Organisational IT Security Policy*[PPT]. Zhe Wang.

Weisman, S. (2020). *What are Denial of Service (DoS) attacks? DoS attacks explained.* Retrieved August 30, 2020 from https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html

WhiteHat Security. (2020). *Unsecured Session Cookie.* Retrieved September 1, 2020 from https://www.whitehatsec.com/glossary/content/unsecured-session-cookie

Whitney, L. (2019). *How firewall automation can help prevent breaches caused by wrong configurations.* Retrieved September 5, 2020 from https://www.techrepublic.com/article/how-firewall-automation-can-help-prevent-breaches-caused-by-wrong-configurations/

Whittle, S. (2008). *The top five internal security threats.* Retrieved September 5, 2020 from https://www.zdnet.com/article/the-top-five-internal-security-threats/