UNIVERSITY OF PORTSMOUTH

Security Risk Assessment for A Typical UK Based University

M25160 (Security Management)

UP2006913
21/11/2023

Executive Summary

This risk assessment seeks to identify the assets critical to a UK university; enumerate and analyse all possible threats and vulnerabilities which threaten those assets and suggest appropriate controls to treat risk —considering especially the universities key functions: the dissemination, creation, and preservation of knowledge.

The risk assessment will be carried out following the ISO 27000 framework, utilising a risk matrix to justify risk values for individual vulnerabilities and incident scenarios and using annexe A of ISO 27001 to propose suitable controls for risk management. Following ISO 27000, the report will be broken down into 4 key tables. Table A for asset identification; Table B for risk identification; Table C for risk evaluation and Table D for risk treatment.

Figures 1 and 2 below outline the effectiveness of the controls suggested within this risk assessment, reducing overall risk by over 50%. Supporting this, figure 3 shows the key asset groups in which the vulnerabilities were grouped and the overall reduction in risk for each category of asset.

The top 5 controls make up 44% of the proposed risk treatment implementations and would significantly reduce risk to the university's critical functions – however, all suggested controls should be considered for implementation to significantly improve the security posture.

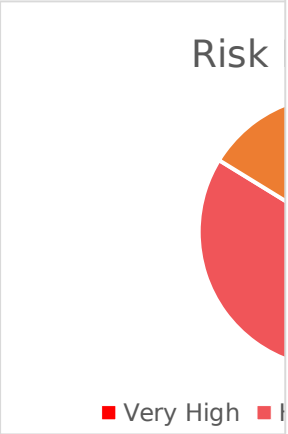

Figure 1 - Risk Frequency

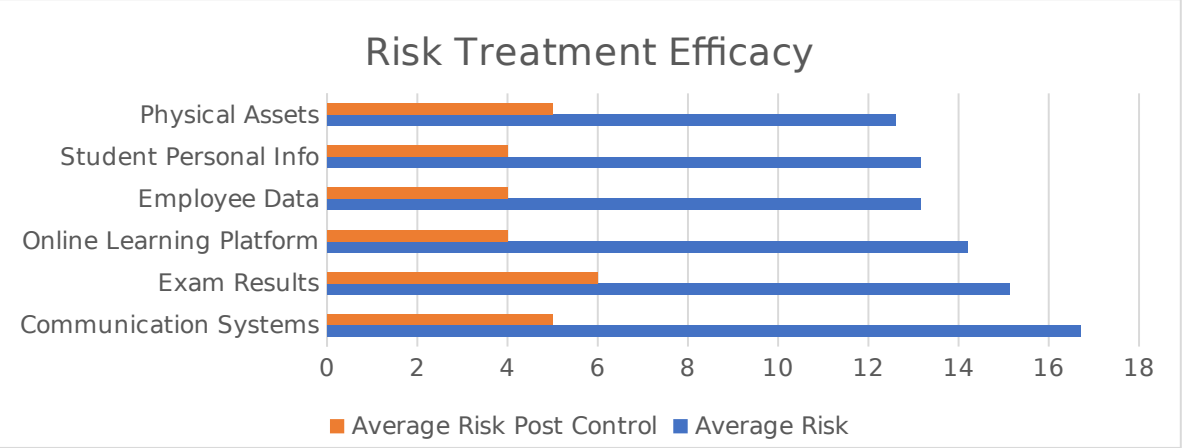

Figure 3 - Risk Frequency by Asset Group

Figure 2 - Risk Frequency (Post Controls)

Table Of Contents

1.0Introduction

Background

In the modern academic landscape, universities are more than just centres of education and research, they are constantly expanding organisations with a vast array of information assets to manage and protect. Behind the scenes, a typical UK university can operate just like a business does, with multifaced and global operations spanning way beyond traditional education.

This increasing scale of modern-day universities brings with it a multitude of new risks, as the institutions grow so too does the value and extent of their information assets. According to a report by the ONS (Office for National Statistics, 2022), “hacking offences” which include the compromise of victim’s details such as emails and social media accounts through large-scale breaches have more than doubled in the year ending March 2022, and a GOV.UK survey on cyber security breaches in 2022 found that at least 39% of UK businesses had identified a cyber-attack within a 12-month period (Department for Digital, Culture, Media & Sport, 2022). In an ever-growing climate of cyber threats, a business or organisation needs to be aware of the threats they are facing and take action to identify all potential vulnerabilities within their operation.

Objectives

This risk assessment takes an asset-centric approach to risk management, focusing on primary information assets, and delving into the identification of potential vulnerabilities and threats which might impact these assets. Following this, there will be a substantial analysis and evaluation using a risk matrix to categorise and score potential threats, followed by a severity and efficiency focussed recommendation of suitable controls to mitigate risk either by reducing the likelihood or impact of any vulnerabilities found.

2.0 Context / Methodology

Assessment Scope

This analysis will encompass the entirety of the university's information assets spanning academic, administrative, research, and operational domains. Utilising ISO 27005 (British Standards Institution, 2022), all critical information assets will be identified ranging from student records and research data to the universitiy IT infrastructure and Intellectual property. The risk assessment will also consider secondary assets such as physical hardware and access control mechanisms will also be considered where they may play a role in the compromise of the primary information assets.

Report Structure

This report will consist of four tables, each one relating to a key phase of the risk assessment such as Asset Identification; Risk Identification; Risk Analysis and Risk Treatment, with each of the tables building on the previous.

Risk Tolerance

It is understood that a typical UK university will be risk-averse, and so their risk appetite, the amount of risk they are willing to take on, will be reasonably low largely due to their reliance on public and private funding and the importance of maintaining their reputation. Breaking down the risk domains, a university will have the lowest risk appetite for anything academic, financial, or reputational whereas their risk appetite may be more moderate for things which are operational or strategic such as expanding the campus or creating new courses. Overall, however, in the interest of protecting both the university's students' well-being and academic integrity and reputation, it is considered in this risk assessment that there will be a low-risk appetite.

Methodology

Adhering to the globally recognized ISO/IEC 27005 standard (British Standards Institution, 2022), this risk assessment employs a structured approach to information security risk management. The ISO 27005 provides a structured and systematic approach to asset identification, assessment, and risk management. Utilising this standard ensures that the undertaking of this risk assessment is thorough, consistent, and aligned with best practices. This approach will ensure that all potential information security risks are evaluated and managed, safeguarding the university's assets.

A semi-quantitative risk matrix will be employed to assess and prioritise all the identified risks, this approach will assign a numerical risk "score" based on a combination of qualitative likelihood and impact ratings. This semi-quantitative approach has been chosen as it will allow for a more

structured evaluation with clear ratings for risks allowing prioritisation of higher-risk vulnerabilities, a fully quantitative approach would have most likely not been possible due to a lack of

Risk Level	(1) Extremely Unlikely	(2) Unlikely	(3) Possible	(4) Likely	(5) Extremely Likely
Impact (1) Negligible	1	2	3	4	5
Impact (2) Low	2	4	6	8	10
Impact (3) Moderate	3	6	9	12	15
Impact (4) High	4	8	12	16	20
Impact (5) Severe	5	10	15	20	25

1-3 : Very Low | 4-6 : Low | 8-10 : Moderate | 12-16 : High | 20-25 : Very High

available data.

Figure 4 - Risk Assessment Matrix

Throughout the assessment, risk scoring will be conducted exclusively using the risk matrix provided above in Figure 1, this semi-quantitative matrix will use qualitative values for impact and likelihood which are chosen using the criteria listed on the following page. By utilising this matrix and criteria exclusively the risk assessment and scores will remain uniform, eliminating the risk *(by reducing the likelihood)* of fluctuating or inconsistent numbers leading to skewed interpretations or misinformed decision-making.

Likelihood Rating

Extremely unlikely

- Expected to occur once in a year.
- Extremely unlikely to be successfully executed, even with all tools/resources.

Unlikely

- Expected to occur once in a month.
- Unlikely to be successfully executed, even with some appropriate tools/means.

Possible

- Expected to occur once in a week.
- Possible to be successfully executed with appropriate tools/means.

Likely

- Expected to occur once in a day.
- Likely to be successfully executed with few tools/resources.

Extremely Likely

- Expected to occur multiple times a day/hour.
- Extremely likely to be successfully executed with few tools/resources.

Impact Rating

Negligible Impact

- No loss of confidentiality, integrity, or availability.

Low Impact

- Temporary loss of availability, minor unauthorized disclosure of non-sensitive data, or minor system integrity issue.

Moderate Impact

- Limited unauthorised disclosure of sensitive data, system integrity issue causing operational disruptions, or temporary loss of critical system availability.

High Impact

- Significant unauthorised disclosure of sensitive data, long-term loss of critical system availability, or major system integrity issue causing significant operational disruptions.

Severe Impact

- Massive unauthorised disclosure of sensitive data with national or international implications, complete and extended shutdown of critical systems, or catastrophic system integrity failures.

Figure 5 – Likelihood and Impact Ratings

3.0 Asset Identification

This section identifies a list of primary information assets, and supporting assets, which a UK university could consider critical to its mission, with the core values of most universities being the collection, creation, and dissemination of knowledge. In addition, there will be some information assets which are seen as valuable to other external parties for malicious use.

Primary Asset	Asset Value	Value Justification
Student Personal Data	High	Critical for student administration, legal compliance. Potentially valuable to malicious 3rd parties.
Online Learning Platforms / VLE	High	Critical to delivery and quality of teaching, one of the universities core focusses. Increasingly more critical post COVID-19 with distanced learning.
Examination Results and Records	High	Loss of records would affect all students' academic progress. Insufficiently protected data could lead to breaches in integrity of the data.
Employee Personal Data and HR Records	High	Required for staff administration, payroll, and legal compliance. Potentially valuable to malicious 3rd party.
Communication Systems	High	Critical for internal and external communication. Potential for infiltration by 3rd party for social engineering.
Physical Asset inventory	High	Crucial for asset management, ensuring tracking and safeguarding of physical assets.

Table A - Asset Identification

4.0 Risk Identification

This section takes the assets identified previously, and for each one gives a series of threats, vulnerabilities which allow the threats to occur, and incident scenarios detailing the vulnerabilities' effect.

Primary Asset	Threats	Vulnerability	Incident Scenario	Label
Student Personal Data	Unauthorised access, breach of confidentiality by internal users.	Insufficient Access controls	An internal user abuses their access privileges to view sensitive student personal data	**IS1.1**
		Insufficient Employee Training	An untrained employee falls for a **phishing** email and inadvertently provides access to student data.	**IS1.2**
	Unauthorised access, breach of confidentiality by external hackers.	Inadequate Network Security	An attacker exploits network vulnerabilities to access student personal data.	**IS1.3**
		Lack of Data Encryption	An attacker intercepts data in transmission, allowing them access to unencrypted student personal data.	**IS1.4**
		Poor Password Policies	An attacker uses brute force to crack a weak password and access student personal data.	**IS1.5**
	Ransomware attack or system failure affecting availability.	Lack of Data backups	A ransomware attack encrypts student personal data and there are no backups available for recovery leading to total loss of data.	**IS1.6**
Online Learning Platforms / VLE	Technical failures and system outages leading to lack of availability.	Inadequate System Redundancy	A server failure causes an outage, access to the platform and all resources is impossible for an extended period	**IS2.1**
	Malware and ransomware attacks from external hackers.	Phishing and Social Engineering vulnerabilities	Users are tricked into providing their credentials, allowing a malicious party access with which they can alter files and spread malware.	**IS2.2**
		Weak Authentication mechanisms	An attacker can gain access due to weak or compromised credentials and a poor authentication mechanism.	**IS2.3**
	Abuse of user privileges.	Insufficient Access Controls	A student with incorrectly set access permissions can modify / delete course content.	**IS2.4**
	Loss of data integrity due to unauthorized content changes.	Inadequate Content Moderation	Unauthorised or malicious changes to the files / content on the platform go undetected.	**IS2.5**
Examination Results / Records	Unauthorised modification of Exam Results.	Insufficient User Authentication	A student/attacker brute forces weak account credentials allowing access to change examination results	**IS3.1**

		Lack of Audit Trails	A staff member with legitimate access changes a students' examination results for them and the change is undetected.	**IS3.2**
	Unauthorised Disclosure of Exam Results.	Insecure Transmission of data	Exam results are sent from staff to staff via unencrypted email, leaving them susceptible to interception in transit.	**IS3.3**
		Insufficient Employee training on Data Handling	A staff member mistakenly attaches a file containing exam results in an email which is sent out to students / other staff.	**IS3.4**
		Phishing attacks	A staff member is tricked into providing access to the examination system through a malicious email.	**IS3.5**
	Loss of all data on Exam results through system failure / ransomware.	Insufficient backup and recovery procedures	A server failure leads to a loss of almost all data on exam results, without proper backups this data / parts of it are forever lost.	**IS3.6**
		Unpatched Software Vulnerabilities	Known vulnerabilities which were left unpatched are exploited for an attacker to deploy ransomware or other malware.	**IS3.7**
		Insufficient Incident Response plan	A ransomware attack succeeds and encrypts all the data on the system, without an appropriate plan to handle the attack it spreads to the whole system without being isolated.	**IS3.8**
Employee personal Data and HR Records	Unauthorised access, breach of confidentiality by internal users.	Insufficient Access controls	An internal user abuses their access privileges to view sensitive personal data on other staff members.	**IS4.1**
		Insufficient Employee Training / awareness	An untrained employee falls for a phishing email and inadvertently provides access to employee data and records.	**IS4.2**
	Unauthorised access, breach of confidentiality by external hackers.	Inadequate Network Security	An attacker exploits network vulnerabilities to access employee personal data and records.	**IS4.3**
		Lack of Data Encryption	An attacker intercepts data in transmission, allowing them access to unencrypted employee personal data.	**IS4.4**
		Poor Password Policies	An attacker uses brute force to crack a weak password and access employee's personal data.	**IS4.5**
	Ransomware attack or system failure affecting availability.	Lack of Data backups	A ransomware attack encrypts all employee personal data and there are no backups available for recovery.	**IS4.6**
Communication Systems / Network	Eavesdropping over sensitive communications.	Unencrypted Communications	Sensitive information transmitted over a network without encryption can be intercepted and read by any unauthorised individual	**IS5.1**

Infrastructure		Compromised endpoints	Devices on the network which may be compromised could be used to capture sensitive communications	**IS5.2**
	Phishing and Social engineering attacks.	Inadequate email filtering	Without email filtering, malicious links and phishing emails are significantly more likely to end up in users' inboxes.	**IS5.3**
		Insufficient Employee Training / awareness	Untrained / unaware employees are more likely to fall victim to phishing emails, often leading to their accounts being used to spread the malicious email around.	**IS5.4**
	Denial of Service attacks.	Lack of network redundancy	Without redundant paths and failover capabilities, the university network will be vulnerable to DoS attacks, which would shut down the whole network / communication system	**IS5.5**
		Insecure Network Infrastructure	Insecure components such as routers, switches and firewalls with unpatched vulnerabilities can be utilised by attackers to disrupt services	**IS5.6**
		Insufficient network monitoring or alert mechanisms	Without a real-time monitoring system to alert admins to unusual network traffic, a DoS attack might not be noticed until it has been completed.	**IS5.7**
	Malware infection.	Inadequate Endpoint protection	Lack of antivirus or out of date antivirus software on end user machines leaves them vulnerable to malware infection.	**IS5.8**
		Insufficient Network monitoring	Without real-time monitoring and filtering over the network, malware can be left to spread over time to other systems and cause significantly more damage.	**IS5.9**
Physical Asset inventory / Management	Theft or misappropriation of assets.	Poor inventory management	If there is not up to date inventory tracking system, assets can easily be stolen or lost without being detected.	**IS6.1**
	Inadequate maintenance leading to asset deterioration.	No maintenance schedule	Unmaintained servers which are critical for the processing of student data may fail and go undetected leading to server failure and loss of data	**IS6.2**
	Compromise of sensitive information on physical media.	Poor disposal procedures	Physical media is not properly sanitised or destroyed when no longer needed, leading to data leakage which could potentially include sensitive data.	**IS6.3**

Table B - Risk Identification

5.0 Risk Analysis

Using the risk matrix *(Figure 4)* provided in the methodology section and the definitions in *Figure 5*, this table presents an overall risk score aggregated from the likelihood and impact scores for each incident scenario, providing justification and context for the ratings given.

L = Likelihood **I** = Impact **R** = Risk Score

Label	Incident Scenario	L	Justification for Likelihood	I	Justification for Impact	R
Asset	**Student Personal Information**					
IS1.1	An internal user abuses their access privileges to view sensitive student personal data	3	It is very possible for an internal user to abuse their privilege without complex tools/knowledge	3	Limited disclosure of sensitive student data, however since it was an internal threat exposure is limited	9
IS1.2	An untrained employee falls for a **phishing** email and inadvertently provides access to student data.	4	Employees may be generally aware of phishing however without regular refreshers social engineering training can be easily forgotten	4	Significant unauthorised disclosure of multiple students' sensitive data is likely and could lead to financial penalties or reputational damage	16
IS1.3	An attacker exploits network vulnerabilities to access student personal data.	3	It is possible, even with somewhat regular updates/patches that an attacker could exploit undetected network flaws.	4	Significant unauthorised disclosure of multiple students' sensitive data is likely, and could lead to significant financial penalties.	12
IS1.4	An attacker intercepts data in transmission, allowing them access to unencrypted student personal data.	4	It is likely that an attacker could succeed in a MITM attack over an unencrypted network with no monitoring, using very few tools.	3	Limited unauthorised disclosure of students' personal data is likely. Use of weak/no encryption could lead to financial penalties.	12
IS1.5	An attacker uses brute force to crack a weak password and access student personal data.	3	Without mandatory password requirements or lockout policies it is possible that an attacker would succeed in a brute force attack on privileged user accounts.	5	Significant unauthorised disclosure of students' sensitive data is likely, along with potential loss of integrity and availability through access to a privileged account.	15
IS1.6	A ransomware attack encrypts student personal data and there are no backups available for recovery leading to total loss of data.	3	Basic security measures and staff training can still leave the possibility of a successful malware/ransomware attack.	5	Complete shutdown of student systems with no available backups will have a critical impact on all student operations for an extended period.	15

Asset	Online Learning Platform					
IS2.1	A server failure causes and outage, access to the platform and all resources is impossible for an extended period	3	It is possible for a server which is well-maintained and has some redundancy measures to fail and lead to outages and inability to access data	4	The online learning platforms' use is critical to university teaching – long-term loss to its resources will critically affect all teaching across the university	12
IS2.2	Users are tricked into providing their credentials, allowing a malicious party access with which they can alter files and spread malware.	4	Users may be generally aware of phishing however without regular training and refreshers, social engineering attempts can often be successful.	5	The online learning platform is critical to the university, any major integrity issues will be severe. In addition, the ability to abuse the platform to spread malware is feasible and could lead to significant university-wide disruptions.	20
IS2.3	An attacker can gain access due to weak or compromised credentials and a poor authentication mechanism.	3	Without mandatory password requirements or lockout policies it is possible that an attacker would succeed in a brute force attack allowing them privileged access to the platform.	5	The online learning platform is critical to the university, unauthorised access could lead to a significant loss of confidentiality, integrity, and availability for the whole university.	15
IS2.4	A student with incorrectly set access permissions can modify / delete course content.	2	Automated systems for permission management mean it is unlikely for a student to receive incorrect permissions. Occasional errors however could be noted.	4	Unauthorised access by a student is less critical than by an unauthorised 3rd party, however the online learning system is a critical function of university teaching, and any unauthorised access could impact the confidentiality and integrity of course materials.	8
IS2.5	Unauthorised or malicious changes to the files / content on the platform go undetected.	4	Without an integrity monitoring system, it is likely that files/content could be changed and go undetected	4	The online learning platform is an authoritative source of information, dissemination of misinformation would have a high impact on the university's student and faculty.	16

Asset	Examination Results / Records					
IS3.1	A student/attacker brute forces weak account credentials allowing access to change examination results	4	Attack methods and tools for a brute force are readily available, without appropriate password strengths it is likely this attack could occur.	4	Unauthorised changes to examination results would lead to significant impacts on the integrity of all academic records kept by the university, potentially requiring re-examination	16
IS3.2	A staff member with legitimate access changes a students' examination results for them and the change is undetected.	4	A staff member could be coerced into modifying grades, without appropriate audit trails these changes would go undetected. However, it is not extremely likely that a staff member would do so willingly.	4	Unauthorised changes to examination results would significantly impact the integrity of academic records kept by the university, potentially requiring re-examination. The use of a staff member to change grades could also cause reputational damage.	16
IS3.3	Exam results are sent from staff to staff via unencrypted email, leaving them susceptible to interception in transit.	3	Use of unencrypted email to transfer data to others would leave it open to interception with appropriate tools and access.	3	Whilst there would be disclosure of some sensitive information, it is likely not whole and cannot be used maliciously by a 3rd party.	9
IS3.4	A staff member mistakenly attaches a file containing exam results in an email which is sent out to students / other staff.	3	Human error is always possible, without any email handling protocols / verification this mistake could easily be made.	3	Accidental exposure of exam results could cause reputational damage to the university however the unintentional disclosure is limited internally to students.	9
IS3.5	A staff member is tricked into providing access to the examination system through a malicious email.	4	Employees may be generally aware of phishing however without regular refreshers social engineering training can be easily forgotten.	4	Unauthorised access to the examination system would lead to a loss of integrity across all students' results, potential loss of availability and a definite breach of confidentiality.	16
IS3.6	A server failure leads to a loss of almost all data on exam results, without proper backups this data / parts of it are forever lost.	3	Server failures are known to occur. Without appropriate backup procedures and maintenance schedules it is possible for all data to be lost.	5	Complete loss of all student exam data would be critical, requiring the university to re-examine all students. Significantly damaging the universities reputation and leading to significant financial consequences to correct.	15
IS3.7	Known vulnerabilities which were left unpatched are exploited for an attacker to deploy ransomware or other	4	If there are known vulnerabilities unpatched, it is likely that an attacker could succeed with the use of ransomware on the systems holding	5	Complete loss of all student exam data would be critical, requiring the university to re-examine all students. Significantly damaging the universities reputation and	20

	malware.		exam records.		costing a significant amount to correct.	
IS3.8	A ransomware attack succeeds and encrypts all the data on the system, without an appropriate plan to handle the attack it spreads to the whole system without being isolated.	4	Ransomware attacks are a prevalent risk, without appropriate security measures is it likely that a system could fall victim to these attacks.	5	Complete loss of all student exam data would be critical, requiring the university to re-examine all students. Significantly damaging the universities reputation and costing a significant amount to correct.	20
Asset	**Employee Personal Data & HR Records**					
IS4.1	An internal user abuses their access privileges to view sensitive personal data on other staff members.	3	It is very possible for an internal user to abuse their privilege without complex tools/knowledge	3	Limited disclosure of sensitive Employee data, however since it was an internal threat the exposure is limited.	9
IS4.2	An untrained employee falls for a phishing email and inadvertently provides access to employee data and records.	4	Employees may be generally aware of phishing however without regular refreshers social engineering training can be easily forgotten	4	Significant unauthorised disclosure of multiple employee's sensitive data is likely and could lead to financial penalties or reputational damage	16
IS4.3	An attacker exploits network vulnerabilities to access employee personal data and records.	3	It is possible, even with somewhat regular updates/patches that an attacker could exploit undetected network flaws.	4	Significant unauthorised disclosure of multiple employee's sensitive data is likely and could lead to significant financial penalties.	12
IS4.4	An attacker intercepts data in transmission, allowing them access to unencrypted employee personal data.	4	It is likely that an attacker could succeed in a MITM attack over an unencrypted network with no monitoring, using very few tools.	3	Limited unauthorised disclosure of Employee's personal data is likely. Use of weak/no encryption could lead to financial penalties.	12
IS4.5	An attacker uses brute force to crack a weak password and access employee's personal data.	3	Without mandatory password requirements or lockout policies it is possible that an attacker would succeed in a brute force attack on privileged user accounts.	5	Significant unauthorised disclosure of employee's sensitive data is likely, along with potential loss of integrity and availability through access to a privileged account.	15
IS4.6	A ransomware attack encrypts all employee personal data and there are no backups available for recovery.	3	Basic security measures and staff training can still leave the possibility of a successful malware/ransomware attack.	5	Complete shutdown of employee systems with no available backups will have a critical impact on all operations for an extended period, likely including payroll.	15
Asse	**Communication Systems / Network Infrastructure**					

t						
IS5.1	Sensitive information transmitted over a network without encryption can be intercepted and read by any unauthorised individual	4	Any information transmitted over an insecure network with no use of encryption or weak encryption can be easily intercepted and read by an unauthorised threat actor.	4	Interception of unencrypted data would stand as a massive breach in confidentiality, potentially resulting in regulatory punishments.	16
IS5.2	Devices on the network which may be compromised could be used to capture sensitive communications	3	Compromised network devices are an ever-increasing risk with the modern WFH/BYOD approaches, if not properly checked these devices could easily be infected with malware unknowingly	4	Even a single compromised device on the network could lead to significant data breaches, resulting in the exposure of personal data and other sensitive information.	12
IS5.3	Without email filtering, malicious links and phishing emails are significantly more likely to end up in users' inboxes.	5	If there are no email filtering mechanisms in place, then the multitude of phishing emails users receive almost guarantee at least one will be successful.	4	Successful delivery of phishing emails to user inboxes increases the risk of data breaches, malware infections and unauthorised access to systems through stolen credentials. Likely incurring high financial loss and leading to operational disruption.	20
IS5.4	Untrained / unaware employees are more likely to fall victim to phishing emails, often leading to their accounts being used to spread the malicious email around.	4	Without appropriate training, which is up to date and refreshed in their mind, employees are likely to fall victim to phishing attempts, especially as they become more sophisticated.	5	Compromised accounts can be used to spread the malicious emails further, with the chances of success increasing when using internal accounts. It is likely that several more devices will become infected leading to large disruptions to networks and potential breach of confidential information.	20
IS5.5	Without redundant paths and failover capabilities, the university network will be vulnerable to DoS attacks shutting down the whole network system.	3	DoS attacks are a common threat, a lack of redundancies and failovers increases the risk of a successful attack. DoS attacks however take a large co-ordinated effort deliberately against one target.	5	If successful, a DoS attack with no fall-backs would be catastrophic, halting all network communications across the university and disrupting academic and administrative operations.	15
IS5.6	Insecure components such as routers, switches and firewalls with unpatched vulnerabilities can be utilised by attackers to disrupt services	4	Network devices are often targeted by attackers since they play a vital role in traffic management, any unpatched vulnerabilities would make is easy for an attacker to target the network.	4	Successful exploitation of network vulnerabilities would potentially give attackers control of the network components, leading to breaches of confidential data, system outages and	16
IS5.7	Without a real-time monitoring system to alert	4	DoS attacks can be easily stopped or mitigated if identified in time, having	4	Unnoticed and undetected, a DoS attack or can be very severe, resulting in significant	16

	admins to unusual network traffic, a DoS attack might not be noticed until it has been completed.		no real-time monitoring systems makes it likely that an attack would be successful.		downtime when eventually discovered and potential loss of data as well as system operations.	
IS5.8	Lack of antivirus or out of date antivirus software on end user machines leaves them vulnerable to malware infection.	4	It is common for individual users to neglect software updates, with a university having so many devices there is an increased probability of unprotected systems.	4	Malware infections, although easily prevented, can have significant impacts on devices with a loss of data integrity likely, as well as the breach of sensitive information and potentially even loss of system function.	16
IS5.9	Without real-time monitoring and filtering over the network, malware can be left to spread over time to other systems and cause significantly more damage.	4	Malware infections are easily detected early on, however without monitoring systems it is likely it will spread across the network.	5	The systematic spread of malware through a network, if undetected can lead to widespread data breaches, long term system outages and damage to the universities reputation. Remedying an extensive malware infection can be incredibly costly.	20
Asset	**Physical Asset Inventory / Management**					
IS6.1	If there is not up to date inventory tracking system, assets can easily be stolen or lost without being detected.	4	Without a system in place to track assets, it is likely that several could go missing or be misappropriated.	3	The theft or loss of physical assets will not only carry a financial burden but could lead to the breach of confidential data stored on said devices.	12
IS6.2	Unmaintained servers which are critical for the processing of student data may fail and go undetected leading to server failure and loss of data	4	If servers and other critical components are not frequently maintained or monitored it is likely that eventually a component will fail and therefore go unnoticed until it causes an issue	5	The impact of server system failure and the subsequent loss of student data / employee information / exam results would drastically affect the universities' ability to function and incur long-term system outages with a costly repair bill.	20
IS6.3	Physical media is not properly sanitised or destroyed when no longer needed, leading to data leakage which count potentially include sensitive data.	3	The improper disposal of media is a realistic risk, without an existing policy on the disposal of media sensitive data could easily be accidentally leaked	2	Whilst the leakage could potentially contain minor amounts of sensitive data, it is unlikely that it would be discovered to be used maliciously. Could have minor financial repercussions if reported.	6

Table C - Risk Analysis

6.0 Risk Treatment

The proposition and evaluation of effective controls to implement will be documented below. Starting from those with the highest risk scores, each incident scenario **IS** will have a new re-calculated risk score to establish the residual risk. For the purposes of this risk assessment, the Incident Scenarios being treated are those which were evaluated in the previous section to have a total risk score of 12 or higher (High). All risk reducing controls suggested are in-line with the ISO 27002:2017 framework (British Standards Institution, 2017).

L = Likelihood **I** = Impact **R** = Risk Score

Incident Scenario	**L**	**I**	**R**	**Control**	**Justification for Controls**	**L**	**I**	**R**
Very High Risk Scores								
IS2.2								
Users are tricked into providing their credentials, allowing a malicious party access with which they can alter files and spread malware.				**Secure Log-On Procedures (A9.4.2)**	Multi-Factor authentication adds an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials as the attacker should not be able to access the system.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing scams.			
				User Access Management (A9.2)	By controlling access to sensitive data to only those who require it, the spread of malware can be controlled effectively reducing the impact of malware infection.			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university to quickly shut down and prevent further damage from a malware infection.			
Risk Score (L.I.R)	4	5	20		**Residual Risk Post Control (L.I.R)**	2	3	6
IS3.7								
Known vulnerabilities which were left unpatched are exploited for an attacker to deploy ransomware or other malware.				**Management Of Technical Vulnerabilities (A12.6.1)**	Regularly updating the system and implementing security patches will prevent attackers abusing known vulnerabilities to exploit the system lowering the likelihood of gaining access to the system.			
				Network Controls (A13.1.1)	Network controls such as firewalls and intrusion detection systems can help admins to mitigate the attack once initiated, reducing the impact of the malware on the system			
				Controls Against Malware (A12.2.1)	Anti-malware software can be used to detect malicious software and prevent its execution, reducing the impact over the whole system.			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university to quickly shut down and prevent further damage from a malware infection.			

			Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of an attack, allowing the system to be reinstated fully in a short period of time.				
			Outsourced Development (A14.2.7)	Outsourcing regular testing of the network to identify any vulnerabilities and patching them appropriately will reduce the likelihood of a successful exploit exposing data.				
Risk Score (L.I.R)	4	5	20	**Residual Risk Post Control (L.I.R)**			2	3	6
IS3.8									
A ransomware attack succeeds and encrypts all the data on the system, without an appropriate plan to handle the attack it spreads to the whole system without being isolated.				**Controls Against Malware (A12.2.1)**	Anti-malware software can be used to detect the malicious software and prevent its execution, reducing the impact over the whole system.				
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university respond quickly and contain the spread of the ransomware virus.				
				Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of an attack, allowing the system to be reinstated fully in a short period of time.				
				Network Segregation (A13.1.3)	Splitting up the network can prevent ransomwares spread across different segments of the network such as student/teacher sections, reducing the impact.				
Risk Score (L.I.R)	4	5	20	**Residual Risk Post Control (L.I.R)**			3	3	9
IS5.3									
Without email filtering, malicious links and phishing emails are significantly more likely to end up in users' inboxes.				**Network Controls (A13.1.1)**	Implementation of an email filter will significantly reduce the number of phishing and other malicious emails reaching users inboxes, thereby lowering the likelihood of a successful phishing attack.				
				Security Education, Training and Awareness (A7.2.2)	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing scams.				
				Secure Log-On Procedures (A9.4.2)	Multi-Factor authentication will add an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials.				
				Incident Response Plans (A16.1)	A well-established incident response plan specific to phishing attacks will allow admins to quickly identify compromised accounts and block the compromised accounts.				
				User Access Management (A9.2)	By limiting access to sensitive data to only those who require it, the data which is accessible and therefore the impact of compromised accounts can be reduced.				
Risk Score	5	4	20	**Residual Risk Post Control (L.I.R)**			2	3	6

(L.I.R)								
IS5.4								
Untrained / unaware employees are more likely to fall victim to phishing emails, often leading to their accounts being used to spread the malicious email around.				**Security Education, Training and Awareness (A7.2.2)**	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing scams.			
				Secure Log-On Procedures (A9.4.2)	Multi-Factor authentication will add an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials.			
				Incident Response Plans (A16.1)	A well-established incident response plan specific to phishing attacks will allow admins to quickly identify compromised accounts and block the compromised accounts.			
				User Access Management (A9.2)	By limiting access to sensitive data to only those who require it, the data which is accessible and therefore the impact of compromised accounts can be reduced.			
Risk Score (L.I.R)	4	5	20		**Residual Risk Post Control (L.I.R)**	2	3	6
IS5.9								
Without real-time monitoring and filtering over the network, malware can be left to spread over time to other systems and cause significantly more damage.				**Event Logging (A12.4.1)**	Real-time network monitoring will alert admins to suspicious network activities, allowing for early response to malware infections and reducing its impact.			
				Network Controls (A13.1.1)	Network controls such as firewalls and intrusion detection systems can help admins to mitigate malwares spread and impact once the network is infected.			
				Network Segregation (A13.1.3)	Splitting up the network can limit spread across different segments of the network, reducing the impact of malware on a system.			
				Controls Against Malware (A12.2.1)	Anti-malware software can be used to detect malicious software and prevent its execution, reducing the impact over the whole system.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training reinforced with awareness campaigns will reduce the likelihood of users downloading malicious files and infecting the network.			
Risk Score (L.I.R)	4	5	20		**Residual Risk Post Control (L.I.R)**	3	3	9
IS6.2								
Unmaintained servers which are critical for the processing of student data may fail and go undetected leading to server failure and				**Operational Procedures and Responsibilities (A12.1.1)**	Documented schedules for the regular maintenance and monitoring of systems ensures optimal performance, early detection of upcoming failures reducing the likelihood of a critical failure			
				Equipment				

loss of data.				**Maintenance (A11.2.4)**				
				Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of a system failure, allowing the system to be reinstated fully in a short period of time.			
Risk Score (L.I.R)	4	5	20	**Residual Risk Post Control (L.I.R)**			2	3	6
High Risk Scores									
IS1.2									
An untrained employee falls for a phishing email and inadvertently provides access to student data.				**Secure Log-On Procedures (A9.4.2)**	Multi-Factor authentication adds an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials as the attacker should not be able to access the system.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing scams.			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university to contain the impact of the data breach.			
Risk Score (L.I.R)	4	4	16	**Residual Risk Post Control (L.I.R)**			2	2	4
IS2.5									
Unauthorised or malicious changes to the files / content on the platform go undetected.				**Logging and Monitoring (A12.4.3)**	A file integrity monitoring system could be implemented, allowing detection and alerts when unauthorised changes are made to files and content, allowing admins to quickly react to security incidents.			
				User Access Management (A9.2)	By limiting access to sensitive data to only those who require it, the data which is accessible and therefore the impact of unauthorised changes can be reduced.			
Risk Score (L.I.R)	4	4	16	**Residual Risk Post Control (L.I.R)**			3	3	9
IS3.1									
A student/attacker brute forces weak account credentials allowing access to change examination results.				**Password Management System (A9.4.3)**	Enforcing strong password policies which include requiring adequate password complexity and change frequency will reduce the likelihood of an attacker successfully brute forcing an account			
				Secure Log-On Procedures (A9.4.2)	The implementation of both Multi-Factor Authentication and an account lockout after several failed login attempts will reduce the likelihood of an attacker gaining access			
				Security Education, Training and Awareness (A7.2.2)	Regular security training will educate users on appropriate password security, reducing the likelihood of brute forced passwords.			
				Logging and	A file integrity monitoring system could be implemented, allowing detection			

				Monitoring (A12.4.3)	and alerts when unauthorised changes are made to files and content, allowing admins to quickly react.			
Risk Score (L.I.R)	4	4	16		**Residual Risk Post Control (L.I.R)**	2	3	6
IS3.2								
A staff member with legitimate access changes a students' examination results for them and the change is undetected.				**Security Education, Training and Awareness (A7.2.2)**	Regular security training will educate staff members on the impacts of changing such critical data, reducing the likelihood of occurrence.			
				Management of Privileged Access Rights (A9.2.3)	Regular reviews of who has access to modify exam results would ensure that only the necessary staff have access reducing the likelihood of this event.			
				Logging and Monitoring (A12.4.3)	A file integrity monitoring system could be implemented, allowing detection and alerts when unauthorised changes are made.			
				Change Management (A12.1.2)	A formal moderation process requiring approval of changes to critical data such as exam results will prevent unauthorised changes being made.			
Risk Score (L.I.R)	4	4	16		**Residual Risk Post Control (L.I.R)**	1	4	4
IS3.5								
A staff member is tricked into providing access to the examination system through a malicious email.				**Security Education, Training and Awareness (A7.2.2)**	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing email scams.			
				Secure Log-On Procedures (A9.4.2)	Multi-Factor authentication adds an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials as the attacker should not be able to access the system.			
				Incident Response Plans (A16.1)	A well-established incident response plan specific to phishing attacks will allow admins to quickly identify compromised accounts and block the compromised accounts.			
Risk Score (L.I.R)	4	4	16		**Residual Risk Post Control (L.I.R)**	2	3	6
IS4.2								
An untrained employee falls for a phishing email and inadvertently provides access to employee data and records.				**Security Education, Training and Awareness (A7.2.2)**	Regular security training reinforced with awareness campaigns will reduce the likelihood of users falling for phishing scams.			
				Secure Log-On Procedures (A9.4.2)	Multi-Factor authentication will add an extra layer of protection to the system, requiring users to use a second verification mechanism lowers the impact in the event of compromised credentials.			
				Incident Response	A well-established incident response plan specific to phishing attacks will			

				Plans (A16.1)	allow admins to quickly identify compromised accounts and block the compromised accounts.			
				User Access Management (A9.2)	By limiting access to sensitive data to only those who require it, the data which is accessible and therefore the impact of compromised accounts can be reduced.			
Risk Score (L.I.R)	4	4	16		**Residual Risk Post Control (L.I.R)**	2	3	6
IS5.1								
Sensitive information transmitted over a network without encryption can be intercepted and read by any unauthorised individual.				**Cryptographic Controls (A10.1)**	Implementing encryption will obscure the content of the data in transit over the network, reducing the impact of any data which is intercepted by making it unintelligible.			
				Network Controls (A13.1.1)	Using secure protocols for communications such as HTTPS and SSL/TLS will add a layer of security to protect data from interception.			
				Information Security Reviews (A18.2.2)	Regular audits on information security will ensure that the network infrastructure is not vulnerable to interception and that encryption is applied effectively.			
				Handling of Assets (A8.2.3)	Implementing policy for the handling of sensitive information will ensure users make use of encryption and secure protocols.			
Risk Score (L.I.R)	4	4	16		**Residual Risk Post Control (L.I.R)**	2	1	2
IS5.6								
Insecure components such as routers, switches and firewalls with unpatched vulnerabilities can be utilised by attackers to disrupt services.				**Management Of Technical Vulnerabilities (A12.6.1)**	Regularly updating the system and implementing security patches will prevent attackers abusing known vulnerabilities to exploit the system lowering the likelihood of disruption and loss of availability.			
				Network Controls (A13.1.1)	Proper configuration of devices such as switches, routers and firewalls including disabling unnecessary services will minimise attack surface and reduce the likelihood of system disruptions.			
				Information Security Reviews (A18.2.2)	Regular audits on information security will ensure that the network infrastructure is not vulnerable to interception and that encryption is applied effectively.			
				Outsourced Development (A14.2.7)	Outsourcing regular testing of the network to identify any vulnerabilities and patching them appropriately will reduce the likelihood of a successful exploit exposing data.			

				Incident Response Plans (A16.1)	A well-established incident response plan for the event of network disruptions and data breaches will allow admins to quickly resolve issues reducing further impact.			
Risk Score (L.I.R)	4	4	16	**Residual Risk Post Control (L.I.R)**		2	3	6
IS5.7								
Without a real-time monitoring system to alert admins to unusual network traffic, a DoS attack might not be noticed until it has been completed.				**Network Controls (A13.1.1)**	Implementation of an Intrusion Detection System would allow automatic detection and potentially even halting of DoS attacks in progress, reducing the impact of such attacks.			
				Incident Response Plans (A16.1)	A well-established incident response plan for the event of network attacks such as DoS attacks will allow admins to quickly resolve issues reducing further impact and preventing complete loss of system availability			
Risk Score (L.I.R)	4	4	16	**Residual Risk Post Control (L.I.R)**		3	2	6
IS5.8								
Lack of antivirus or out of date antivirus software on end user machines leaves them vulnerable to malware infection.				**Controls Against Malware (A12.2.1)**	Installing and maintaining software on end user machines to detect and prevent malware infections is the easiest way to quickly reduce the likelihood of accidental malware infection and the impact of malware itself.			
				Installation of Software on Operational Systems (A12.5.1)	Procedures for the maintenance and control of applications/software on end-user machines will ensure adequate antivirus safety measures are working.			
				User Access Management (A9.2)	By limiting accessibility to sensitive data or critical systems the potential impact of a malware infection can be minimised.			
Risk Score (L.I.R)	4	4	16	**Residual Risk Post Control (L.I.R)**		2	2	4
IS1.5								
An attacker uses brute force to crack a weak password and access student personal data.				**Password Management System (A9.4.3)**	Enforcing strong password policies which include requiring adequate password complexity and change frequency will reduce the likelihood of an attacker successfully brute forcing an account			
				Secure Log-On Procedures (A9.4.2)	The implementation of both Multi-Factor Authentication and an account lockout after several failed login attempts will reduce the likelihood of an attacker gaining access.			
				Security Education, Training and	Regular security training will educate users on appropriate password security, reducing the likelihood of brute forced passwords.			

				Awareness (A7.2.2)				
				Logging and Monitoring (A12.4.3)	A file integrity monitoring system could be implemented, allowing detection and alerts when unauthorised changes are made to files and content, allowing admins to quickly react.			
Risk Score (L.I.R)	3	5	15		**Residual Risk Post Control (L.I.R)**	2	3	6
IS1.6								
A ransomware attack encrypts student personal data and there are no backups available for recovery leading to total loss of data.				**Controls Against Malware (A12.2.1)**	Anti-malware software can be used to detect the malicious ransomware and prevent its execution, reducing the impact over the whole system.			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university respond quickly and contain the spread of the ransomware through to other systems.			
				Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of an attack, allowing the system to be reinstated fully in a short period of time.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training can reduce the likelihood of the ransomware infiltrating the system, whether it came from a phishing email or was an unsolicited download.			
Risk Score (L.I.R)	3	5	15		**Residual Risk Post Control (L.I.R)**	2	2	4
IS2.3								
An attacker can gain access due to weak or compromised credentials and a poor authentication mechanism				**Password Management System (A9.4.3)**	Enforcing strong password policies which include requiring adequate password complexity and change frequency will reduce the likelihood of an attacker successfully brute forcing an account.			
				Secure Log-On Procedures (A9.4.2)	The implementation of both Multi-Factor Authentication and an account lockout after several failed login attempts will reduce the likelihood of an attacker gaining access.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training will educate users on appropriate password security, reducing the likelihood of brute forced passwords.			
Risk Score (L.I.R)	3	5	15		**Residual Risk Post Control (L.I.R)**	2	3	6
IS3.6								
A server failure leads to a loss of almost all data on exam results, without proper backups this data / parts of it are forever lost.				**Operational Procedures and Responsibilities (A12.1.1)**	Documented schedules for the regular maintenance and monitoring of systems ensures optimal performance, early detection of upcoming failures reducing the likelihood of a critical failure.			
				Equipment Maintenance (A11.2.4)				

			Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of a system failure, allowing admins to restore most/all the data with minimal long-term impact				
			Incident Response Plans (A16.1)	A well-established incident response plan will allow the university to quickly react and restore lost data.				
Risk Score (L.I.R)	3	5	15	**Residual Risk Post Control (L.I.R)**	2	2	4	
IS4.5								
An attacker uses brute force to crack a weak password and access employee's personal data.				**Password Management System (A9.4.3)**	Enforcing strong password policies which include requiring adequate password complexity and change frequency will reduce the likelihood of an attacker successfully brute forcing an account.			
				Secure Log-On Procedures (A9.4.2)	The implementation of both Multi-Factor Authentication and an account lockout after several failed login attempts will reduce the likelihood of an attacker gaining access.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training will educate users on appropriate password security, reducing the likelihood of brute forced passwords.			
Risk Score (L.I.R)	3	5	15	**Residual Risk Post Control (L.I.R)**	2	3	6	
IS4.6								
A ransomware attack encrypts all employee personal data and there are no backups available for recovery.				**Controls Against Malware (A12.2.1)**	Anti-malware software can be used to detect the malicious ransomware and prevent its execution, reducing the impact over the whole system.			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university respond quickly and contain the spread of the ransomware through to other systems.			
				Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of an attack, allowing the system to be reinstated fully in a short period of time.			
				Security Education, Training and Awareness (A7.2.2)	Regular security training can reduce the likelihood of the ransomware infiltrating the system, whether it came from a phishing email or was an unsolicited download.			
Risk Score (L.I.R)	3	5	15	**Residual Risk Post Control (L.I.R)**	2	2	4	
IS5.5								
Without redundant paths and failover capabilities, the university network will be vulnerable to DoS attacks shutting down the whole network system.				**Segregation in Networks (A13.1.3)**	Redundant network paths and failover capabilities will allow traffic to be routed elsewhere in the event of a DoS attack, maintaining network availability.			
				Network Controls (A13.1.1)	Intrusion Detection Systems allow for early detection of impending DoS attacks allowing admins to prevent them or reduce their impact on the network.			

			Management Of Technical Vulnerabilities (A12.6.1)	Regularly updating the system and implementing security patches will prevent attackers abusing known vulnerabilities to exploit the system lowering the likelihood of gaining access to the system.				
			Information Security Reviews (A18.2.2)	Regular audits on information security will ensure that the network infrastructure is not vulnerable to DoS attacks.				
			Outsourced Development (A14.2.7)	Outsourcing regular testing of the redundancy and failover mechanisms will ensure that the network in not vulnerable and reduce likelihood of a successful DoS attack.				
Risk Score (L.I.R)	3	5	15	**Residual Risk Post Control (L.I.R)**	2	3	6	
IS1.3								
An attacker exploits network vulnerabilities to access student personal data.			**Management Of Technical Vulnerabilities (A12.6.1)**	Regularly updating the system and implementing security patches will prevent attackers abusing known vulnerabilities to exploit the system lowering the likelihood of gaining access to the system.				
			Network Controls (A13.1.1)	Network controls such as firewalls and intrusion detection systems alert admins to ongoing system attacks and allow for them to be stopped before they’ve had a great impact				
			Outsourced Development (A14.2.7)	Outsourcing regular testing of the network to identify any vulnerabilities and patching them appropriately will reduce the likelihood of a successful exploit exposing data.				
Risk Score (L.I.R)	3	4	12	**Residual Risk Post Control (L.I.R)**	2	2	4	
IS1.4								
An attacker intercepts data in transmission, allowing them access to unencrypted student personal data.			**Cryptographic Controls (A10.1)**	Implementing encryption will obscure the content of the data in transit over the network, reducing the impact of any data which is intercepted by making it unintelligible.				
			Network Controls (A13.1.1)	Implementing encryption will obscure the content of the data in transit over the network, reducing the impact of any data intercepted by making it unintelligible.				
			Information Security Reviews (A18.2.2)	Regular audits on information security will ensure that the network infrastructure is not vulnerable to interception and that encryption is applied effectively.				
			Handling of Assets (A8.2.3)	Implementing policy for the handling of sensitive information will ensure users make use of encryption and secure protocols.				
Risk Score (L.I.R)	4	3	12	**Residual Risk Post Control (L.I.R)**	2	1	2	
IS2.1								

A server failure causes and outage, access to the platform and all resources is impossible for an extended period.				**Operational Procedures and Responsibilities (A12.1.1)**	Documented schedules for the regular maintenance and monitoring of systems ensures optimal performance, early detection of upcoming failures reducing the likelihood of a critical failure.			
				Equipment Maintenance (A11.2.4)				
				Information Backup (A12.3.1)	Regular backups of the critical data stored within the system will drastically reduce the impact of a system failure, allowing admins to restore most/all the data with minimal long-term impact			
				Incident Response Plans (A16.1)	A well-established incident response plan will allow the university to quickly react and restore lost data.			
Risk Score (L.I.R)	3	4	12			**Residual Risk Post Control (L.I.R)**	3	3	9
IS4.3								
An attacker exploits network vulnerabilities to access employee personal data and records.				**Management Of Technical Vulnerabilities (A12.6.1)**	Regularly updating the system and implementing security patches will prevent attackers abusing known vulnerabilities to exploit the system lowering the likelihood of gaining access to the system.			
				Network Controls (A13.1.1)	Network controls such as firewalls and intrusion detection systems alert admins to ongoing system attacks and allow for them to be stopped before they’ve had a great impact			
				Outsourced Development (A14.2.7)	Outsourcing regular testing of the network to identify any vulnerabilities and patching them appropriately will reduce the likelihood of a successful exploit exposing data.			
Risk Score (L.I.R)	3	4	12			**Residual Risk Post Control (L.I.R)**	2	2	4
IS4.4								
An attacker intercepts data in transmission, allowing them access to unencrypted				**Cryptographic Controls (A10.1)**	Implementing encryption will obscure the content of the data in transit over the network, reducing the impact of any data which is intercepted by making it unintelligible.			
				Network Controls (A13.1.1)	Implementing encryption will obscure the content of the data in transit over the network, reducing the impact of any data which is intercepted by making it unintelligible.			
				Information Security Reviews (A18.2.2)	Regular audits on information security will ensure that the network infrastructure is not vulnerable to interception and that encryption is applied effectively.			
				Handling of Assets (A8.2.3)	Implementing policy for the handling of sensitive information will ensure users make use of encryption and secure protocols.			
Risk Score	4	3	12			**Residual Risk Post Control (L.I.R)**	2	1	2

(L.I.R)								
IS5.2								
Devices on the network which may be compromised could be used to capture sensitive communications				**Management Of Technical Vulnerabilities (A12.6.1)**	Regular audits and vulnerability assessments can help identify any security weaknesses in network devices			
				Network Controls (A13.1.1)	Network Access Control systems can be used to prevent unauthorised devices and to isolate and quarantine compromised devices, preventing them from accessing and capturing sensitive information			
					Intrusion Detection Systems could detect malicious activities on the network, including unauthorised interception and capture of sensitive data.			
				Cryptographic Controls (A10.1)	Implementing encryption will obscure the data in transit over the network, reducing the impact of any content which is intercepted by making it unintelligible.			
Risk Score (L.I.R)	3	4	12		**Residual Risk Post Control (L.I.R)**	2	1	2
IS6.1								
If there is not up to date inventory tracking system, assets can easily be stolen or lost without being detected				**Responsibility for Assets (A8.1)**	Implementation of an asset management system, including documentation of assets outgoing and incoming will reduce the risk of assets being lost through theft. Asset management systems can also include the use of asset tags and regular inventory checks.			
				Physical Entry Controls (A11.1.2)	Ensuring that assets are securely stored with physical security measures guarding them such as cameras and locks will reduce the risks and ability for theft of property.			
				Disposal of Media (A8.3.2)	Wiping hard drives when devices return ensures that there is no sensitive data remaining, reducing the risk of data leakage when assets are reassigned, disposed of or misappropriated.			
				Insurance Policies	By taking out an insurance policy on physical assets, any monetary loss from their theft can be recouped, lowering its impact on the university.			
Risk Score (L.I.R)	4	3	12		**Residual Risk Post Control (L.I.R)**	2	2	4

Table D - Risk Treatment

7.0 Conclusion / Recommendations

Throughout the risk assessment, a wealth of information assets and supporting physical assets have been identified, analysed, and treated for vulnerabilities. The results of the risk treatment are shown below in *figures 7,8,9*.

As shown in *figure 7*, almost half of all controls implemented would be procedural, with the next most common being technical.

Implementation of the suggested controls would lead to a risk reduction of over 50%, with average risk reducing from High to Low, the 5 controls listed in *figure 6* make up 49% of the total risk-reducing controls and as such implementation of them is of paramount importance to immediately reduce the risk posture of the university.

All the controls suggested however, together, are required to reduce risk as seen in the *figure 9* below and subject to a cost-benefit-analysis the implementation of all those mentioned in *Table D* should be considered for a more complete reduction in risk across this broad set of a university's information assets.

Control	Frequency	%
Security Education, Training and Awareness (A7.2.2)	**14**	**12**
Incident Response Plans (A16.1)	**14**	**12**
Network Controls (A13.1.1)	**12**	**10**
Secure Log-On Procedures (A9.4.2)	**10**	**9**
User Access Management (A9.2)	**7**	**6**

Figure 6 - Top 5 Controls

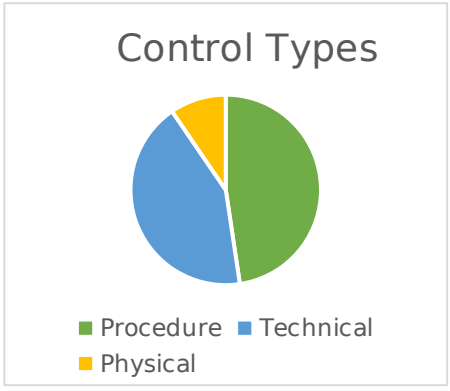

Figure 7 – Control Types

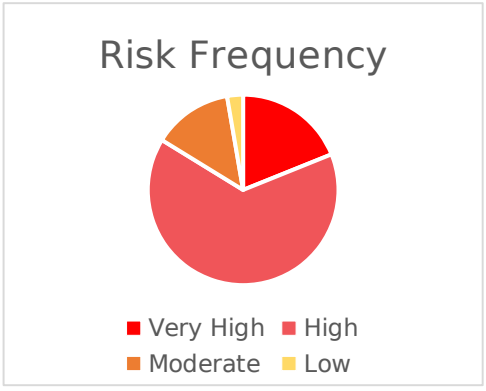

Figure 8 – Risk Frequency

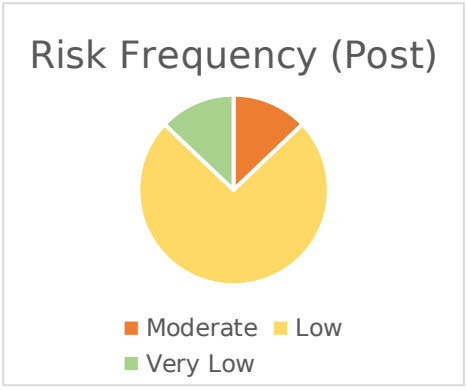

Figure 9 – Risk Frequency Post Control

As is demonstrated above in *figure 10*, average risk has been significantly reduced due to the treatments suggested for all risks and vulnerabilities identified throughout this report. Whilst there has been a strong focus on information security risks aligning with ISO 27000 principles, supporting physical assets have also been considered to reduce the risks faced by a typical UK university.

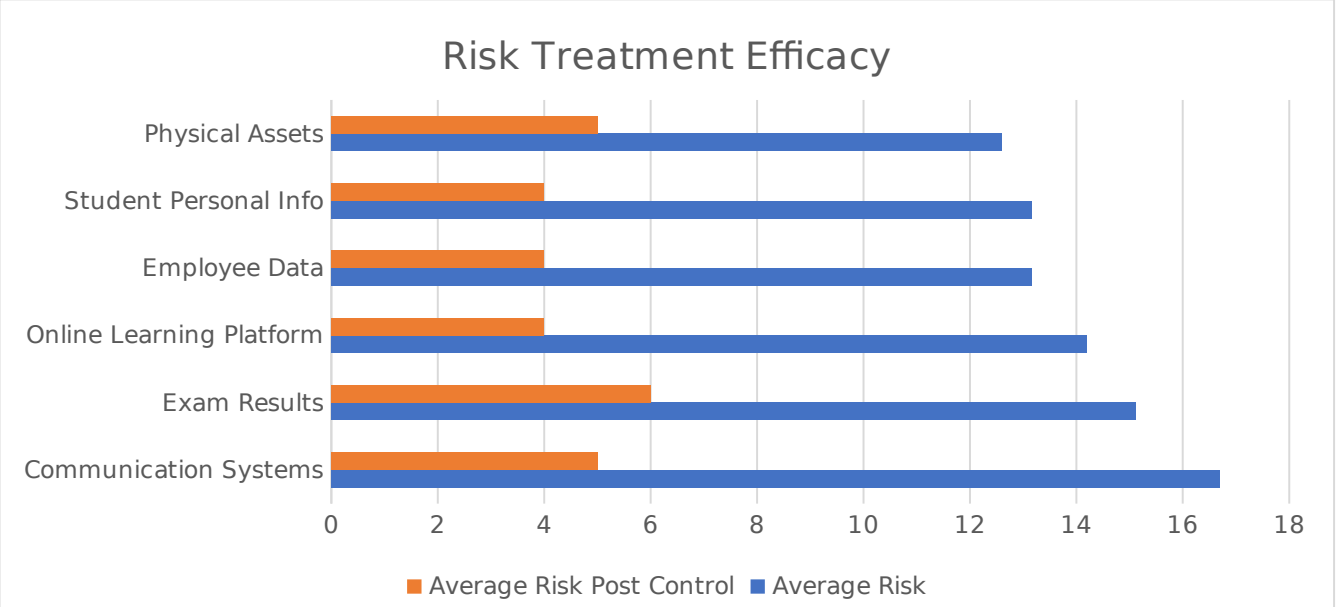

Figure 10 – Risk Treatment Efficacy

Following these recommendations for risk treatment, to maintain effective controls, regular reviews must be arranged with further risk assessments to be carried out at a regular interval analysing the efficacy of the control implementation over a greater period and focussing further on cost-benefit analysis where relevant.

8.0 References

Department for Digital, Culture, Media & Sport. (2022, March 30). *Cyber Security Breaches Survey 2022*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Office for National Statistics. (2022, September 26). *Nature of fraud and computer misuse in England and Wales - Office for National Statistics*. www.ons.gov.uk. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

British Standards Institution. (2023). *BS EN ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. Retrieved from https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030468519

British Standards Institution. (2017). *Information technology. Security techniques. Code of practice for information security controls (BS EN ISO/IEC 27002:2017)*. Retrieved from https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030347481

British Standards Institution. (2022). *BS ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks*. Retrieved from https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030412541