Enterprise Cyber Security Assessed Course Work

Cyber Security Concerns of Employees Using Their Own Personal Cloud

Written by Group X:

Saige Liu
Zhengyang Bi
Runqi Wang
Richard Quartey
Stuart Armit

An investigation into the use of personal clouds by employees in the Mostel & Wilder firm, its impacts on the cybersecurity of the financial company, the varied risks involved, policies that could help mitigate the risks and metrics to monitor the effectiveness of these policies after they have been implemented.

1. Risk Identifications

1.1 Risk1 - breaching data protection and personal data transmission regulation.

When employees use their personal cloud to store and save customer and enterprise's documents, the security of data storage and personal information is paramount. Since Mostel & Wilder (Referred as M&W) have headquartered within the European Union, they are subject to data and privacy protection regulations known as the Guide to the General Data Protection Regulation (Referred as GDPR). GDPR is set to be the default infrastructure of the company's business process [1]. All the company's policies and actions should be following the data storage and transmission rules in GDPR, otherwise, the company will be liable for compensation with fines up to €20 million [2, 3], or 4% of the firms' annual revenue. Therefore, it is an unacceptable risk for the company to breach GDPR [4].

1.2 Risk 2 - data movement and transmission between different countries/regions.

There are different data storing and transmission jurisdictions for data holders to abide by in different countries [5]. As such there are geographical limitations in these jurisdictions. The concern for M&W is that cloud data could move from one server to another. As the servers' locations are not disclosed to the public, during the process of transmission and processing, data could travel through various countries. Resulting in the user unknowingly breaching data protection laws. This is a critical and concealed risk in personal cloud storages.

1.3 Risk 3 - Freedom of information and other such legal requests

Freedom of information (FOI) is a law to ensure the public have the right to request information from government, public officials or an enterprise. The new Freedom of Information Act 2014 (UK) ensures individuals have the right to access information held by "a body to which FOI legislation applies" [6]. If the enterprise is using personal clouds to store sensitive financial or personal data, it will be very hard for the public to get information that they need to know. Especially as different countries and regions have different policies to ensure people have freedom of information rights [7].

In some situation, there will be some conflict between data protection principles in Article 5(1) of GDPR and FOI requests. For example, if there's an FOI request for public information stored by an employee on their personal cloud, disclosing this data could contravene the data protection principles in Article 5(1) of the General Data Protection Regulations. However, not releasing the public data to the person may violate the right of FOI. It is complex for the M&W to find a balance between these two rules [8].

1.4 Risk 4 - Collusion concerns between providers and competing firms, state or parties involved in on-going cases.

Collusion using a personal cloud is a major concern for M&W since lots of client's sensitive financial data can be stolen. Research has proven that the financial industry is prone to cyber-attacks. In 2016 the financial industry suffered an alarming rate of 65% more cyber-attacks than any other industry [9]. The financial industry also records the second highest cost of client loss as a result of data breach, with the highest being the health sector [10]. Although collusion issues may happen in every enterprise, the use of personal clouds provides an easier way. Employees' behaviors become harder to audit while they store sensitive data and files in their personal clouds, since the accessibility of the accounts are controlled by themselves. They may sell their private key to the competing firms so that all the source stored in the personal cloud or shared in the group can be stolen. In this case, it is also very hard to find out the data leakage and even harder to address the informer.

The use of distributed storage systems is also associated with the risk of cloud collusion, in which the cloud provider colludes with competing firms through unfaithful employees. If the colluder can identify the personal cloud account, they may easily get access to the confidential data in the storage systems with the help of provider staffs. For instance, shared groups on the personal cloud can be used to address where the data is, colluder staff can then download it through these infrastructures.

1.5 Risk 5 - Extensibility and accessibility of applications, access of authorized and unauthorized entities gaining access to tools and gaining insight into business processes.

Using a cloud-based system to increase portability and accessibility of data although efficient is not without issues. Information integrity can become problematic when removed from a company's authority; key data is no longer under their complete control and key decisions no longer the enterprises to make. Key concerns raised regarding access and potential manipulation by authorized or unauthorized parties are not without merit, with a plethora of examples of both user and service issues noted in recent years. (Most notably Cambridge Analytica, Facebook and Marriott Starwood Hotels breaches [11]. Also, in the Verizon Data Breach Investigations report it was captured that the use of malwares was relatively high when it came to the mode of attacks used by adversaries [10].

User issues:

- Ransomware
- Compromised credentials via phishing and malware
- Poor security practices
- Sharing links to personal cloud files or accidental public uploads of data

Provider Issues:

- Man, in the cloud attack (The bypass of server unique sync token avoiding the need for a username and password)
- Distributed Denial-of-Service attacks
- Phishing and malware threats
- Inconsistent use of encryption data storage and recoverability

- Credential management authentication process and key management
- System outages
- Deduplication
- Data leakage

1.6 Risk 6 - Personal hardware, improper disposal, loss and permission leakages

Computers and other hardware (such as smartphones and tablets) have become ubiquitous in the modern era, with cloud storage allowing easy access across multiple devices. Work can therefore be carried out over several devices outside the ownership of the company, known as Bring Your Own Device (BYOD).

BYOD's raise several issues for data security as devices without password or biometrics can accessed physically with no manipulation required, a 2016 study by Poneman revealed that half of respondents had no mobile device security despite storing or having access to sensitive work-related data [12].

BYOD's are often misplaced, damaged or lost these devices can also be deemed past their life cycle very quickly and retired. These events are out with the control or supervision of the company, with no requirement for secure deletion of stored data or the device permission privileges for cloud storage i.e. through applications access rights or autofill password features. With no oversight it is down to the individual employee, creating a potential data breach point [13]. M&W will therefore be at risk of disclosing sensitive data with very little recourse.

2. Risk Assessments

See Appendix E for Risk Distribution table.
ENISA is a center for excellence for European Union Member States and European Institutions in network and security [14]. They give advice and recommendation on good practices in information security. They categorize risks into policy and organizational risks, technical risks, legal risks and risks not specific to the cloud. The risk probability, impact matrix was deduced from the guidelines provided by ENISA for risk assessment.

2.1 Compliance challenges on Data Storage (R1)

Most European countries have now implemented GDPR. According to GDPR, there is a legal responsibility on every provider including M&W to ensure that their data subjects are compliant with legal requirements for every jurisdiction where their data may be stored. It is a company's responsibility to make sure the following aspects comply with GDPR rules; data capture, the way data is held, the way data is used and where the data would go. For this risk, the probability of breach is very high, and the impact is high according to the reference article [15].

- The current cloud storage services lack universal standards and technologies
- Lack transparency on data storage and data transmission
- Lack certifications schemes on cloud infrastructures.

2.2 Risk from changes of Jurisdiction. (R2)

Another high probability and high impact risk would be from changes of jurisdiction. For example, if the data storage location changes or if the user's geographical location changes while using the cloud storage service; then this change of jurisdiction may lead to non-compliance of specific policies and laws such as GDPR. Failure of compliance might therefore affect the company's reputation, customer trust, service delivery and the personal data in question. For an international accountancy company like M&W, the factors that might be affected are essential to its business, which is why the risk is marked as high.

- Company or users lack information on jurisdictions within each country
- Lack of transparency storing data in multiple jurisdictions.

2.3 Freedom of information and other such legal requests, specifically how the enterprise manage responds to such requests. (R3)

In M&W, an international company, if an employee in a different region uses a personal cloud, documents can be stored in servers around the world. The storage location of these documents means compliance within the laws and policies of that region. As such depending on the laws of that region these files, especially sensitive data and business secrets, may be confiscated by authorities. Moreover, limitations of cloud servers, make data accessibility difficult for the enterprise when complying with FOI requests as access of data by third parties can violate GDPR 5(1). However, the enterprise should be able to reduce this risk by always storing important data in a local server to prevent this situation. If the M&W breaks compliance law, they may receive fines, lose contracts and the ability to gain future projects.

2.4 Collusion concerns between providers and competing firms, state or parties involved in on-going cases. (R4)

The risk of collusion accompanied by data leakage to competing firms and lose client's trust, which has approximately high impact on accounting business according to the ENISA risk assessment. The collusion between provider and competing firms is severe because all sensitive data on the cloud could be stolen secretly. Fortunately, cloud providers build up a series of resorts to handle this concern. Two-step verification used in Dropbox also add an extra security method to reduce unauthorized access. All these resorts make collusion unlikely to happen, but it's still in the medium possibility.

2.5 Extensibility and accessibility of applications, access of authorized and unauthorized entities gaining access to tools and gaining insight into business processes. (R5)

Phishing and malware attacks expose both the cloud provider and client to a regular threat [16]. However, with loss of data governance already a key concern for most businesses, data attacks are to be expected and as such already mitigated through good security practice and staff training. Data leakage through inconsistent use of encryption and credential management authentication has proven to be another major issue within the cloud storage industry, despite improvements being made this is a high-risk threat with minimal solutions for enterprises [17]. With much of the improvements being centered towards paid for business accounts rather than free to use personal storage accounts.

The use of cloud storage also creates the possibility of accidental over sharing of information through direct URL links or account permission (the user may intend to grant access to one file but instead allows access to all stored files). Although cloud storage offers data restoration from previous points in time, if access is removed the user is at risk of extortion. With the implication that the employee may prefer to pay than admit the security breach, leaving the employer unaware and thus unable to enact any policy for future prevention [17].
Consequently, without adequate backups in place the employee may also be vulnerable to any loss of service by the cloud provider, whether scheduled or malicious in nature, such as DDOS attacks. Personal cloud storage providers offer virtually no recourse for the loss of business that can potentially arise in this case.

2.6 Personal hardware, improper disposal, loss and permission leakages (R6 and R7)
M&W must be extremely careful with the potential to allow sensitive data to be stored via personal smart devices. 85% of mobile applications violate basic security standards [18].

If secure data is allowed on the cloud and then accessed via unsecure mobile devices, a clear threat can be determined, with a very high likelihood of loss of data resulting in severe consequences, both financially and in reputation.

Improper disposal of redundant hardware (or loss) creates a low risk likelihood although it still carries the same consequence. As it requires the employee to fail to remove sensitive data and fail to properly dispose of the device, further to this it would require the hardware to be accessed by an adversary, creating a high attack value; the attacker would not know the value of data and most likely would focus on the value of hardware.

3. Data Protection Policies
Proper cloud storage policies are essential to prevent access of unauthorized entities gaining access to tools and gaining insight into business processes [19]. Google drive and Dropbox fall under the Software as a Service delivery model, so clients using these services will have to solely depend on the cloud service security measures [20]. However, they can come up with concise policies that help reduce the rate and impact of cybersecurity attacks.

In order to be effective, our policy intends to gain account governance for the enterprise through limiting usage and employee training to develop good habit in using personal cloud. It is recommended all policies suggestions be enacted in line with Mostel & Wilder current IT policies. It is also the recommendation of this report that the company specifies definitive roles for each personnel and as such their access to defined files and data [21].
It is also suggested that the IT department themselves generates phishing emails or attacks to test the internal services [22].

As a conclusion, our final policy presents below:

1. IT department will choose one business cloud provider, with no personal cloud accounts authorized for any employee. The personal cloud term of services needs to comply with the law and regulation in Mostel & Wilder regarding to data handling and

personal information storages [23]. This policy will be assessed by IT department and renewed annually. The result of training course and internal attacks will be recorded to help the policy assessment, as well as broader security ability of the chosen cloud provider vs other cloud providers.

2. IT department creates account for each employee on their behalf. It is also forbidden for Employees to share their log-in credentials with others. Accounts will be return to the enterprise when employee leave the job (Secure passwords created by IT department and stored securely with encryption)
3. Enterprise IT department will decide the authority level of different file, including which can/cannot be stored in the personal cloud or which need/needn't to be published or which can/cannot be shared. Since the Mostel & Wilder company is operating within the EU, it will be necessary to have a Data Protection Officer (DPO) to ensure that their data protection strategy and its implementation follows GDPR requirements and help avoid legal sanctions [24]. Enterprise IT department remain the right and ability to audit the account of the given personal cloud any time and will audit a percentage of randomized employees frequently (once a month recommended, goal of 5-10% of employees checked).
4. Medium and high-risk data (see Appendix A) will be encrypted prior to any file sharing and financial data will only be transmitted in packages of relevant data. Clients will be provided with encryption software via a download link when joining the company [25].
5. A system must be incorporated into existing data management software to record file locations (e.g. user 123 downloaded file1 tagged cloud storage).
6. Cloud accounts given by the enterprise must be used only on work computers/devices and prohibits the use of personal hardware. The IT department keep tracking of the Cloud accounts logged in devices.
7. IT department themselves will generate phishing emails or attacks to test the internal services without notification, along with security classes designed to improve employee security awareness.

4. Policies Assessments

For the policies assessments, we assess each policy through the metrics below (see Table 1). The outcome will be used to renew the policy annually.

Policy No.	Metric	Motive	Source
1	Success of security testing (%, COUNT)	Understand the performance of cloud provider	IT Department
	Costs of Business Cloud Service	Associated cost vs usage	Accounts Department
2	Number of employees left/Number of returned account (%, COUNT)	Accuracy of prevention plan stopping former employees' accessing data.	HR Department, IT Department
3	The frequency and amount that the IT department audits	Understanding staff behavior uptake	IT Department

	employees' cloud. (% COUNT)		
	The rate of incidents that illegal data storage, data sharing found by auditor in IT department. (%)	Accuracy of encryption policy and staff behavior uptake	IT Department
4	The ratio of medium and high-level files encrypted in personal storage during each audit by IT department (%)	Accuracy of encryption policy and staff behavior uptake	IT Department
5	Calculate cloud use through download rate linked to cloud storage (% COUNT)	Accuracy of file authority, maintaining GDPR compliance and file permissions	IT System
6	Personal Devices logged in (%, COUNT)	Understanding staff behavior	IT Department
7	The failure rate of employees in the phishing/malware attacks (%)	Accuracy of encryption policy and staff behavior uptake	IT Department
	The pass rate of security training courses (%)	Understanding staff behavior	IT Department

Table 1 Metrics table for policy assessment

Although it is important to monitor and review the performance of the chosen cloud platform, enterprise security concerns are ever changing, and although cloud storage is without question important, reviewing an outside entity with its own goals and security plan is not time efficient. Through continual yearly assessment of the service, improvements will be made to M&W policy improving internal security overall and inform the value of using cloud storage.

Limiting data access and encryption for medium and high-level data may be restrictive to company employees and customers; if for example data access is slow or unavailable. This should be addressed in the review process. It is unclear what effective this will have on productivity and cloud usage; policy 3 and 5 data should help inform this.

Data will be far more secure after implementing these policies, but at a cost to the IT department; whom will be required to dedicate a large amount of time to maintaining and monitoring cloud usage. In addition, employees may be bothered by the phishing email test when they may not consider it an important part of the job, management must convey its importance to improve risk adverse behaviors.

Reducing risk adverse behavior and increasing staff knowledge is extremely useful, however disrupting an entire multinational business is not without cost. The results of which once again only improve internal cyber security and does nothing to mitigate the risk posed by loss of service from the cloud provider.

References

[1] CDW. (2018). FINANCE AND GDPR: WHAT YOU NEED TO KNOW [eBook]. Retrieved from https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/tech-solutions-library/security/gdpr-finance-wp.pdf

[2] Wolford, B. (2019). What are the GDPR Fines? - GDPR.eu. Retrieved 5 December 2019, from https://gdpr.eu/fines/

[3] New Bill Imposing Increased Fines for Violations of Russian Data Protection Laws Under Consideration | HL Chronicle of Data Protection: 2019. https://www.hldataprotection.com/2019/06/articles/international-eu-privacy/new-bill-imposing-increased-fines-for-violations-of-russian-data-protection-laws-under-consideration/. Accessed: 2019- 12- 06.

[4] Information Commissioners Office (ICO). (2018). Guide to the general data protection regulation (GDPR).

[5] National Board of Trade. (2012). How Borderless is the Cloud? - Kommerskollegium. Retrieved 5 December 2019, from https://www.kommers.se/In-English/Publications/2012/How-Borderless-is-the-Cloud/

[6] CitizenInformation. (2018). Freedom of information. Retrieved 5 December 2019, from https://www.citizensinformation.ie/en/government_in_ireland/national_government/standards_and_accountability/freedom_of_information.html

[7] Vollmer, N. (2019). Article 5 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan. Retrieved 5 December 2019, from http://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.html

[8] Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision: 2018. https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision. Accessed: 2019- 12- 06.

[9] Verizon 2019. 2019 Data Breach Investigations Report.

[10] 2019 Cost of a Data Breach Report| IBM Security: 2019. https://databreachcalculator.mybluemix.net/. Accessed: 2019- 12- 06.

[11] Lee, B. (2019). Top Cloud Data Breaches in 2018 Lessons Learned. Retrieved 5 December 2019, from https://spinbackup.com/blog/top-cloud-data-breaches-2018-lessons-learned/

[12] Ponemon. (2016). How Much Is the Data on Your Mobile Device Worth? [eBook] Retrieved from

https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf

[13] Nordquist, B. (2019). Don't Let Personal Cloud Storage Become an IT Nightmare | StorageCraft. Retrieved 5 December 2019, from https://blog.storagecraft.com/personal-cloud-storage/

[14] ENISA, C. C. (2009). Benefits, risks and recommendations for information security. European Network and Information Security.

[15] IMPERVA. (2013). Assessing the Threat Landscape of DBaaS [eBook] (18th ed.). Retrieved from https://www.imperva.com/docs/HII_Assessing_the_Threat_Landscape_of_DBaaS.pdf

[16] Virtru. (2019). Dropbox Encryption vs. Google Drive Encryption. Retrieved 5 December 2019, from https://www.virtru.com/blog/dropbox-encryption/

[17] Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, 8(1), 2.

[18] Positive Technologies. (2019). Vulnerabilities and threats in mobile applications. Retrieved 5 December 2019, from https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

[19] Butler, J. (2019). Bring your own cloud: Understanding the right policies for employees. Retrieved 5 December 2019, from https://www.cloudcomputing-news.net/news/2015/may/22/bring-your-own-cloud-understanding-right-policies-employees/

[20] The Dangers of Recycling Passwords:2013. https://www.safesystems.com/blog/2013/10/dangers-recycling-passwords/. Accessed: 2019- 12- 06.

[21] Subashini, S. and Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 34, 1 (2011), 1-11.

[22] McAfee. (2019). Creating a Cloud Security Policy | McAfee. Retrieved 5 December 2019, from https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/cloud-security-policy.html

[23] Berry, M. (2019). Cloud Computing Policy Template. Retrieved 5 December 2019, from http://www.itmanagerdaily.com/cloud-computing-policy-template/

[24] Lord, N. (2019). What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019. Retrieved 5 December 2019, from

https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance

[25] Edwards, C., Montgomery, D., & Gilmour, R. (2017). University of Glasgow - MyGlasgow - IT Services - Information Security - Policies - Cloud Policy. Retrieved 5 December 2019, from https://www.gla.ac.uk/myglasgow/it/informationsecurity/policies/cloudpolicy/

[26] Montgomery, D., Edwards, C., & King, J. (2018). Information Risk Classifications [eBook]. Glasgow: University of Glasgow. Retrieved from https://www.gla.ac.uk/media/Media_537721_smxx.pdf

Bibliography

Corpuz, M. (2011). Enterprise information security policy assessment: an extended framework for metrics development utilizing the goal-question-metric approach. In Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics (Vol. 3, pp. 269-274). International Institute of Informatics and Systemics (IIIS).

Michener, G. (2011). FOI laws around the world. Journal of Democracy, 22(2), 145-159.

Tchernykh, A., Babenko, M., Chervyakov, N., Cortés-Mendoza, J. M., Kucherov, N., Miranda-López, V., ... & Radchenko, G. (2017, August). Towards mitigating uncertainty of data security breaches and collusion in cloud computing. In 2017 28th International Workshop on Database and Expert Systems Applications (DEXA) (pp. 137-141). IEEE.

Winder, D. (2019). Cloud storage: How secure are Dropbox, OneDrive, Google Drive and iCloud? Retrieved 5 December 2019, from https://www.itpro.co.uk/cloud-security/34663/cloud-storage-how-secure-are-dropbox-onedrive-google-drive-and-icloud

Zhu, Z., & Jiang, R. (2015). A secure anti-collusion data sharing scheme for dynamic groups in the cloud. IEEE Transactions on parallel and distributed systems, 27(1), 40-50.

Appendix A

Risk Classifications

Low Risk	Medium Risk	High Risk
Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and: 1 The data is intended for public disclosure, or: 2 The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and: 1 The data are not generally available to the public, or: 2 Defined by the GDPR as "personal data", or: 3 The loss of confidentiality, integrity, or availability could have a mildly adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as High Risk if: 1 Defined by the GDPR as "special category data" see list directly below, or: 2 The loss of confidentiality, integrity, or availability could have a significant adverse impact on our mission, safety, finances, or reputation, or result in damage/distress to students, staff or other individuals.

Table 1 Information on Risk Classifications (Montgomery, Edwards & King, 2018) [26]

Information/Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data

When mixed data falls into multiple risk categories, use the highest

Low Risk	Medium Risk	High Risk
▪ Research data (at PI discretion) ▪ Staff work contact info ▪ Policies and Guidance, unless specific requirement to restrict ▪ College/School/Course details, marketing or press Information ▪ Job adverts ▪ Publicly available campus maps ▪ Anything in UofG FoI publication scheme ▪ Information in the public domain	▪ Unpublished research data (at PI discretion) ▪ Student names and email addresses ▪ Individuals' dates of birth, personal contact details (e.g. home address, phone number) ▪ NI or passport numbers ▪ Staff and student ID numbers ▪ Unpublished planning and budgeting info ▪ Commercially sensitive information ▪ Embargoed theses	▪ Special Category data - personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a person, health, sex life or sexual orientation ▪ Criminal convictions or alleged offences ▪ Individuals' financial information, including credit card/bank numbers. ▪ **Details of many individuals, that would otherwise be rated Medium Risk.*** ▪ Donor contact information and non-public gift information ▪ Exam questions prior to use

Table 2 Information on Risk Classifications Example (Montgomery, Edwards & King, 2018) [26]

Appendix B

ENTERPRISE CYBER SECURITY (M)
PLAN FOR ACTION ONE

TEAM NAME	Group X
MEMBERS (student numbers)	2471294
	2471061
	2443170
	2458479
	2495357
REVIEW	Reviewer 1

BADGES	**YES/NO**
Independent and Critical Thinker	Yes
Effective Communicator	No

STOP
Outline the most important piece of 'stop' feedback you received about your draft report from the review (100 words limit).
• Look at formatting – there are inconsistencies in the report. • References are not in ACM format I would consider these two points the same, as they simply state that we need to tighten up the document and maintain consistency in formatting and referencing.
Outline the actions taken in the final report to address feedback (100 words limit).
Formatting has been undertaken according to assessment specification and referencing formatted in ACM.
Evidence of actions in final report (provide references)
Overall formatting of document and reference section

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
Start considering measurements and metrics to show the effectiveness of policy implementation. The policy and implementation sections require more focus, so it was no surprise the reviewer identified the need for improvements.
Outline the actions taken in the final report to address feedback (100 words limit).
We have completely reworked the policy section and added a metrics table detailing the Metric, Motive and Source; to better ensure each policy has a useful metric to calculate each policy 's effectiveness.

Evidence of actions in final report (provide references)
See policy, policy assessment (policy assessment table) in comparison to draft report.

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
Developing policies and consider explaining them explicitly. It is suggested that the policies should be given headers and examples to make them more succinct and digestible for management (as a method of gaining approval).
Outline the actions taken in the final report to address feedback (100 words limit).
Each policy has been numbered to define and then later further explain its use, with the intention of making them clear to any potential decision makers. Effort has also been made overall to improve the document making it more applicable to business than academia.
Evidence of actions in final report (provide references)
See numbered policies in policy section

Appendix C

ENTERPRISE CYBER SECURITY (M)
PLAN FOR ACTION TWO

TEAM NAME	Group X
MEMBERS (student numbers)	2471294
	2471061
	2458479
	2443170
	2495357
REVIEW	Reviewer 2

BADGES	**YES/NO**
Independent and Critical Thinker	YES
Effective Communicator	NO

STOP
Outline the most important piece of 'stop' feedback you received about your draft report from the review (100 words limit).
The discussion of 'Risk Appetite' in risk assessment introduction section should be supported with

examples or just deleted.
Outline the actions taken in the final report to address feedback (100 words limit).
After reviewing the risk assessment in section 2, we found out that 'Risk Appetite' does not compliment the structure, however a more specific introduction on how we rank the risk is needed. We discussed a bit on ENISA, the organization which provides guidelines for risk assessment and general good practices in information security.
Evidence of actions in final report (provide references)
See description of ENISA in section 2.

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
• Provide adequate metrics to evaluate the performance and success of the proposed policy
Outline the actions taken in the final report to address feedback (100 words limit).
The policies were redone to improve the metrics. The metrics table was created to detail the metrics, policies, motives and source of metrics.
Evidence of actions in final report (provide references)
See policy section and policy table

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
• Address the specific context of Mostel and Wilder like section 2.5
Outline the actions taken in the final report to address feedback (100 words limit).
The document was reviewed, and more focus was put on the requirements of an accounting firm rather than a general enterprise
Evidence of actions in final report (provide references)
Improvements made overdraft report

Appendix D

ENTERPRISE CYBER SECURITY (M)
PLAN FOR ACTION THREE

TEAM NAME	Group X
MEMBERS (student numbers)	2471294
	2471061
	2458479
	2443170

	2495357
REVIEW	Reviewer 3

BADGES	**YES/NO**
Independent and Critical Thinker	YES
Effective Communicator	YES

STOP
Outline the most important piece of 'stop' feedback you received about your draft report from the review (100 words limit).
• Stop using cloud auditor work as independent bodies Nothing else mentioned in the 'stop' part of review other than 'Grammatical mistakes make the report confusing and often hard to fully understand.' but in the rubric, they said we should stop using 'cloud auditor' as a third-party service, because auditor out of the enterprise may not understand the intern demand thus cannot protect enterprise assets properly.
Outline the actions taken in the final report to address feedback (100 words limit).
Cloud auditor is our key resort in account governance which cannot be removed. Therefore, we change to internal cloud auditor rather than the independent body ones. In the final report, IT department of M&W will take charge in creating account for every employee so that they can keep the governance of the account password, and thus make it easier to audit each account. As a part of the enterprise, IT department would know exactly what the demand is, and as well lower the risk of data leakage from the audit process.
Evidence of actions in final report (provide references)
See policy section (page 9-10) and policy 3.

START
Outline the most important piece of 'start' feedback you received about your draft report from the review (100 words limit).
• For the risk 1 and 2, should raise some new concerns about the enterprise cyber security problem, for example, rubric's risk assessment section for ideas. For risk 3, add some training policy of employee We choose two most significant points in the review for our draft modification. The first one is in the risk part. Our report needs to raise some new concerns about enterprise cyber risk which are not mentioned in the article and give some examples of it. The second one is in the policy part. We decided to add some specific policies such as training normal employees to obey the security rules.
Outline the actions taken in the final report to address feedback (100 words limit).
we add two new concerns into the risk part and give particular explanation of them. We also list some examples of the two new concerns. We also find some new references and make some new policies. One of them is giving the cyber security courses for employees to improve their security consciousness.
Evidence of actions in final report (provide references)
Please check 1.5 and 1.6 in the risk part and the last policy

CONTINUE
Outline the most important piece of 'continue' feedback you received about your draft report from the review (100 words limit).
• The focus on GDPR regulations over other national and international laws GDPR regulations and other national and international laws. Consider about the differences, in the policy part, we make the policy more dynamically than the first time we made and give some specific rules. Moreover, we correct grammar mistakes and modify phrases when we finish the final draft.
Outline the actions taken in the final report to address feedback (100 words limit).
We continue working on the differences between GDPR and local policy, and then give more details and examples about it. We also correct our spelling errors and grammar mistakes after we finish the final draft.
Evidence of actions in final report (provide references)
Please check 1.3 in the risk part and 2.3 in the risk assessment part

Appendix E

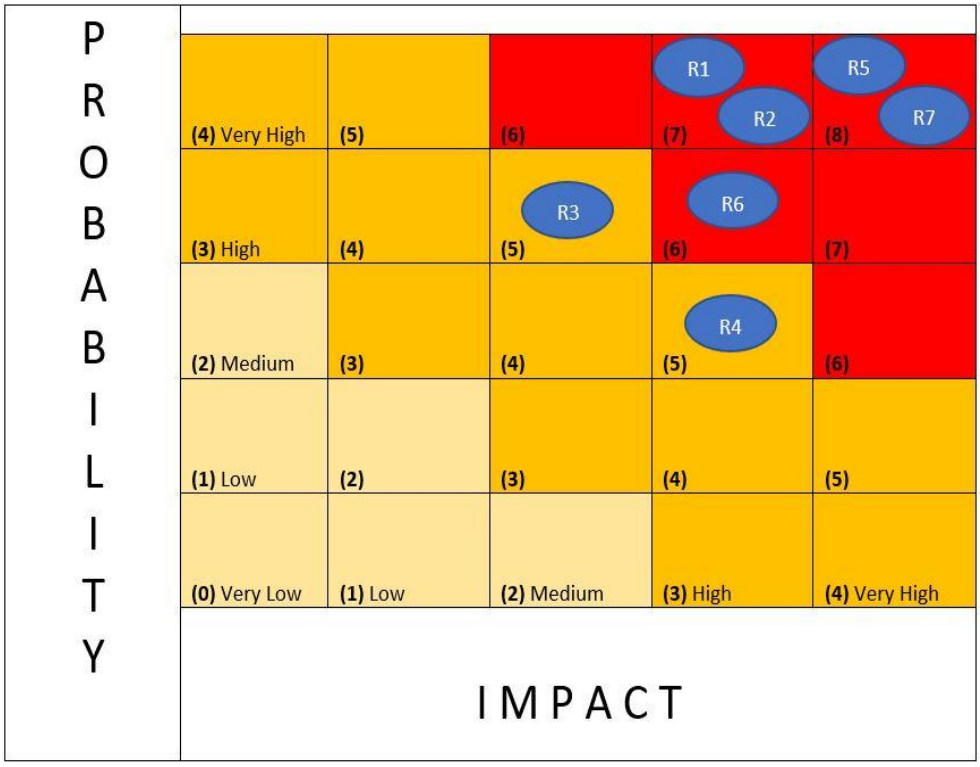

TABLE 3: RISK DISTRIBUTION.

Appendix F

WORKLOAD REPORT
This report is separated into 20% for each member in the team.