Summative Assessment Report

Cyber Security Threats

University of York

Word Count - 2915

Table of Contents

| 1 Introduction | 3 |
| --- | --- |
| 2 Risk Management | 3 |
| 2.1 Methodology | 3 |
| 2.2 Assets | 5 |
| 2.3 Risk Management Plan | 6 |
| 2.4 Risk Treatment | 9 |
| 3 Legal Issues | 11 |
| 4 Future Recommendations | 12 |
| 5 Conclusion | 14 |
| Reference List | 15 |
| Appendix A - Risk Appetite Matrix | 18 |

# 

1 Introduction

The spin out company, based on the Autonomous Robotic Surgery (ARS) Project, will be United Kingdom (UK) based and will provide training and education for surgeons in the field of surgical robots.

Services will include using surgical robots, such as the Da Vinci Surgical Systems model, alongside custom made scenarios which will be developed by the company for the training of surgeons. A second service offered will be the collection of data from the surgeons' reactions and decisions. This will be captured by the company and analysed for later use by ARS for the development of an autonomous surgical robot; development of Artificial Intelligence (AI) to react to unexpected events in a surgical environment [[1]](https://www.zotero.org/google-docs/?broken=BoQc1W), is one or ARS’s research outcomes. Finally, a website will be another service offered which will allow clients to book training and the platform will be used to advertise the company’s services.

An Information Security Management System (ISMS) for the described company will be created by: identifying context, risk identification and analysis, risk treatments, identification of legal issues and identification of technical areas for future work.

2 Risk Management

2.1 Methodology

ISO 27001 has been selected as an appropriate standard because of its robust and comprehensive framework. For example, three attributes identified by ISO 27001 for information security are: people, processes and technology [[2]](https://www.zotero.org/google-docs/?broken=NeDI1N). This illustrates how the critical components of an organisation's information security are considered together and not in isolation. For instance, [[3]](https://www.zotero.org/google-docs/?broken=UVCm95) argues that a culture of following procedures must be developed within the organisation. This highlights how the attributes of ISO 27001 are aligned to the creation and continuous improvement of an ISMS. Moreover, a framework for information security considerations, including: risk assessment, risk treatment, incident response and continuous improvement are used. These considerations facilitate proactive security and maintain the Confidentiality, Integrity and Availability (CIA) of assets.

Certification is gained from ISO 27001 and is beneficial in reassuring clients that robust ISMS procedures are in place [[4]](https://www.zotero.org/google-docs/?broken=M8iya3). Accordingly, certification offers reassurance that proper procedures and controls are in place and followed. As a result, this provides confidence in the company’s ISMS. On the other hand, [[5]](https://www.zotero.org/google-docs/?broken=JRz27N) puts forward that ISO 27001 certification does not offer a competitive advantage and could be seen as merely a paperwork exercise. Ultimately, decreasing confidence in the standard. Having said that, [[6]](https://www.zotero.org/google-docs/?broken=jPzvMJ) found that companies with ISO 27001 certification have an improved risk based approach to information security and demonstrate good internal controls and processes. Therefore, a strong argument is made for the benefits outweighing the potential subjective ‘cons’ of certification and selection of ISO 27001.

Defined structures in ISO 27001, such as controls in Annex A, provide a comprehensive methodology for risk management. Indeed, [[7]](https://www.zotero.org/google-docs/?broken=43XF4q) places Annex A controls into five categories: data, hardware, software, people and network. This allows threats to be grouped using the CIA triad to assess the impact of risk. In comparison, Factor Analysis of Information Risk (FAIR) is a quantifiable methodology which uses four factors to measure and quantify risk [[8]](https://www.zotero.org/google-docs/?broken=lqbWbf). This is beneficial to view financial loss but is limited within a rigid framework which is difficult to expand. Indeed, [[9]](https://www.zotero.org/google-docs/?broken=qehBaB) supports this by arguing that not all threats can be supported by the FAIR methodology. Overall, ISO 27001 provides a comprehensive understanding of risks and controls for risk management.

With ISO 27001 additional documentation is suggested as guidance, such as ISO 27005 and ISO 31000, which support the creation of the ISMS.

Implementation of ISO 27001 for the company will be:

1. Context establishment (Clause 4)
2. Risk identification (Clause 6)
3. Risk analysis (Clause 6)
4. Risk evaluation (Clause 6)
5. Risk treatment (Clause 6)
6. Monitoring and review (Clause 9, 10)

2.2 Assets

Context is established to identify assets and identify risks by using Clause 4 and 6 of ISO 27001 [[10]](https://www.zotero.org/google-docs/?broken=k6XYpe) alongside Clause10 of ISO 27005 [[11]](https://www.zotero.org/google-docs/?broken=O3WXQg) for additional guidance.

Firstly, [11] states the organisation requires a strategic understanding of issues affecting the ISMS. This strategic understanding is: the storage of data, such as personal information and data captured during training from surgeons.

Secondly, internal and external context will be established, ISO 31000 clause 4.3.1 [[12]](https://www.zotero.org/google-docs/?broken=hpqi0C) provides guidance on this. The company will be responsible for everything within the ISMS boundary, such as the systems it has complete control over. However, responsibility cannot be taken for data which has left the company’s system, for instance data being transmitted on a public network.

External context is identified as:

1. Stakeholders, such as customers and shareholders
2. Research aims of ARS
3. Compliance to UK and EU laws and regulations
4. Ethics of how data is used to train AI

Internal context is identified as:

1. Employees
2. Security of data and information
3. Directors and shareholders
4. AI development

Assets are defined in ISO 27005 as activities, process and information [11]. Following ISO 27001 Annex A: A.8.11, A.8.1.2, an inventory of assets and owners to maintain them [10] are shown in Table 1. Notably, assets need to be identified in order for the company to know what information to protect [[13]](https://www.zotero.org/google-docs/?broken=Nj8ORp).

| **Asset** | **Owner** | **CIA** | **Associated Risk(s)** |
| --- | --- | --- | --- |
| Training software | Head of Development | A/I | - Theft of software  - Malicious code |
| Surgical robots | Head of Operations | A/I | - Not updated  - Physical damage/theft |
| Collected data from surgical simulations | CISO | C/I | - Weak encryption  - Weak hash |
| Client and employee databases | CISO | C/I/A | - SQL injection  - Ransomware |
| Network infrastructure | Head of IT | C/I/A | - DDOS  - Open ports |
| Physical security of premises | Head of Operations | C/I/A | - Unlocked server room  - Man in the middle attack |

*Table 1 - Company Assets*

In order to identify the importance of assets, the CIA triad is utilised [12]. CIA are terms which have shaped both the understanding of cyber security and how processes are created to identify and mitigate threats. However, as the sophistication of threats has evolved, so has the scope of CIA. Indeed, [[14]](https://www.zotero.org/google-docs/?broken=xEQajw) puts forward that CIA are broad terms which since the 1970s have encompassed additional definitions. For instance, authenticity and non-repudiation are categorised under integrity, highlighting the diversity of threat type. This aids the company in prioritising assets and the impact of associated risks.

2.3 Risk Management Plan

Following ISO 27005 guidance: risks need to be identified, Clause 7.2, analysed, Clause 7.3, and evaluated, Clause 7.4 [11]. Using Clause 6.1.2a-c of ISO 27001 [10] risks have been identified using the criteria of company assets. This is highlighted in Table 2 through the risk calculation score from the impact multiplied by the likelihood.

| **Asset** | **Threat** | **Vulnerability** | **Risk owner** | **Impact (1-5)** | **Likelihood (1-5)** | **Risk (=I\*L)** | **Treatment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Database of client information | Insider Threats | Poor access control | CISO | 5 | 3 | 15 | Strict access controls |
| Malware/ ransomware | Lack of updates | 4 | 3 | 12 | Regular updates |
| Employees | Social engineering | Lack of staff training. | HR Manager | 5 | 2 | 10 | Security awareness training |
| Data in Transit | Man In The Middle | Poor/weak encryption | Network Manager | 5 | 2 | 10 | SSL/TLS |
| No digital signature | 3 | 1 | 3 | Implement digital signatures |
| Weak authentication | 4 | 2 | 8 | MFA |
| Website | DDOS | Lack of DDoS mitigation measures. | CISO | 4 | 4 | 16 | Traffic monitoring |
| Defacement | Unpatched vulnerabilities in content management systems | 4 | 1 | 4 | Web application firewall |
| Cross site scripting | Improper input validation | 4 | 2 | 8 | Update/patch website |
| Insider threats | Inadequate access controls | 5 | 1 | 5 | Access controls |

*Table 2 - Risk Assessment*

Analysis of risks is qualitative which is in line with ISO 27001 Clause 7.3.1 [10]. An advantage of qualitative risk assessments is the speed for completion and clear delivery of risk likelihood to business stakeholders [[15]](https://www.zotero.org/google-docs/?broken=ZemrWl). However, quantifiable risk assessments allow for a greater understanding of risks which are assigned specific values, however, more time and quantitative data is required [[16]](https://www.zotero.org/google-docs/?broken=1W7Q53). For instance, [[17]](https://www.zotero.org/google-docs/?broken=gH60Rm) conducted a Monte Carlo analysis, alongside additional statistical analysis, to create a quantitative risk assessment. Notably, the resources were available for a successful quantitative risk assessment. However, the company does not have the required data for a quantitative risk assessment, therefore a qualitative risk assessment is justified to delineate acceptance criteria.

In order to prioritise risk, a risk matrix has been utilised (see *Appendix A*). This is based on Table A.6 in ISO 27005 [11], and is used for guidance in order to assess risk appetite by matching the risk score from Table 2 to the risk matrix. A priority of risks is identified as follows:

1. DDOS attack
2. Insider threats
3. Malware
4. Cross site scripting
5. Social engineering
6. MITM
7. Weak encryption
8. Insider threats
9. Website defacement
10. No digital signatures

Risks 1 and 2 fall into an unacceptable category and actions to reduce the risk need to be taken [11]. Risks 3-7 are tolerable under control and a risk management follow up will need to be conducted [11]. Lastly, risks 8-10 are acceptable as they are.

2.4 Risk Treatment

Insider threats are identified because they pose an unacceptable level of risk. Controls for this type of threat are identified in Annex A A.12.4 Logging [11], which advises the monitoring and protection of information.

One treatment is to consider access controls and removing excessive privileges. Notably, [[18]](https://www.zotero.org/google-docs/?broken=mo4f1E) highlights how an access control policy and auditing of legitimate users to produce an audit trail are effective. For instance, strict access controls and a database active monitoring system such as IBM Security Guardium, are efficient treatments. This is supported by [[19]](https://www.zotero.org/google-docs/?broken=8QuEnt) alongside revoking rights once a user no longer requires them. Similarly, reducing the risk with an Intruder Detection System (IDS) to monitor unauthorised access is considered. However, [[20]](https://www.zotero.org/google-docs/?broken=3sLXoN) highlights that a modern machine learning IDS provides limited explanations of why detections are made. This can create a lack of transparency in the system, making it difficult to validate an IDS’s effectiveness.

Alternatively, a Deep Feedforward Neural Networks (DFNN) can be used to recognise the normal behaviour of users. For instance, parameters and thresholds can be utilised to detect abnormal actions [[21]](https://www.zotero.org/google-docs/?broken=XXSJFx). An advantage is DFNN’s can be established quickly to capture threats, however DFNN’s do not capture the temporal information of users [[22]](https://www.zotero.org/google-docs/?broken=6QClqw) which limits contextual understanding.

Given the potential drawback of using a DFNN, the spin out company will employ strict access controls and user privileges to restrict access to the database in order to reduce the threat.

DDOS attacks impact organisations by removing the availability of services. This could result in reputational damage and financial loss if the attack is persistent and over an extended period of time. An example of a recent DDOS attack on the Belgium parliament [[23]](https://www.zotero.org/google-docs/?broken=V4iR9K) illustrates that DDOS attacks are increasing in number and volume. Indeed, attacks using 100 gigabits per second grew by 67% and attacks lasting for over three hours increased by 87% in 2022 [[24]](https://www.zotero.org/google-docs/?broken=tpwd0G).

A possible treatment is the use of machine learning and artificial intelligence to provide warning and mitigation techniques. Research form [[25]](https://www.zotero.org/google-docs/?broken=mDzXwI) argues that a Long Short Term Memory neural network can achieve this with a high degree of results. However, this research focuses on HTTP based flooding attacks. An alternative to this is Extreme Gradient Boosting (XGBoost) to identify legitimate traffic. For instance, [[26]](https://www.zotero.org/google-docs/?broken=ZjdVKR) presents research that XGBoost achieved 85%-95% accuracy. This is supported by, [[27]](https://www.zotero.org/google-docs/?broken=rWKa0J) who argue that XGBoost outperforms other algorithms and has improved accuracy. Importantly, accurate predictions can enable information technology teams to mitigate the effects of a DDOS attack. Therefore, XGBoost is selected as a treatment to give warnings of potential DDOS attacks and reduce the threat.

3 Legal Issues

The Data Protection Act 2018 (DPA) for the UK aligns with the European Union’s General Data Protection Regulation (GDPR) and are legal requirements for the company to operate. To address this, ISO 27001 is beneficial as the standard facilitates compliance with law. Indeed, [[28]](https://www.zotero.org/google-docs/?broken=H8vy0x) highlights principles such as: accountability, risk assessments and a security framework as integral aspects of ISO 27001. This shows that implementation of ISO 27001 addresses legal compliance through its framework, with audit trails as a control specified in Annex A. Furthermore, this can be augmented with the employment of a dedicated Data Protection Officer and encryption of data held in company databases [[29]](https://www.zotero.org/google-docs/?broken=1DHWEk)[10].

Implications for not complying with the DPA, or GDPR, can be severe because this can result in monetary fines, restrictions on processing data and reputational damage [[30]](https://www.zotero.org/google-docs/?broken=6gVOGh). A method for addressing this is by using controls specified in Clause A.18.1.1 within Annex A. This will ensure the company is compliant with the law. Evidently, [[31]](https://www.zotero.org/google-docs/?broken=fqtP0J) puts forward that fines have made organisations privacy aware, which has improved risk management and increased reputational trustworthiness. Therefore, this control is wholly appropriate as it will allow the company to operate without hindrance or reputational damage.

Medical Device Regulation (MDR) in the UK is a consideration for surgical robot assets owned by the company. Although devices used by the company will not be used in real surgeries, compliance is still required. An implication of MDR is that devices must be monitored for performance and safety [[32]](https://www.zotero.org/google-docs/?broken=fs53D7). A method to address this is the regular maintenance and testing of devices to ensure that they meet industry standards. This is appropriate and is supported by Annex A.12.5.1 [10], which clearly states that software should be managed, such as receiving regular updates.

Consumer protection regulations will apply to the spin out company because it is offering a training program. For instance, the Consumer Rights Act 2015 (CRA) has the implications of complaints and disputes which can relate to data security [[33]](https://www.zotero.org/google-docs/?broken=DnRmzp). Specifically, if a customer has a concern about a data breach, or the mishandling of data, an implication is that the company will be required to address this concern or face financial penalties. To address this issue, one method is to publicly declare any data breaches and inform customers. A second control for this issue is a review of the company’s risk assessment, ISO 27001 Clause 9 and 10 [10], to establish why it happened and prevent it happening again.

4 Future Recommendations

Ransomware attacks are becoming increasingly sophisticated, with implications of an attack being reputationally and financially damaging. Backing up data, detection and then blocking ransomware are traditional defences. However, ransomware can be difficult to discover if its behaviour is unobserved. Indeed, packing techniques can be used for it to remain undetected [[34]](https://www.zotero.org/google-docs/?broken=uE8mUO). This makes detection and prevention of ransomware difficult, especially if the backed up data is also targeted. A treatment is Device Level Backup Solid State Devices (DLB-SSD), such as Flashguard, which can detect ransomware by monitoring for its input/output writing pattern. An alternative viewpoint argues that DLB-SSD can predict excessive false-positives and generate space overhead by performing unnecessary backups [[35]](https://www.zotero.org/google-docs/?broken=TvDmy6).

A recommendation for management to consider for future inclusion is content based ransomware based detection because of improved space overheads and reduced false positives. For instance, [[36]](https://www.zotero.org/google-docs/?broken=jsK6d9) put forward Amoeba, using rule based detection, to monitor the number of writes, similarity and entropy of page write operations. Amoeba is highly effective against known ransomware, albeit, new or zero day ransomware attacks are identified as weaknesses. However [35] shows that Amoeba outperforms traditional anti-ransomware software. With the potential negative impact from ransomware, future consideration for its mitigation is strongly recommended.

Multi-Factor Authentication (MFA) is a technical area which will enhance authenticity for the company because it adds additional security. Indeed, submission of additional information, such as: fingerprints, one time passwords or facial recognition adds additional levels of depth to existing security. Notably, these attributes fall into categories, such as: what someone knows, where someone is and what someone has in order to ensure only legitimate people have access to a system [[37]](https://www.zotero.org/google-docs/?broken=k3J9Nj). Significantly, MFA will mitigate unauthorised access and improve security.

Justifications for the consideration of MFA are risk reduction, by lowering the possibilities of account hijacking, and security enhancement of sensitive data. Supporting this, [[38]](https://www.zotero.org/google-docs/?broken=nPlfyO) argues for risk based authentication where attributes, such as: time of day, device information and internet protocol address information to form a risk assessment and request different authentication from those details and level of risk generated. With the importance given to data security, and how the company will handle that data, MFA is strongly suggested for future inclusion.

The company will be analysing data and a future capacity to develop software could be required. To facilitate this, a Secure Software Development Lifecycle (SDLC) should be implemented because it ensures security is considered in every phase of development. For instance, security can be deferred until the testing phase and if issues arise they can cause delays [[39]](https://www.zotero.org/google-docs/?broken=cVa5ip). However, [[40]](https://www.zotero.org/google-docs/?broken=cTgPSE) posits that a SDLC process helps by integrating security with development. Arguably, this results in more secure software and early detection of software flaws. For instance, vulnerabilities in software can be identified before it is deployed as vulnerabilities were considered at the design phase and not during a test phase. As a future consideration a SDLC framework will reduce security issues during the development stages and provide customers with reassurance of the company’s commitment to secure services.

5 Conclusion

In conclusion, ISO 27001 provides a comprehensive methodology for assessing, analysing and evaluating risk. Significantly, certification is beneficial for the company’s reputation as it projects a serious attitude towards threats and a culture of following procedure. Furthermore, assets are accounted for within the company with assigned owners to take responsibility. From this threats have been identified, analysed and prioritised. With a risk rating assigned, threats are then managed with the two highest risks being reduced through use of Annex A controls.

Reference List

[[1] ‘ARS: Autonomous Robotic Surgery’, *ars-project.eu*. https://www.ars-project.eu/ (accessed Jun. 12, 2023).](https://www.zotero.org/google-docs/?broken=6mPzbc)

[[2] I. M. Lopes, T. Guarda, and P. Oliveira, ‘Implementation of ISO 27001 Standards as GDPR Compliance Facilitator’, *J. Inf. Syst. Eng. Manag.*, vol. 4, no. 2, Aug. 2019, doi: 10.29333/jisem/5888.](https://www.zotero.org/google-docs/?broken=evoeua)

[[3] S. H. Björnsdóttir, P. Jensson, R. J. Boer, and S. E. Thorsteinsson, ‘The Importance of Risk Management: What is Missing in ISO Standards?’, *Risk Anal.*, vol. 42, no. 4, pp. 659–691, Apr. 2022, doi: 10.1111/risa.13803.](https://www.zotero.org/google-docs/?broken=xAqIUv)

[[4] S. Patino, E. F. Solis, S. G. Yoo, and R. Arroyo, ‘ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005’, in *2018 International Conference on eDemocracy & eGovernment (ICEDEG)*, Ambato: IEEE, Apr. 2018, pp. 75–82. doi: 10.1109/ICEDEG.2018.8372361.](https://www.zotero.org/google-docs/?broken=KYxGRN)

[[5] C. Hsu, T. Wang, and A. Lu, ‘The Impact of ISO 27001 Certification on Firm Performance’, in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA: IEEE, Jan. 2016, pp. 4842–4848. doi: 10.1109/HICSS.2016.600.](https://www.zotero.org/google-docs/?broken=z5k32o)

[[6] D. N. K. Sharma, ‘EFFECTIVENESS OF ISO 27001, AS AN INFORMATION SECURITY MANAGEMENT SYSTEM: AN ANALYTICAL STUDY OF FINANCIAL ASPECTS.’, vol. 9, no. 3, 2012.](https://www.zotero.org/google-docs/?broken=LklpmL)

[[7] B. Shojaie, H. Federrath, and I. Saberi, ‘Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A’, in *2014 Ninth International Conference on Availability, Reliability and Security*, Fribourg, Switzerland: IEEE, Sep. 2014, pp. 259–264. doi: 10.1109/ARES.2014.41.](https://www.zotero.org/google-docs/?broken=ndB2Ec)

[[8] ‘What is Fair?’, *Fairinstitute.org*. https://www.fairinstitute.org/what-is-fair (accessed Jun. 22, 2023).](https://www.zotero.org/google-docs/?broken=MrcyFq)

[[9] J. Wang, M. Neil, and N. Fenton, ‘A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model’, *Comput. Secur.*, vol. 89, p. 101659, Feb. 2020, doi: 10.1016/j.cose.2019.101659.](https://www.zotero.org/google-docs/?broken=QUC3Ap)

[[10] ‘BS EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements.’ International Organization for Standardization, Geneva, Switzerland, 2017.](https://www.zotero.org/google-docs/?broken=SLN8QN)

[[11] ‘BS ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks’. International Organization for Standardization, Geneva, Switzerland, 2022.](https://www.zotero.org/google-docs/?broken=gvHzB4)

[[12] ‘BS ISO 31000:2018 Risk management. Guidelines’. International Organization for Standardization, Geneva, Switzerland, 2018.](https://www.zotero.org/google-docs/?broken=LpjCPp)

[[13] A. Asosheh, P. Hajinazari, and H. Khodkari, ‘A practical implementation of ISMS’, in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*, Kish Island, Iran: IEEE, Apr. 2013, pp. 1–17. doi: 10.1109/ECDC.2013.6556730.](https://www.zotero.org/google-docs/?broken=V9ImhW)

[[14] S. Samonas and D. Coss, ‘THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY’.](https://www.zotero.org/google-docs/?broken=dNDk5E)

[[15] Joint Task Force Transformation Initiative, ‘Guide for conducting risk assessments’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.](https://www.zotero.org/google-docs/?broken=UmwFCY)

[[16] S. Li, F. Bi, W. Chen, X. Miao, J. Liu, and C. Tang, ‘An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking’, *IEEE Access*, vol. 6, pp. 10311–10319, 2018, doi: 10.1109/ACCESS.2018.2800664.](https://www.zotero.org/google-docs/?broken=PXvVKk)

[[17] J. P. De Vries, U. Livnat, and S. Tonkin, ‘A Risk-Informed Interference Assessment of MetSat/LTE Coexistence’, *IEEE Access*, vol. 5, pp. 6290–6313, 2017, doi: 10.1109/ACCESS.2017.2685592.](https://www.zotero.org/google-docs/?broken=fQPKsl)

[[18] M. Malik and T. Patel, ‘Database Security - Attacks and Control Methods’, *Int. J. Inf. Sci. Tech.*, vol. 6, no. 1/2, pp. 175–183, Mar. 2016, doi: 10.5121/ijist.2016.6218.](https://www.zotero.org/google-docs/?broken=HBSF5F)

[[19] A. Mousa, M. Karabatak, and T. Mustafa, ‘Database Security Threats and Challenges’, in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon: IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/ISDFS49300.2020.9116436.](https://www.zotero.org/google-docs/?broken=J0Dl0N)

[[20] M. Wang, K. Zheng, Y. Yang, and X. Wang, ‘An Explainable Machine Learning Framework for Intrusion Detection Systems’, *IEEE Access*, vol. 8, pp. 73127–73141, 2020, doi: 10.1109/ACCESS.2020.2988359.](https://www.zotero.org/google-docs/?broken=KVZ4UC)

[[21] L. Fuchs and G. Pernul, ‘Minimizing insider misuse through secure Identity Management: Secure Identity Management’, *Secur. Commun. Netw.*, vol. 5, no. 8, pp. 847–862, Aug. 2012, doi: 10.1002/sec.314.](https://www.zotero.org/google-docs/?broken=SBdZYT)

[[22] S. Yuan and X. Wu, ‘Deep learning for insider threat detection: Review, challenges and opportunities’, *Comput. Secur.*, vol. 104, p. 102221, May 2021, doi: 10.1016/j.cose.2021.102221.](https://www.zotero.org/google-docs/?broken=CNTp4V)

[[23] S. Coble, ‘Cyber-Attack on Belgian Parliament’, *infosecurity-magazine*, May 05, 2021. https://www.infosecurity-magazine.com/news/cyber-attack-on-belgian-parliament/ (accessed Jun. 13, 2023).](https://www.zotero.org/google-docs/?broken=snWg1I)

[[24] O. Yoachimik, ‘Cloudflare DDoS threat report for 2022 Q4’, *Cloudflare.com*, Jan. 10, 2023. https://blog.cloudflare.com/ddos-threat-report-2022-q4/](https://www.zotero.org/google-docs/?broken=nYpi2z)

[[25] N. Kathirkamanathan, B. Thevarasa, G. Mahadevan, N. Skandhakumar, and N. Kuruwitaarachchi, ‘Prevention of DDoS Attacks Targeting Financial Services using Supervised Machine Learning and Stacked LSTM’, in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, Mumbai, India: IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/I2CT54291.2022.9825228.](https://www.zotero.org/google-docs/?broken=QOAEvw)

[[26] R. Raj and S. Singh Kang, ‘Mitigating DDoS Attack using Machine Learning Approach in SDN’, in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India: IEEE, Dec. 2022, pp. 462–467. doi: 10.1109/ICAC3N56670.2022.10074307.](https://www.zotero.org/google-docs/?broken=6HtsRu)

[[27] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, ‘XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-Based Cloud’, in *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai: IEEE, Jan. 2018, pp. 251–256. doi: 10.1109/BigComp.2018.00044.](https://www.zotero.org/google-docs/?broken=VMWTsQ)

[[28] I. M. Lopes, T. Guarda, and P. Oliveira, ‘How ISO 27001 Can Help Achieve GDPR Compliance’, in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, Coimbra, Portugal: IEEE, Jun. 2019, pp. 1–6. doi: 10.23919/CISTI.2019.8760937.](https://www.zotero.org/google-docs/?broken=cgBp3n)

[[29] J. Mohan, M. Wasserman, and V. Chidambaram, ‘Analyzing GDPR Compliance Through the Lens of Privacy Policy’, in *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, V. Gadepally, T. Mattson, M. Stonebraker, F. Wang, G. Luo, Y. Laing, and A. Dubovitskaya, Eds., in Lecture Notes in Computer Science, vol. 11721. Cham: Springer International Publishing, 2019, pp. 82–95. doi: 10.1007/978-3-030-33752-0\_6.](https://www.zotero.org/google-docs/?broken=coetfW)

[[30] ‘Data Protection Act 2018’, *Legislation*. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed Jun. 16, 2023).](https://www.zotero.org/google-docs/?broken=EyoREk)

[[31] G. Buckley, T. Caulfield, and I. Becker, ‘``It may be a pain in the backside but...’’ Insights into the resilience of business after GDPR’, 2022.](https://www.zotero.org/google-docs/?broken=uxivPJ)

[[32] ‘The Medical Devices Regulations 2002’, *legislation.gov.uk*. https://www.legislation.gov.uk/uksi/2002/618/contents/made (accessed Jun. 20, 2023).](https://www.zotero.org/google-docs/?broken=3ydsOj)

[[33] ‘Consumer Rights Act 2015’, *Legislation.gov.uk*. https://www.legislation.gov.uk/ukpga/2015/15/contents/enacted (accessed Jun. 22, 2023).](https://www.zotero.org/google-docs/?broken=h4x5ya)

[[34] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, ‘CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data’, in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan: IEEE, Jun. 2016, pp. 303–312. doi: 10.1109/ICDCS.2016.46.](https://www.zotero.org/google-docs/?broken=WJVRZ8)

[[35] J. Huang, J. Xu, X. Xing, P. Liu, and M. K. Qureshi, ‘FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware’, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas Texas USA: ACM, Oct. 2017, pp. 2231–2244. doi: 10.1145/3133956.3134035.](https://www.zotero.org/google-docs/?broken=EkiYqQ)

[[36] D. Min, Y. Ko, R. Walker, J. Lee, and Y. Kim, ‘A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense’, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 41, no. 7, pp. 2038–2051, Jul. 2022, doi: 10.1109/TCAD.2021.3099084.](https://www.zotero.org/google-docs/?broken=DnaRrT)

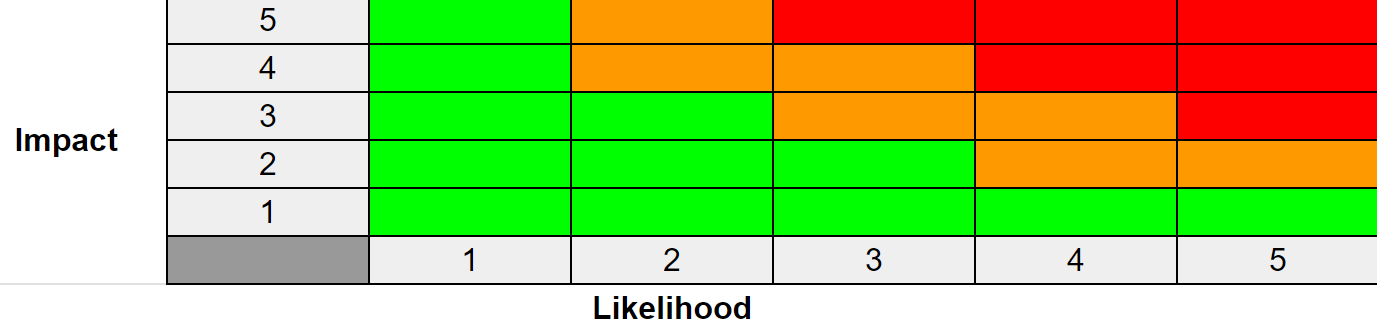
[[37] D. Dasgupta, A. Roy, and A. Nag, ‘Multi-Factor Authentication’, in *Advances in User Authentication*, in Infosys Science Foundation Series. Cham: Springer International Publishing, 2017, pp. 185–233. doi: 10.1007/978-3-319-58808-7\_5.](https://www.zotero.org/google-docs/?broken=Z9J5yt)

[[38] L. Dostalek, ‘Multi-Factor Authentication Modelling’, in *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, Ceske Budejovice, Czech Republic: IEEE, Jun. 2019, pp. 443–446. doi: 10.1109/ACITT.2019.8780068.](https://www.zotero.org/google-docs/?broken=4FsuUI)

[[39] ‘Security in the software development lifecycle’, *Redhat.com*, Sep. 30, 2022. https://www.redhat.com/en/topics/security/software-development-lifecycle-security (accessed Jun. 21, 2023).](https://www.zotero.org/google-docs/?broken=LX56XA)

[[40] L. Y. Banowosari and B. A. Gifari, ‘System Analysis and Design Using Secure Software Development Life Cycle Based On ISO 31000 and STRIDE. Case Study Mutiara Ban Workshop’, in *2019 Fourth International Conference on Informatics and Computing (ICIC)*, Semarang, Indonesia: IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/ICIC47613.2019.8985938.](https://www.zotero.org/google-docs/?broken=2rC86r)

Appendix A - Risk Appetite Matrix



*Table 3 - Risk Appetite Matrix*