21/11/23 – UP2009045

2023

UK Based University Risk Assessment

SECURITY MANAGEMENT
ADAM COOPER
UP2009045
WORD COUNT: 2117

Contents

Introduction

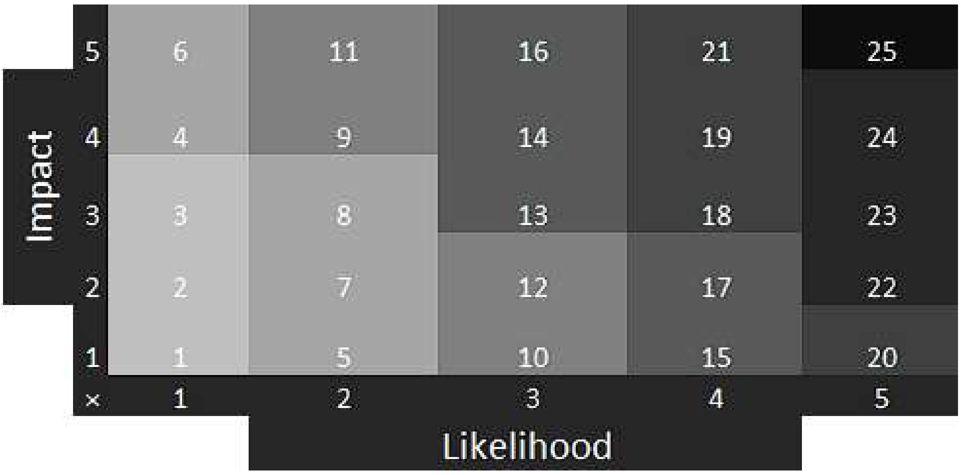
The aim of this report is to undertake a security risk assessment of a typical university which would be based in the United Kingdom to define areas where security can be improved further or any current threat areas that need to be followed up.

Following on from this, this report will follow these main objectives. Firstly, identifying assets of a UK university. Secondly, the threats associated with each of these assets. Lastly, the vulnerabilities associated with the threats. This will give us a good overview of the threat landscape and allow us to produce a risk score based on the impact and likelihood of each individual threat to an asset.

After the initial risk score has been calculated, treatment/controls will be suggested, and a reviewed risk score will be generated to act like these changes were actioned and threats had been remediated.

What constitutes an information security risk?
An information security risk is based on anything which breaches the CIA triad, thus breaking either confidentiality or integrity, or preventing the availability of information.

Risk Metrics



Impact	5	6	11	16	21	25
	4	4	9	14	19	24
	3	3	8	13	18	23
	2	2	7	12	17	22
	1	1	5	10	15	20
	×	1	2	3	4	5
			Likelihood			

Risk score will be calculated following ISO 27005 requirements of impact × likelihood and an enhanced risk matrix for the calculation of risks where 1 is notable and 25 is potentially catastrophic.

Nature of business
The typical UK based university has a primary focus of providing education, public or private sector with the production of two main outputs graduates and research.

Executive Summary

Context

The main purpose of this risk assessment is to verify the university's risk compliance via identifying and evaluating threats and vulnerabilities, assessing them against the ISO 27005 standard. Both asset owners and extended management team members will find this report useful endeavouring to reduce and remediate risk.

Methodology

Curating a qualitative asset-based approach along with the application of binary risk analysis, we calculated the impact/likelihood of individual threats to each identified asset. This produced our risk register providing an overview of the university's threat landscape.

Key Identified Risks

To calculate risk, we used the risk matrix calculation defined in ISO 27005 requirements of impact × likelihood and an enhanced risk matrix for the calculation of risks where 1 is notable and 25 is potentially catastrophic. Below are both key risks discovered and controls most needed in accordance with frequency along with recommendations for going forward.

Key Risks

- Improper access control.
- Out of date software/hardware for current/backup systems and software.
- Data theft.
- Insufficient password management.

Key Controls

- Multifactor authentication.
- Update: Software, hardware, firmware, operating systems.
- Staff training for data security, sensitivity, and social engineering scenarios.
- Enforce strong password and encryption policies for files.

Recommendations

The following controls are those which are recommended, can be implemented quickly with no impact to current services in the estate and would have an overall benefit most risks identified.

Multifactor authentication – Remediates brute forcing and unauthorised access to accounts.

Update software/operating systems of both current and backup equipment – Reduces system vulnerabilities.

Organisational Benefit

The overall benefit of this risk assessment to the university is to identify the vulnerabilities which are currently present within the organisation, weaknesses which can be controlled sufficiently and security measures which can be implemented to ensure best remediation of any threats which remain and pose the greatest risk.

As the university compiles personal data, research data along with dealing with other sensitive information i.e., financial information, it is of the utmost importance that the university complies with all applicable industry regulations and standards like HIPAA for ensuring that sensitive health information is kept confidential, this would apply to any student with a disability, EC claims, the University dentist and surgery. GDPR to protect the confidentiality of student and staff information, PCI for processing payments i.e., the student union and compliance with ISO27001 for risk management against data being handled, processed and any potential risks towards assets within the university. Carrying out the risk assessment successfully demonstrates compliance towards these standards and regulations avoiding any legal actions or other adverse actions by not abiding.

This security risk assessment will also provide a better vision and understanding of Return of Investment (ROI) allowing for enhanced strategic planning with more identifiable goals and achievements for security in the future. ROI for security is not easily identified without a risk assessment leaving justification of security investments, stakeholder communication and quantification of potential losses to be a mystery or lacking. Conducting this risk assessment allows for the quantification of potential loss comparing to what can be invested at that time and providing a justification for investment, how security controls will help, what threats/vulnerabilities they will remove and how potential loss or damages to the organisation will be reduced.

Risk Assessment

Threat & Vulnerability Identification

Assets	Threats	Vulnerabilities	Description	Inherent Risk		
				Impact	Probability	Risk Level
Operating Systems	Improper access controls	Malware - Brute force attacks	Brute force attacks on operating systems with incorrect access controls such as MFA present the risk of attackers gaining access	3	5	23
Cloud Software	Theft of documents	Open S3 buckets	Misconfigured S3 buckets which are open potentially allow data theft via internal staff or external threat actors if completely open	5	4	21
Operating Systems	Malware attacks	Unchanged superuser credentials	Standard superusers i.e., admin:admin are well known and easily guessed by attackers	5	5	25
Internal Systems	Device failure	Outdated operating system / Software	Old OS/Software versions can produce incompatibility issues, performance issues or system failure	4	5	24

Table 1 – Table containing example risks of the highest threat to the university.

Table 1 displays four risks which pose the highest threat to the university across various areas covering cloud applications, operating systems, and internal systems. These all present a risk to one of more aspects of the CIA triad and are substantial enough that they can generate or contribute to other risks present within the risk register leading to potential catastrophic consequences.

Cloud software – Theft of documents

Misconfigured S3 buckets (AWS) or equivalent dependent on cloud services the university is using (e.g., blob storage for Azure) creates an access point to stored documentation and the network. Focusing on S3 buckets, providing these are open, this allows anyone, threat actors or current employees to access them without any verification needed.

Should any sensitive documentation be stored in these S3's, this creates confidentiality, integrity, and availability issues. The free access to this documentation can allow for data manipulation, destruction and access to sensitive data which would otherwise be locked down to certain staff members.

Operating Systems – Brute force attacks

Improperly enforced access controls on operating systems such as poor password policies and/or lack of multi-factor authentication for user accounts will lead to successful brute force attacks by threat actors. These attacks open risk to confidentiality and integrity of sensitive documentation and the integrity of the systems themselves.

This is rated as a highly likely threat due to the risk being relatively simple following misconfigured controls with a medium impact score as although this would leave the threat actor with potential access to documentation and the ability to brake systems, administrative controls and individual file encryption would lessen the impact of this.

Operating Systems – Malware attacks

Similarly, to brute force attacks, both windows, Linux and OSX systems have standard admin users which have common username and password combinations such as admin:admin. This is one of the very first areas a threat actor will attack to escalate privileges within a network hence why this is rates as five for both impact and probability as it could not only allow them admin access to several services such as active directory but potentially a large knock-on effect throughout the entire estate.

Internal Systems – Device failure

Systems, components, and services with out-of-date software open the university up to device failure via compromised integrity. These old software versions introduce compatibility, performance, and security issues. This has been rated at five for probability as this is a common recurrence and is something which regularly presents threats to internal systems. Also presenting significant impact to internal systems, due to not only the loss of integrity but also the loss of availability potentially affecting the entire estate.

The affect on controlling these risks whether through remediation or risk reduction could dramatically lower the domino effect of other assets such as personally identifiable information, sensitive documents and infrastructure components being affected and further reducing compromise of CIA.

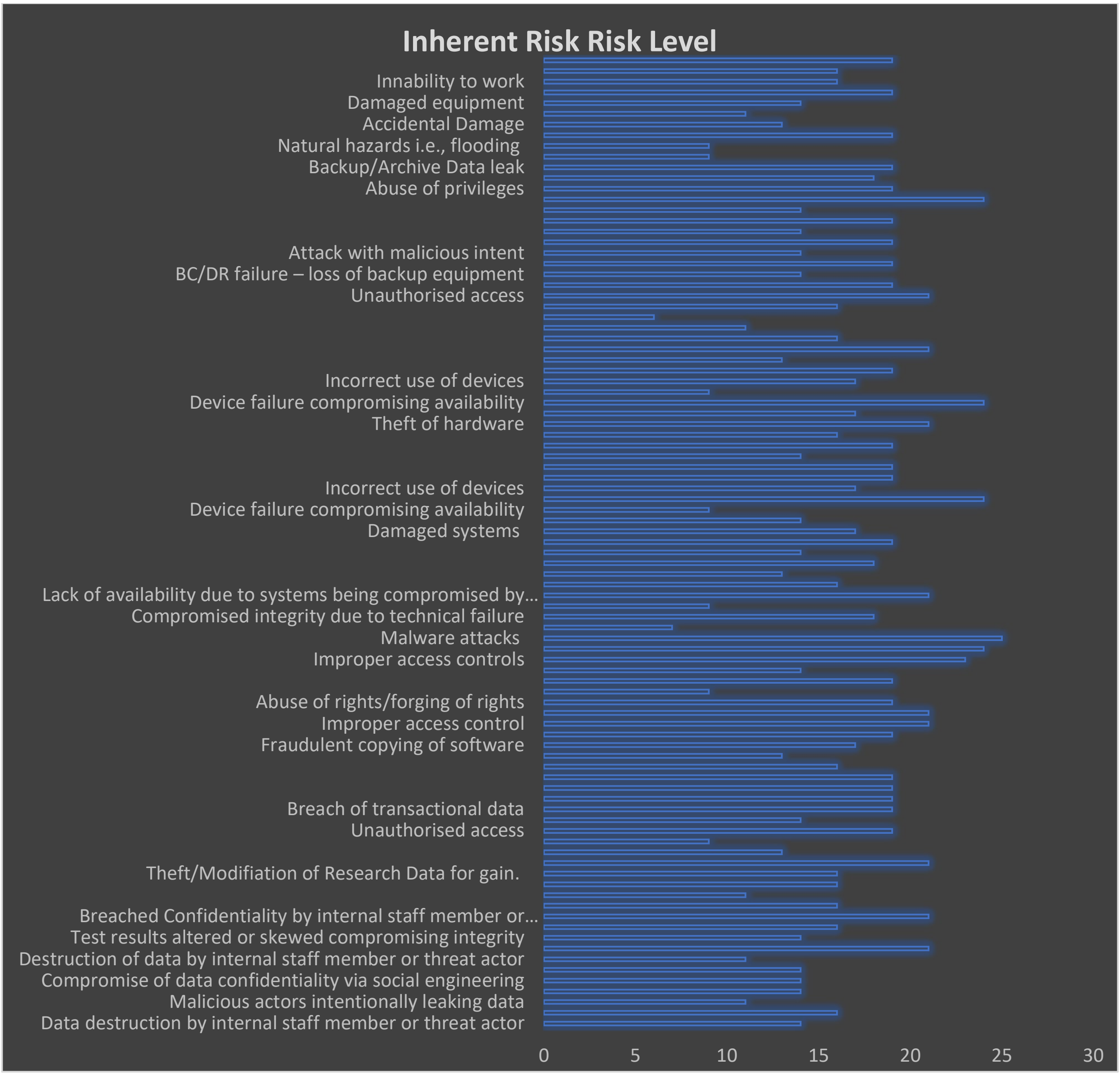


Figure 1 - Inherent risk level before controls have been implemented.

Risk Treatment/Control

The most identified risk controls fall in-line with risks associated with the highest threat towards the university's estate and found to be potential remediations, reductions or avoidance of multiple risks throughout separate asset groups also preventing collateral damage via a chain of consequences.

Unauthorised access	Lack of multifactor authentication	Systems lacking MFA are wide open to attacks which allow unauthorised access to the network	4	3	14	Implement Multifactor authentication such a SDO and Fido	2	2	7
Equipment Failure	Outdated server software/operating system	Improperly maintained server could lead to lack of availability following equipment failure	5	4	21	Implement regular update for both software and operating systems.	3	3	13
Compromise of data confidentiality via social engineering	Lack of staff training in social engineering scenarios i.e., phishing	Staff with improper training will not be able to easily recognise social engineering scenarios and therefore are more likely to hand out sensitive information	4	3	14	Dedicate training time to staff towards social engineering to increase social awareness within these scenarios	4	2	9
Lateral Movement	Server misconfiguration	Misconfiguration can easily allow threat actors to bypass security controls or gain access to high level accounts	5	2	11	Ensure server is configured as expected, applications/services are setup correctly	3	2	8

Table 2 – Table containing example risks associated with highest frequency controls.

Table 2 displays four risks to the university across various areas. These again all present a risk to one of more aspects of the CIA triad and are substantial enough that they can generate or contribute to other risks present within the risk register leading to potential catastrophic consequences. Attached are the controls and re-calculated risk score in accordance with these controls being applied.

Multifactor authentication and enforcement of strong password policies/file encryption

Implementing multifactor authentication into the university's estate instantly provides an extra layer of security whether this be something you have such as a soft or hard token, something you are i.e., FIDO key or something you know i.e., personal identification number. Usually these are forms of authentication an attacker would not be able to guess or brute force making gaining access near impossible without specific knowledge.

Pairing MFA with strong password policies for accounts and encrypted files significantly reduces both the impact and probability of a risk.

Update: Software, hardware, firmware, operating systems

Multiple threats identified within the risk registers are related to poor maintenance of computer systems and hardware. Creating a maintenance schedule to carry out important hardware, software and firmware updates will reduce the overall risk score and remediate any previous vulnerabilities to systems.

Staff training for data security, sensitivity, and social engineering scenarios

Providing training for staff on data security and social engineering scenarios to increase awareness of threat actors attempting to gain information, for example by acting as the person in question or a trusted third party the university deals with, greatly reduces the probability of compromised confidentiality. Although the impact score of this doesn't necessarily change, the significant impact this threat would originally introduce to the estate prior to staff training can easily be avoided.

Correct configuration of systems and services

Ensuring systems, servers, services, and applications are configured and setup correctly is paramount to preventing high level threats such as lateral movement. When working with cloud service providers, this risk must be shared as the university won't have full control over some settings.

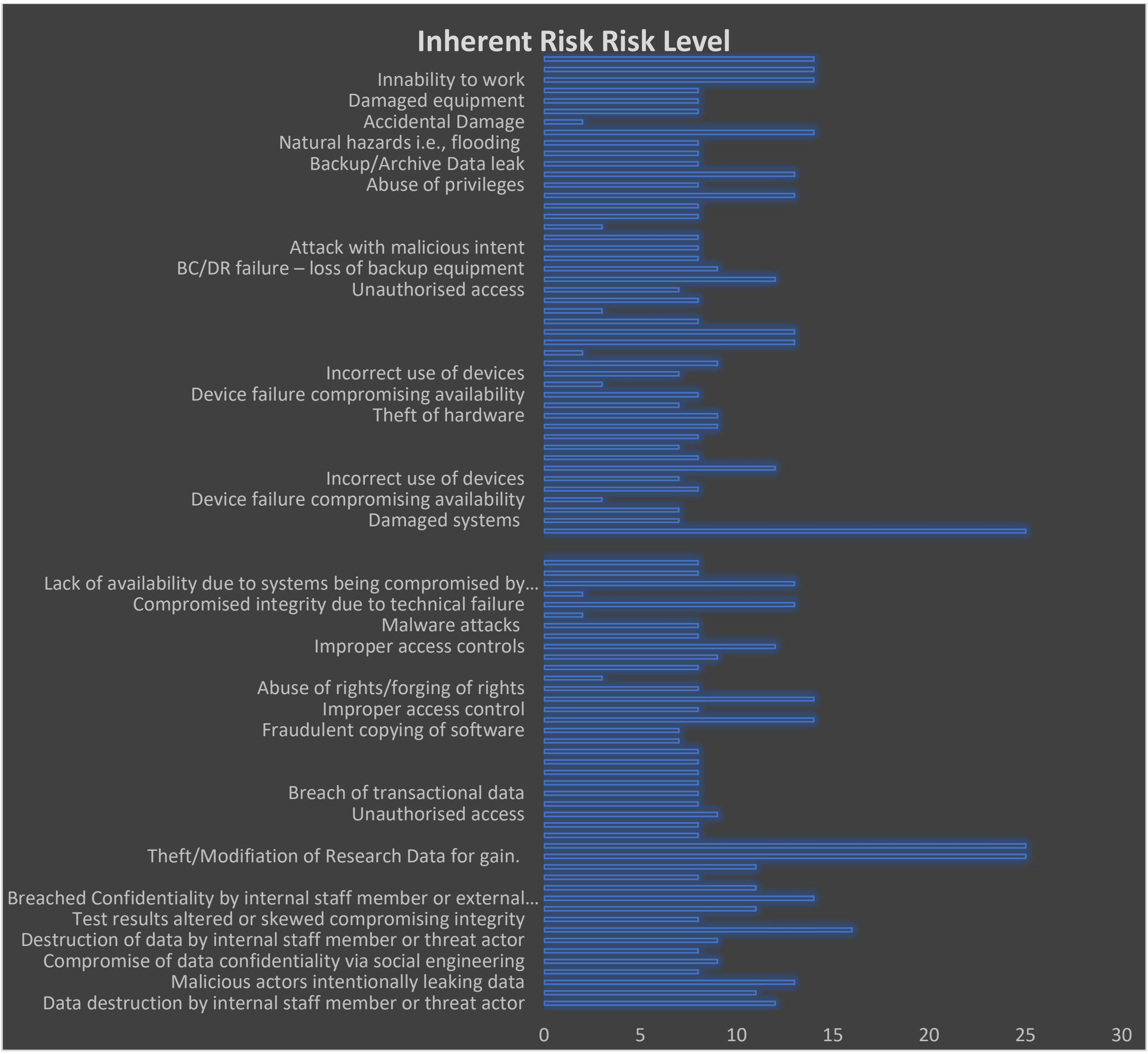


Figure 2 - Inherent risk level post control implementation (significantly reduced)

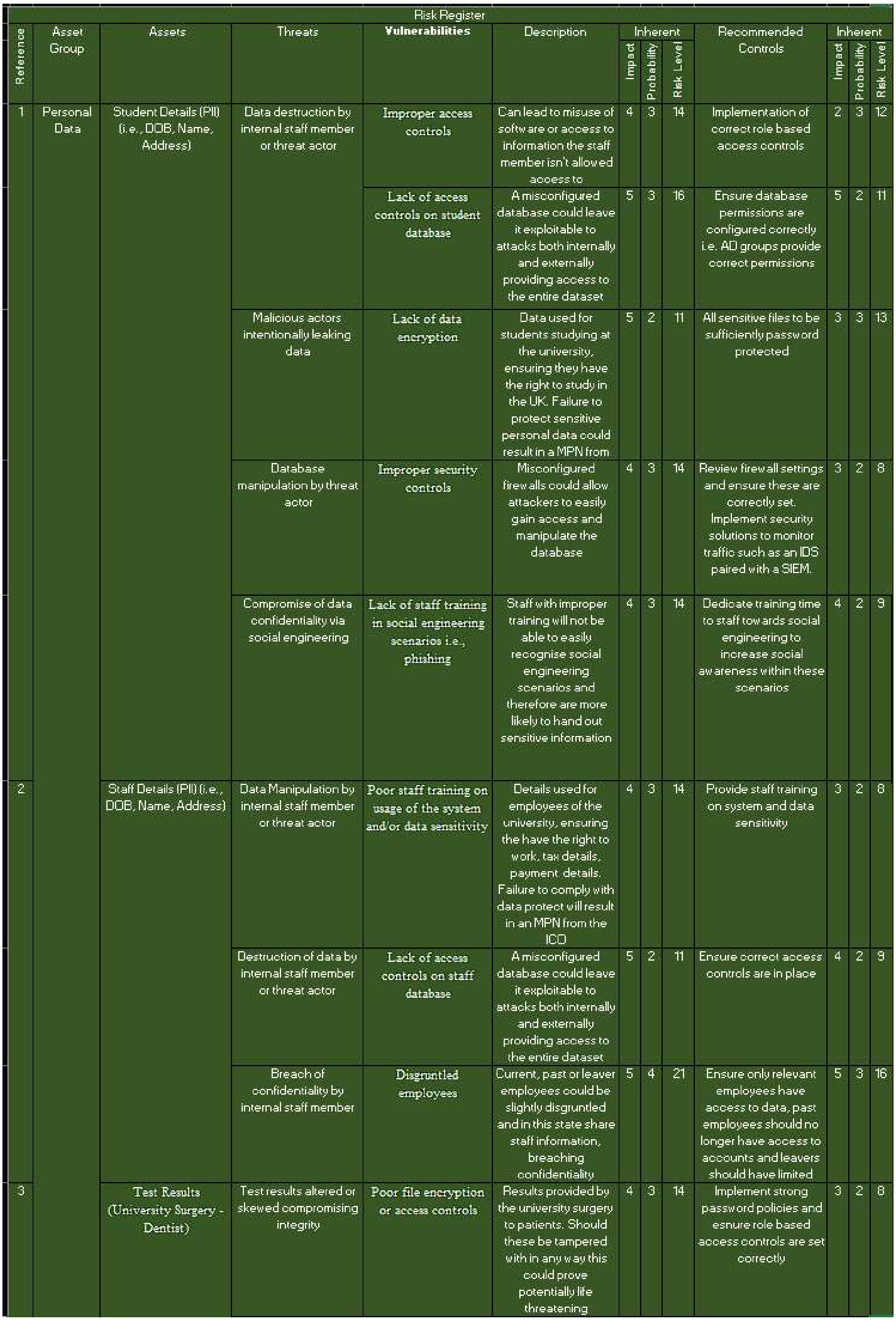
Recommendations

The main controls which would have the most success and be effective in preventing threats within the university are the combination of multifactor authentication and frequent organisational updates. MFA provides an extra layer of security to systems throughout the estate which preventing attacks and ensuring the user who is accessing the account or service is the user who should have access.

Secondly the frequent updates reduce system and network vulnerabilities significantly lowering the routes a threat actor can take to exploit and gain access to confidential information, implementing a schedule to carry out these updates will further enforce this.

Lastly the combination of both MFA and regular updates significantly reduces the probability of many risks found throughout the risk register, making it drastically more arduous to not only gain access to the network and its systems, but access PII/sensitive documentation and modify, destroy or exfiltrate.

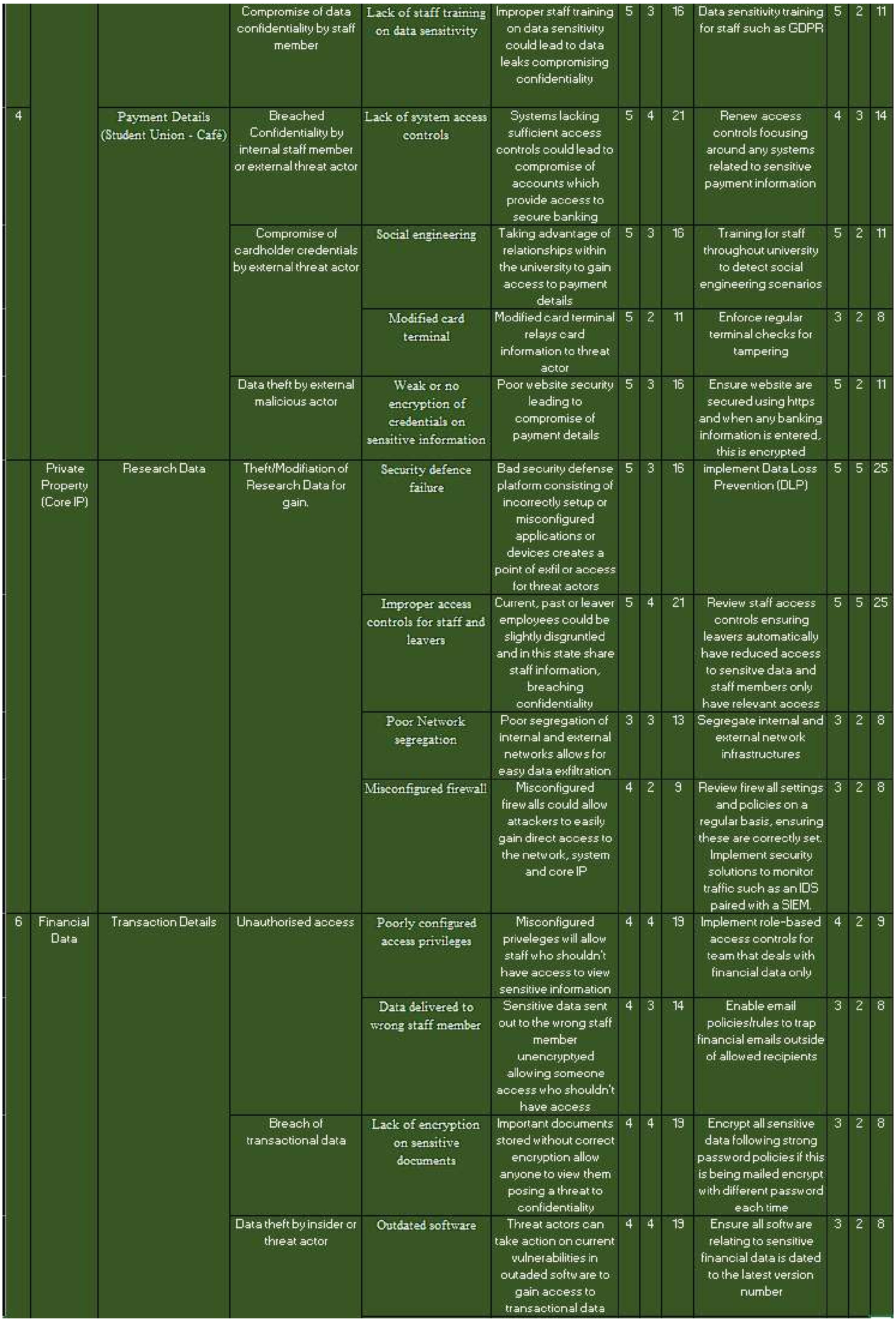
Appendices



Risk Register

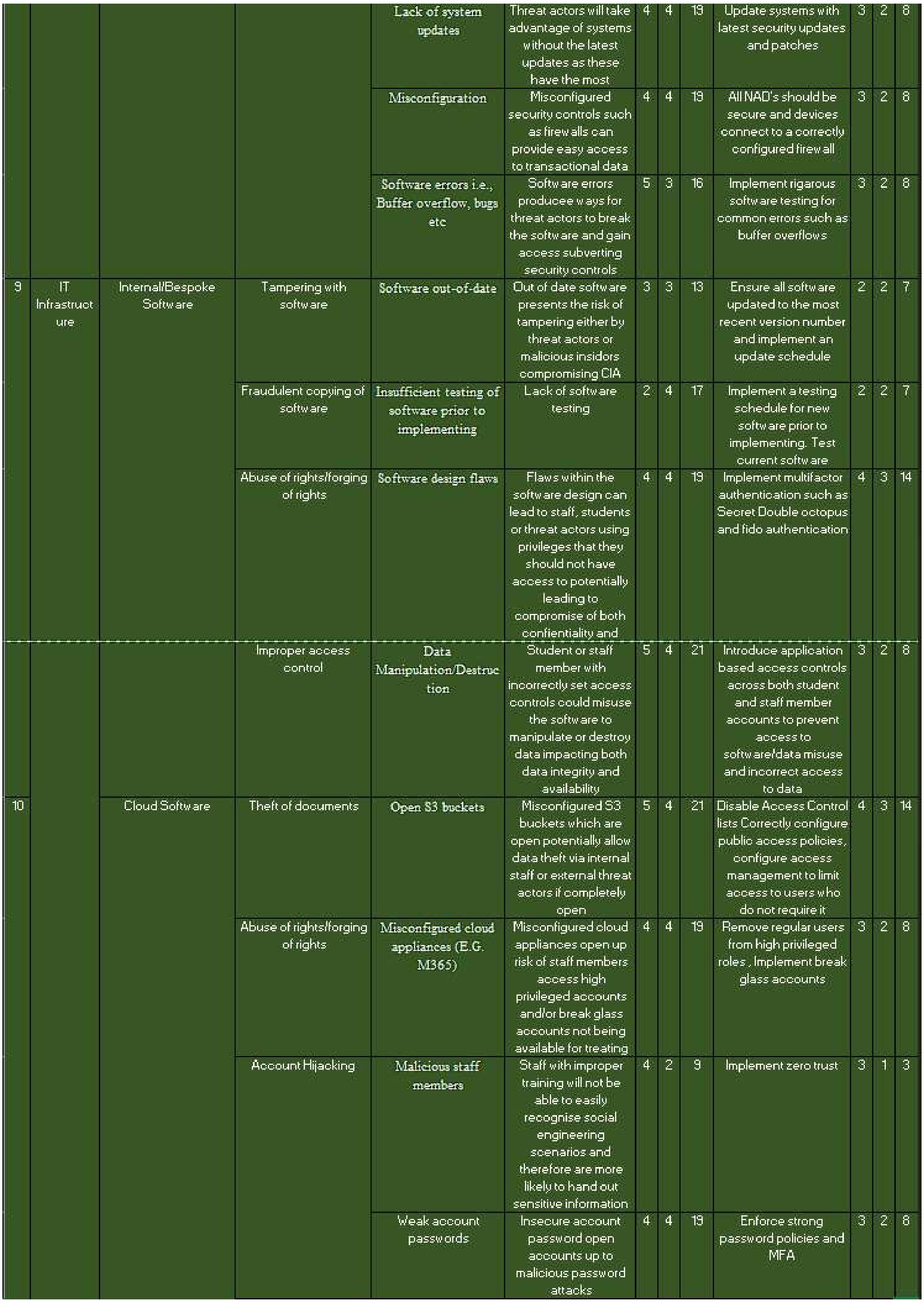
Reference	Asset Group	Assets	Threats	**Vulnerabilities**	Description	Inherent			Recommended Controls	Inherent		
						Impact	Probability	Risk Level		Impact	Probability	Risk Level
1	Personal Data	Student Details (PII) (i.e., DOB, Name, Address)	Data destruction by internal staff member or threat actor	Improper access controls	Can lead to misuse of software or access to information the staff member isn't allowed access to	4	3	14	Implementation of correct role based access controls	2	3	12
				Lack of access controls on student database	A misconfigured database could leave it exploitable to attacks both internally and externally providing access to the entire dataset	5	3	16	Ensure database permissions are configured correctly i.e. AD groups provide correct permissions	5	2	11
			Malicious actors intentionally leaking data	Lack of data encryption	Data used for students studying at the university, ensuring they have the right to study in the UK. Failure to protect sensitive personal data could result in a MPN from	5	2	11	All sensitive files to be sufficiently password protected	3	3	13
			Database manipulation by threat actor	Improper security controls	Misconfigured firewalls could allow attackers to easily gain access and manipulate the database	4	3	14	Review firewall settings and ensure these are correctly set. Implement security solutions to monitor traffic such as an IDS paired with a SIEM.	3	2	8
			Compromise of data confidentiality via social engineering	Lack of staff training in social engineering scenarios i.e., phishing	Staff with improper training will not be able to easily recognise social engineering scenarios and therefore are more likely to hand out sensitive information	4	3	14	Dedicate training time to staff towards social engineering to increase social awareness within these scenarios	4	2	9
2		Staff Details (PII) (i.e., DOB, Name, Address)	Data Manipulation by internal staff member or threat actor	Poor staff training on usage of the system and/or data sensitivity	Details used for employees of the university, ensuring the have the right to work, tax details, payment details. Failure to comply with data protect will result in an MPN from the ICO	4	3	14	Provide staff training on system and data sensitivity	3	2	8
			Destruction of data by internal staff member or threat actor	Lack of access controls on staff database	A misconfigured database could leave it exploitable to attacks both internally and externally providing access to the entire dataset	5	2	11	Ensure correct access controls are in place	4	2	9
			Breach of confidentiality by internal staff member	Disgruntled employees	Current, past or leaver employees could be slightly disgruntled and in this state share staff information, breaching confidentiality	5	4	21	Ensure only relevant employees have access to data, past employees should no longer have access to accounts and leavers should have limited	5	3	16
3		Test Results (University Surgery - Dentist)	Test results altered or skewed compromising integrity	Poor file encryption or access controls	Results provided by the university surgery to patients. Should these be tampered with in any way this could prove potentially life threatening	4	3	14	Implement strong password policies and esnure role based access controls are set correctly	3	2	8

Figure 3 - Risk Register



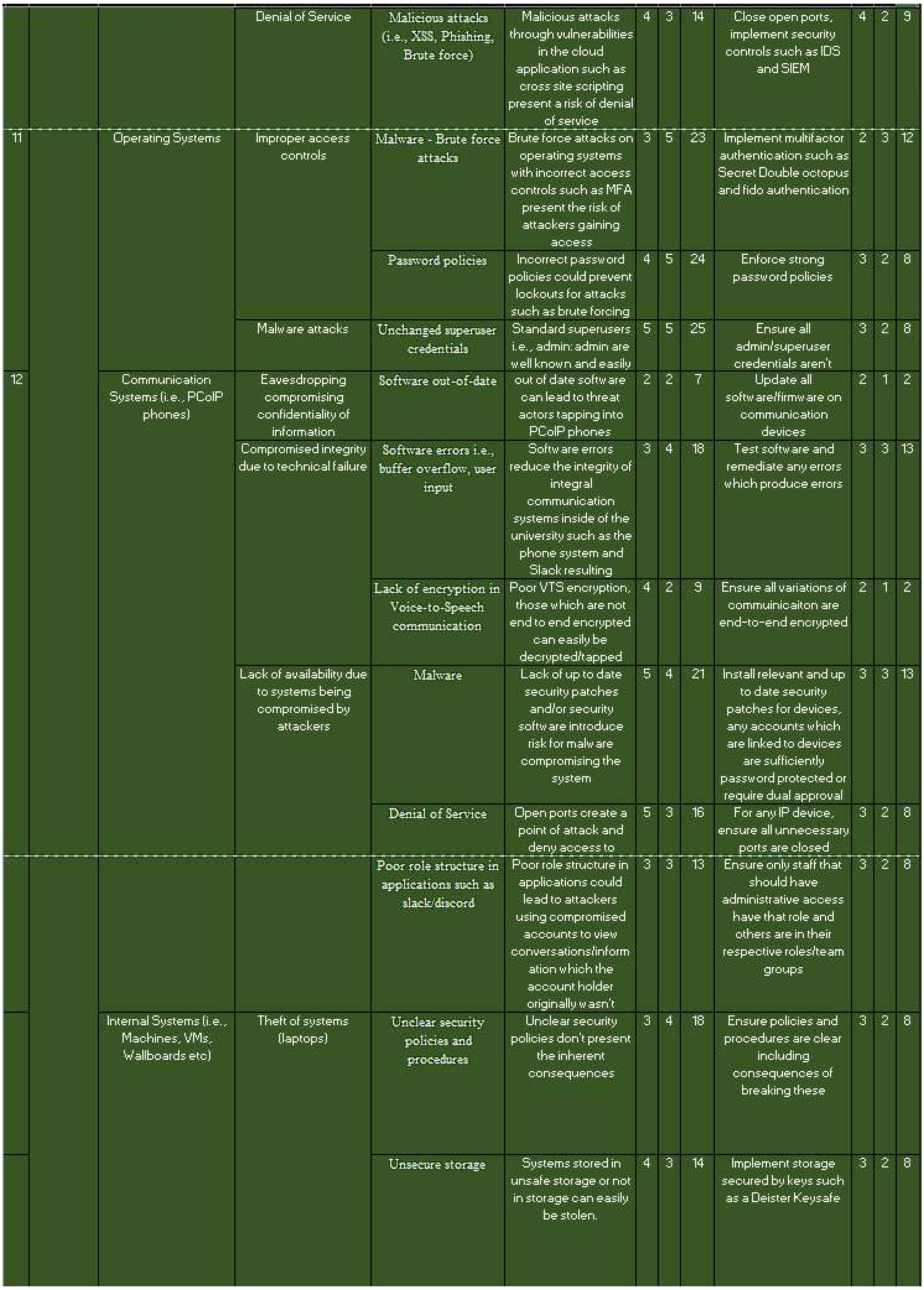
			Compromise of data confidentiality by staff member	Lack of staff training on data sensitivity	Improper staff training on data sensitivity could lead to data leaks compromising confidentiality	5	3	16	Data sensitivity training for staff such as GDPR	5	2	11
4		Payment Details (Student Union - Café)	Breached Confidentiality by internal staff member or external threat actor	Lack of system access controls	Systems lacking sufficient access controls could lead to compromise of accounts which provide access to secure banking	5	4	21	Renew access controls focusing around any systems related to sensitive payment information	4	3	14
			Compromise of cardholder credentials by external threat actor	Social engineering	Taking advantage of relationships within the university to gain access to payment details	5	3	16	Training for staff throughout university to detect social engineering scenarios	5	2	11
				Modified card terminal	Modified card terminal relays card information to threat actor	5	2	11	Enforce regular terminal checks for tampering	3	2	8
			Data theft by external malicious actor	Weak or no encryption of credentials on sensitive information	Poor website security leading to compromise of payment details	5	3	16	Ensure website are secured using https and when any banking information is entered, this is encrypted	5	2	11
	Private Property (Core IP)	Research Data	Theft/Modification of Research Data for gain.	Security defence failure	Bad security defense platform consisting of incorrectly setup or misconfigured applications or devices creates a point of exfil or access for threat actors	5	3	16	implement Data Loss Prevention (DLP)	5	5	25
				Improper access controls for staff and leavers	Current, past or leaver employees could be slightly disgruntled and in this state share staff information, breaching confidentiality	5	4	21	Review staff access controls ensuring leavers automatically have reduced access to sensitve data and staff members only have relevant access	5	5	25
				Poor Network segregation	Poor segregation of internal and external networks allows for easy data exfiltration	3	3	13	Segregate internal and external network infrastructures	3	2	8
				Misconfigured firewall	Misconfigured firewalls could allow attackers to easily gain direct access to the network, system and core IP	4	2	9	Review firewall settings and policies on a regular basis, ensuring these are correctly set. Implement security solutions to monitor traffic such as an IDS paired with a SIEM.	3	2	8
6	Financial Data	Transaction Details	Unauthorised access	Poorly configured access privileges	Misconfigured priveleges will allow staff who shouldn't have access to view sensitive information	4	4	19	Implement role-based access controls for team that deals with financial data only	4	2	9
				Data delivered to wrong staff member	Sensitive data sent out to the wrong staff member unencryptyed allowing someone access who shouldn't have access	4	3	14	Enable email policies/rules to trap financial emails outside of allowed recipients	3	2	8
			Breach of transactional data	Lack of encryption on sensitive documents	Important documents stored without correct encryption allow anyone to view them posing a threat to confidentiality	4	4	19	Encrypt all sensitive data following strong password policies if this is being mailed encrypt with different password each time	3	2	8
			Data theft by insider or threat actor	Outdated software	Threat actors can take action on current vulnerabilities in outaded software to gain access to transactional data	4	4	19	Ensure all software relating to sensitive financial data is dated to the latest version number	3	2	8

Figure 4 - Risk Register



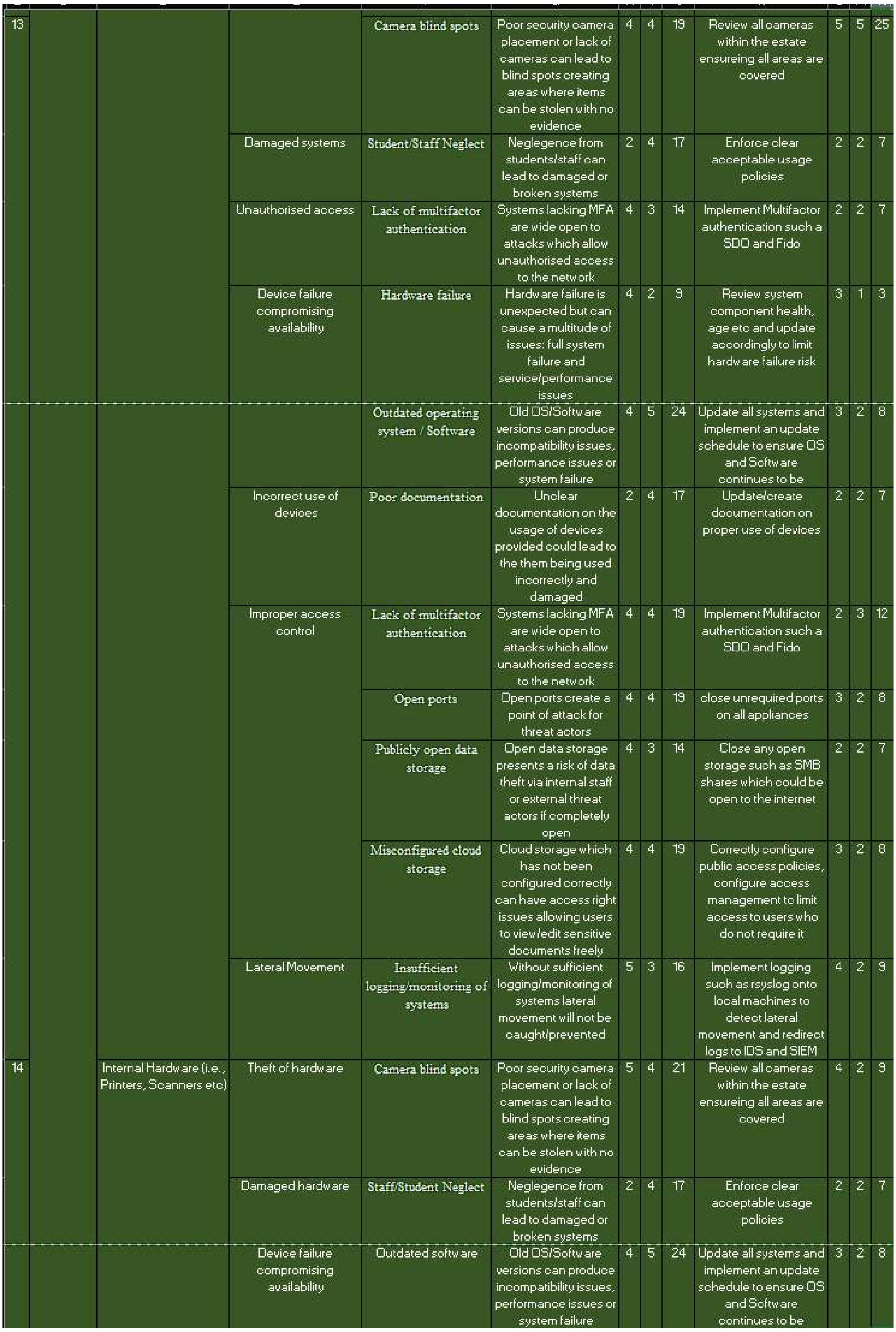
				Lack of system updates	Threat actors will take advantage of systems without the latest updates as these have the most	4	4	19	Update systems with latest security updates and patches	3	2	8
				Misconfiguration	Misconfigured security controls such as firewalls can provide easy access to transactional data	4	4	19	All NAD's should be secure and devices connect to a correctly configured firewall	3	2	8
				Software errors i.e., Buffer overflow, bugs etc	Software errors producee ways for threat actors to break the software and gain access subverting security controls	5	3	16	Implement rigarous software testing for common errors such as buffer overflows	3	2	8
9	IT Infrastructure	Internal/Bespoke Software	Tampering with software	Software out-of-date	Out of date software presents the risk of tampering either by threat actors or malicious insidors compromising CIA	3	3	13	Ensure all software updated to the most recent version number and implement an update schedule	2	2	7
			Fraudulent copying of software	Insufficient testing of software prior to implementing	Lack of software testing	2	4	17	Implement a testing schedule for new software prior to implementing. Test current software	2	2	7
			Abuse of rights/forging of rights	Software design flaws	Flaws within the software design can lead to staff, students or threat actors using privileges that they should not have access to potentially leading to compromise of both confientiality and	4	4	19	Implement multifactor authentication such as Secret Double octopus and fido authentication	4	3	14
			Improper access control	Data Manipulation/Destruction	Student or staff member with incorrectly set access controls could misuse the software to manipulate or destroy data impacting both data integrity and availability	5	4	21	Introduce application based access controls across both student and staff member accounts to prevent access to software/data misuse and incorrect access to data	3	2	8
10		Cloud Software	Theft of documents	Open S3 buckets	Misconfigured S3 buckets which are open potentially allow data theft via internal staff or external threat actors if completely open	5	4	21	Disable Access Control lists Correctly configure public access policies, configure access management to limit access to users who do not require it	4	3	14
			Abuse of rights/forging of rights	Misconfigured cloud appliances (E.G. M365)	Misconfigured cloud appliances open up risk of staff members access high privileged accounts and/or break glass accounts not being available for treating	4	4	19	Remove regular users from high privileged roles , Implement break glass accounts	3	2	8
			Account Hijacking	Malicious staff members	Staff with improper training will not be able to easily recognise social engineering scenarios and therefore are more likely to hand out sensitive information	4	2	9	Implement zero trust	3	1	3
				Weak account passwords	Insecure account password open accounts up to malicious password attacks	4	4	19	Enforce strong password policies and MFA	3	2	8

Figure 5 - Risk Register



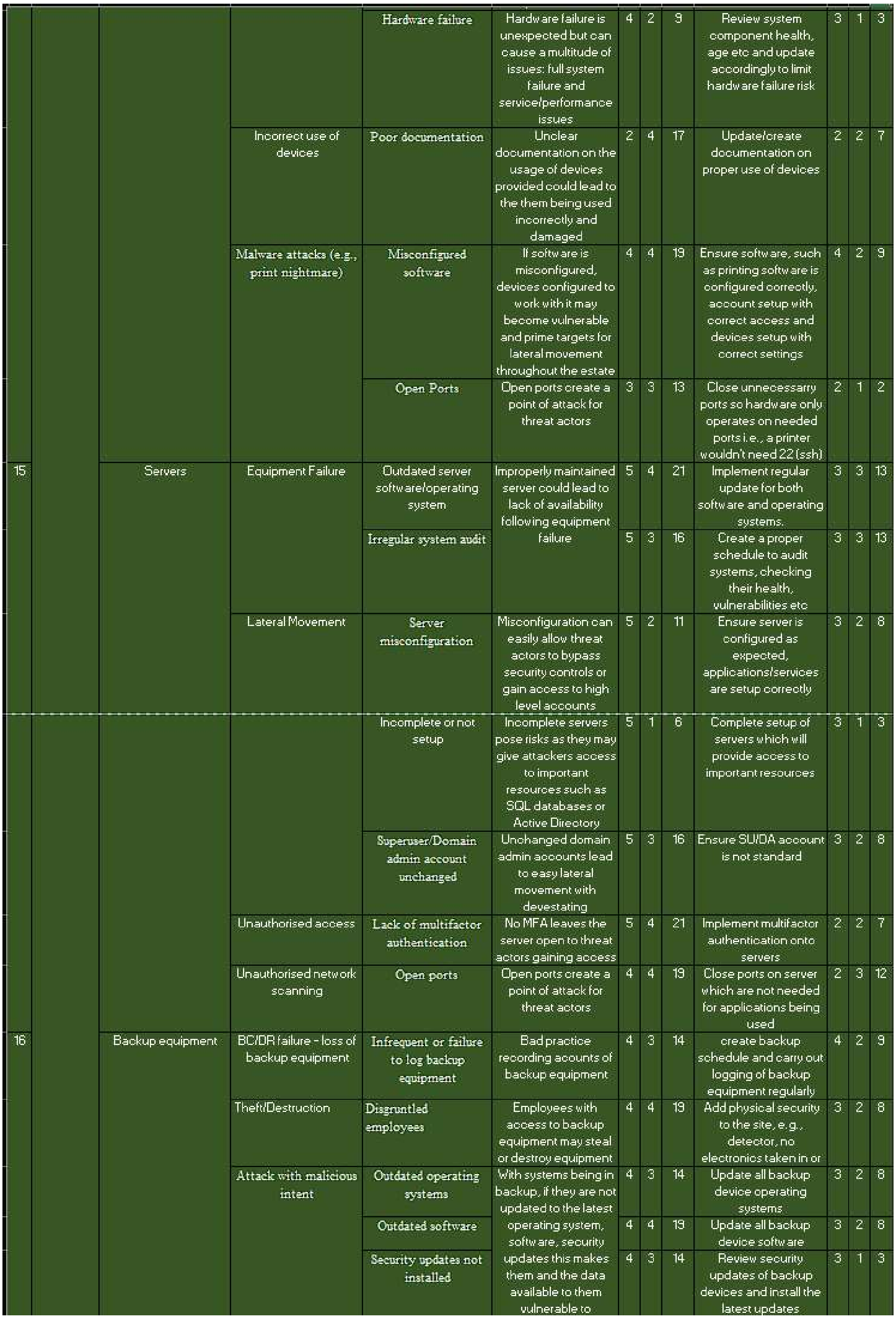
			Denial of Service	Malicious attacks (i.e., XSS, Phishing, Brute force)	Malicious attacks through vulnerabilities in the cloud application such as cross site scripting present a risk of denial of service	4	3	14	Close open ports, implement security controls such as IDS and SIEM	4	2	9
11		Operating Systems	Improper access controls	Malware - Brute force attacks	Brute force attacks on operating systems with incorrect access controls such as MFA present the risk of attackers gaining access	3	5	23	Implement multifactor authentication such as Secret Double octopus and fido authentication	2	3	12
				Password policies	Incorrect password policies could prevent lockouts for attacks such as brute forcing	4	5	24	Enforce strong password policies	3	2	8
			Malware attacks	Unchanged superuser credentials	Standard superusers i.e., admin:admin are well known and easily	5	5	25	Ensure all admin/superuser credentials aren't	3	2	8
12		Communication Systems (i.e., PCoIP phones)	Eavesdropping compromising confidentiality of information	Software out-of-date	out of date software can lead to threat actors tapping into PCoIP phones	2	2	7	Update all software/firmware on communication devices	2	1	2
			Compromised integrity due to technical failure	Software errors i.e., buffer overflow, user input	Software errors reduce the integrity of integral communication systems inside of the university such as the phone system and Slack resulting	3	4	18	Test software and remediate any errors which produce errors	3	3	13
				Lack of encryption in Voice-to-Speech communication	Poor VTS encryption, those which are not end to end encrypted can easily be decrypted/tapped	4	2	9	Ensure all variations of commuinicaiton are end-to-end encrypted	2	1	2
			Lack of availability due to systems being compromised by attackers	Malware	Lack of up to date security patches and/or security software introduce risk for malware compromising the system	5	4	21	Install relevant and up to date security patches for devices, any accounts which are linked to devices are sufficiently password protected or require dual approval	3	3	13
				Denial of Service	Open ports create a point of attack and deny access to	5	3	16	For any IP device, ensure all unnecessary ports are closed	3	2	8
				Poor role structure in applications such as slack/discord	Poor role structure in applications could lead to attackers using compromised accounts to view conversations/information which the account holder originally wasn't	3	3	13	Ensure only staff that should have administrative access have that role and others are in their respective roles/team groups	3	2	8
		Internal Systems (i.e., Machines, VMs, Wallboards etc)	Theft of systems (laptops)	Unclear security policies and procedures	Unclear security policies don't present the inherent consequences	3	4	18	Ensure policies and procedures are clear including consequences of breaking these	3	2	8
				Unsecure storage	Systems stored in unsafe storage or not in storage can easily be stolen.	4	3	14	Implement storage secured by keys such as a Deister Keysafe	3	2	8

Figure 6 - Risk Register



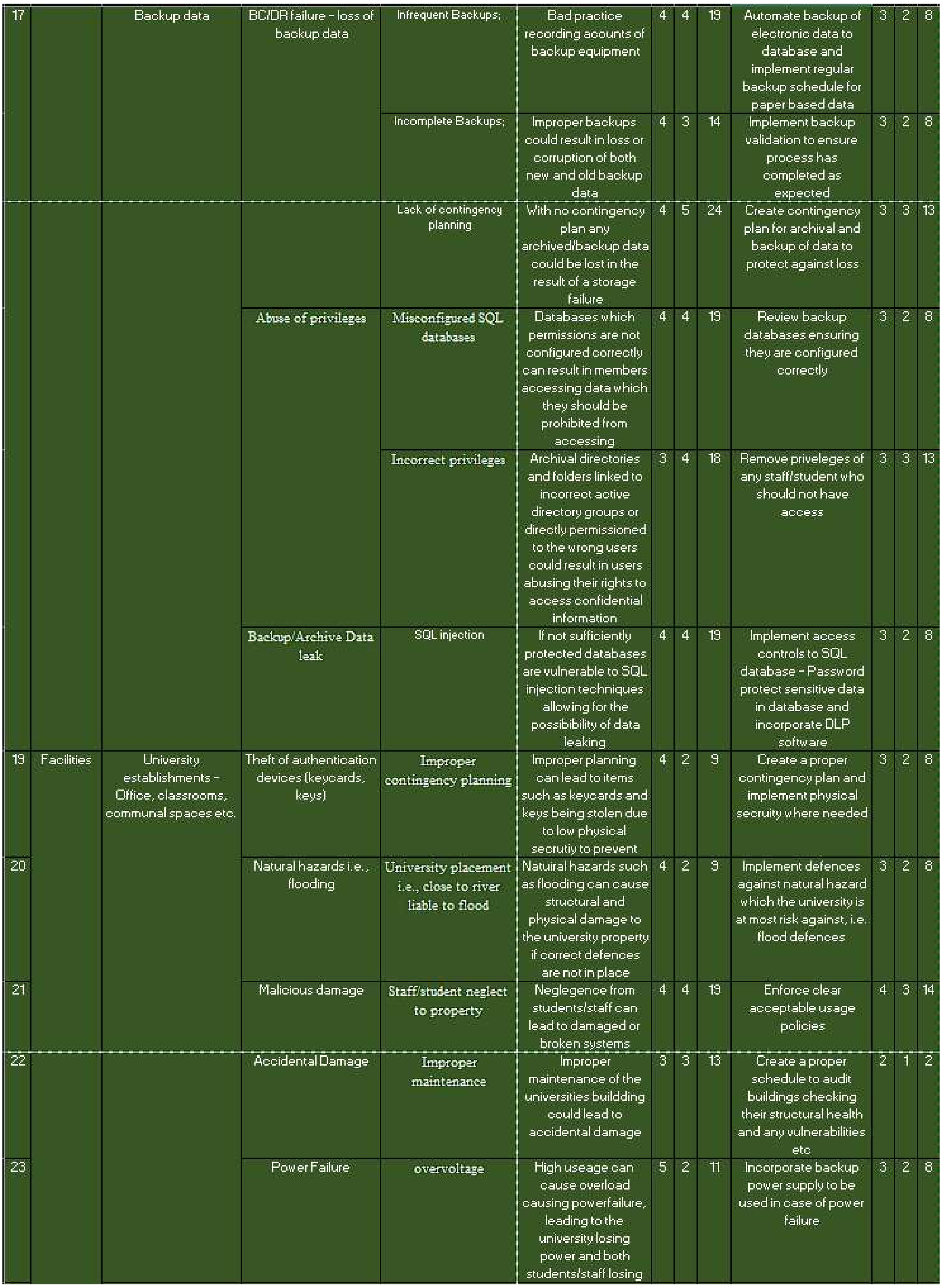
13				Camera blind spots	Poor security camera placement or lack of cameras can lead to blind spots creating areas where items can be stolen with no evidence	4	4	19	Review all cameras within the estate ensureing all areas are covered	5	5	25
			Damaged systems	Student/Staff Neglect	Neglegence from students/staff can lead to damaged or broken systems	2	4	17	Enforce clear acceptable usage policies	2	2	7
			Unauthorised access	Lack of multifactor authentication	Systems lacking MFA are wide open to attacks which allow unauthorised access to the network	4	3	14	Implement Multifactor authentication such a SDO and Fido	2	2	7
			Device failure compromising availability	Hardware failure	Hardware failure is unexpected but can cause a multitude of issues: full system failure and service/performance issues	4	2	9	Review system component health, age etc and update accordingly to limit hardware failure risk	3	1	3
				Outdated operating system / Software	Old OS/Software versions can produce incompatibility issues, performance issues or system failure	4	5	24	Update all systems and implement an update schedule to ensure OS and Software continues to be	3	2	8
			Incorrect use of devices	Poor documentation	Unclear documentation on the usage of devices provided could lead to the them being used incorrectly and damaged	2	4	17	Update/create documentation on proper use of devices	2	2	7
			Improper access control	Lack of multifactor authentication	Systems lacking MFA are wide open to attacks which allow unauthorised access to the network	4	4	19	Implement Multifactor authentication such a SDO and Fido	2	3	12
				Open ports	Open ports create a point of attack for threat actors	4	4	19	close unrequired ports on all appliances	3	2	8
				Publicly open data storage	Open data storage presents a risk of data theft via internal staff or external threat actors if completely open	4	3	14	Close any open storage such as SMB shares which could be open to the internet	2	2	7
				Misconfigured cloud storage	Cloud storage which has not been configured correctly can have access right issues allowing users to view/edit sensitive documents freely	4	4	19	Correctly configure public access policies, configure access management to limit access to users who do not require it	3	2	8
			Lateral Movement	Insufficient logging/monitoring of systems	Without sufficient logging/monitoring of systems lateral movement will not be caught/prevented	5	3	16	Implement logging such as rsyslog onto local machines to detect lateral movement and redirect logs to IDS and SIEM	4	2	9
14		Internal Hardware (i.e., Printers, Scanners etc)	Theft of hardware	Camera blind spots	Poor security camera placement or lack of cameras can lead to blind spots creating areas where items can be stolen with no evidence	5	4	21	Review all cameras within the estate ensureing all areas are covered	4	2	9
			Damaged hardware	Staff/Student Neglect	Neglegence from students/staff can lead to damaged or broken systems	2	4	17	Enforce clear acceptable usage policies	2	2	7
			Device failure compromising availability	Outdated software	Old OS/Software versions can produce incompatibility issues, performance issues or system failure	4	5	24	Update all systems and implement an update schedule to ensure OS and Software continues to be	3	2	8

Figure 7 - Risk Register



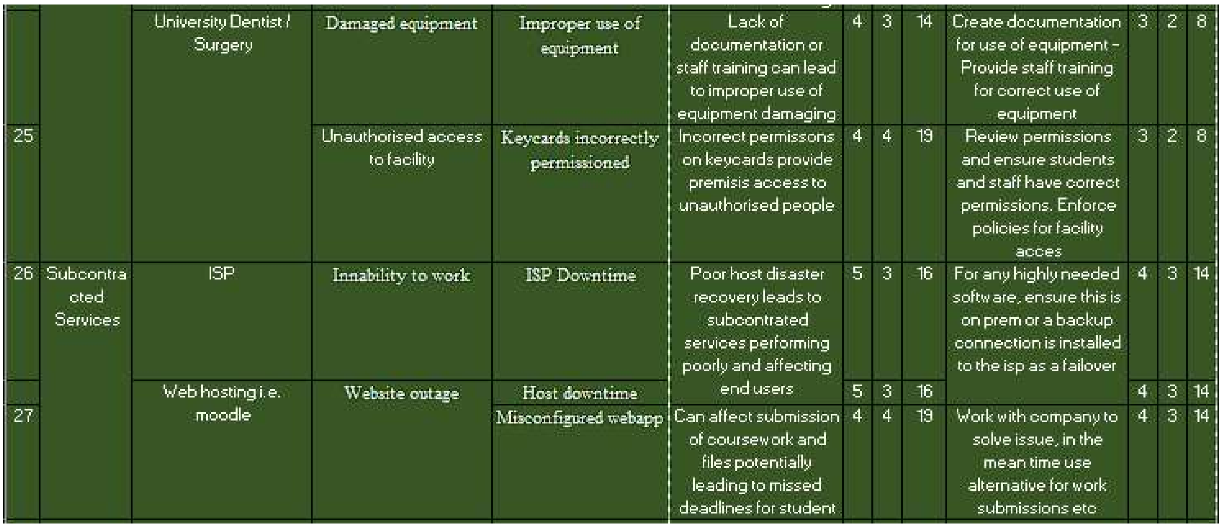
				Hardware failure	Hardware failure is unexpected but can cause a multitude of issues: full system failure and service/performance issues	4	2	9	Review system component health, age etc and update accordingly to limit hardware failure risk	3	1	3
			Incorrect use of devices	Poor documentation	Unclear documentation on the usage of devices provided could lead to the them being used incorrectly and damaged	2	4	17	Update/create documentation on proper use of devices	2	2	7
			Malware attacks (e.g., print nightmare)	Misconfigured software	If software are is misconfigured, devices configured to work with it may become vulnerable and prime targets for lateral movement throughout the estate	4	4	19	Ensure software, such as printing software is configured correctly, account setup with correct access and devices setup with correct settings	4	2	9
				Open Ports	Open ports create a point of attack for threat actors	3	3	13	Close unnecessarry ports so hardware only operates on needed ports i.e., a printer wouldn't need 22 (ssh)	2	1	2
15		Servers	Equipment Failure	Outdated server software/operating system	Improperly maintained server could lead to lack of availability following equipment failure	5	4	21	Implement regular update for both software and operating systems.	3	3	13
				Irregular system audit		5	3	16	Create a proper schedule to audit systems, checking their health, vulnerabilities etc	3	3	13
			Lateral Movement	Server misconfiguration	Misconfiguration can easily allow threat actors to bypass security controls or gain access to high level accounts	5	2	11	Ensure server is configured as expected, applications/services are setup correctly	3	2	8
				Incomplete or not setup	Incomplete servers pose risks as they may give attackers access to important resources such as SQL databases or Active Directory	5	1	6	Complete setup of servers which will provide access to important resources	3	1	3
				Superuser/Domain admin account unchanged	Unchanged domain admin accounts lead to easy lateral movement with devestating	5	3	16	Ensure SU/DA account is not standard	3	2	8
			Unauthorised access	Lack of multifactor authentication	No MFA leaves the server open to threat actors gaining access	5	4	21	Implement multifactor authentication onto servers	2	2	7
			Unauthorised network scanning	Open ports	Open ports create a point of attack for threat actors	4	4	19	Close ports on server which are not needed for applications being used	2	3	12
16		Backup equipment	BC/DR failure - loss of backup equipment	Infrequent or failure to log backup equipment	Bad practice recording acounts of backup equipment	4	3	14	create backup schedule and carry out logging of backup equipment regularly	4	2	9
			Theft/Destruction	Disgruntled employees	Employees with access to backup equipment may steal or destroy equipment	4	4	19	Add physical security to the site, e.g., detector, no electronics taken in or	3	2	8
			Attack with malicious intent	Outdated operating systems	With systems being in backup, if they are not updated to the latest operating system, software, security updates this makes them and the data available to them vulnerable to	4	3	14	Update all backup device operating systems	3	2	8
				Outdated software		4	4	19	Update all backup device software	3	2	8
				Security updates not installed		4	3	14	Review security updates of backup devices and install the latest updates	3	1	3

Figure 8 - Risk Register



17		Backup data	BC/DR failure - loss of backup data	Infrequent Backups;	Bad practice recording acounts of backup equipment	4	4	19	Automate backup of electronic data to database and implement regular backup schedule for paper based data	3	2	8
				Incomplete Backups;	Improper backups could result in loss or corruption of both new and old backup data	4	3	14	Implement backup validation to ensure process has completed as expected	3	2	8
				Lack of contingency planning	With no contingency plan any archived/backup data could be lost in the result of a storage failure	4	5	24	Create contingency plan for archival and backup of data to protect against loss	3	3	13
			Abuse of privileges	Misconfigured SQL databases	Databases which permissions are not configured correctly can result in members accessing data which they should be prohibited from accessing	4	4	19	Review backup databases ensuring they are configured correctly	3	2	8
				Incorrect privileges	Archival directories and folders linked to incorrect active directory groups or directly permissioned to the wrong users could result in users abusing their rights to access confidential information	3	4	18	Remove priveleges of any staff/student who should not have access	3	3	13
			Backup/Archive Data leak	SQL injection	If not sufficiently protected databases are vulnerable to SQL injection techniques allowing for the possibility of data leaking	4	4	19	Implement access controls to SQL database - Password protect sensitive data in database and incorporate DLP software	3	2	8
19	Facilities	University establishments - Office, classrooms, communal spaces etc.	Theft of authentication devices (keycards, keys)	Improper contingency planning	Improper planning can lead to items such as keycards and keys being stolen due to low physical secrutiy to prevent	4	2	9	Create a proper contingency plan and implement physical secruity where needed	3	2	8
20			Natural hazards i.e., flooding	University placement i.e., close to river liable to flood	Natuiral hazards such as flooding can cause structural and physical damage to the university property if correct defences are not in place	4	2	9	Implement defences against natural hazard which the university is at most risk against, i.e. flood defences	3	2	8
21			Malicious damage	Staff/student neglect to property	Neglegence from students/staff can lead to damaged or broken systems	4	4	19	Enforce clear acceptable usage policies	4	3	14
22			Accidental Damage	Improper maintenance	Improper maintenance of the universities buildding could lead to accidental damage	3	3	13	Create a proper schedule to audit buildings checking their structural health and any vulnerabilities etc	2	1	2
23			Power Failure	overvoltage	High useage can cause overload causing powerfailure, leading to the university losing power and both students/staff losing	5	2	11	Incorporate backup power supply to be used in case of power failure	3	2	8

Figure 9 - Risk Register



		University Dentist / Surgery	Damaged equipment	Improper use of equipment	Lack of documentation or staff training can lead to improper use of equipment damaging	4	3	14	Create documentation for use of equipment - Provide staff training for correct use of equipment	3	2	8
25			Unauthorised access to facility	Keycards incorrectly permissioned	Incorrect permissons on keycards provide premisis access to unauthorised people	4	4	19	Review permissions and ensure students and staff have correct permissions. Enforce policies for facility acces	3	2	8
26	Subcontracted Services	ISP	Innability to work	ISP Downtime	Poor host disaster recovery leads to subcontrated services performing poorly and affecting end users	5	3	16	For any highly needed software, ensure this is on prem or a backup connection is installed to the isp as a failover	4	3	14
		Web hosting i.e. moodle	Website outage	Host downtime		5	3	16		4	3	14
27				Misconfigured webapp	Can affect submission of coursework and files potentially leading to missed deadlines for student	4	4	19	Work with company to solve issue, in the mean time use alternative for work submissions etc	4	3	14

Figure 10 - Risk Register

Figures

Tables