**Security Management in Practice – UFCFRB-15-3**

**ISMS - Aneurin Bevan University Health Board**

A logo with blue and white text

Description automatically generated

**Table of contents**

**1.Introduction………………………………………………………………………………………….…3**

**2. Organisational context ……………………………………………………………………………4**

**3. Risk Assessment: Risk Identification…………………………………………………………7**

**4. Risk Assessment: Risk Analysis…………………………………………………………………8**

**5. Risk Assessment: Risk Evaluation……………………………………………………………12**

**6. Risk Treatment Plan……………………………………………………………………………….16**

**7. Monitoring and Communication ……………………………………………………………21**

**8. Critical analysis ………………………………………………………………………………………21**

**9. Conclusion …………………………………………………………………………………………….23**

**10. References ………………………………………………………………………………………….24**

**1.Introduction**

Aneurin Bevan University Health Board is the operational name of the local health board, which is a subsection of the NHS, covering the areas of Blaenau Gwent, Caerphilly, Monmouthshire, Newport, Torfaen and South Powys in Southeast Wales. The health board was established on the 1st of October 2009 and employs over 14,000 staff, two thirds of whom are involved in direct patient care. The health board covers over 1000 hospitals and general practise doctors consisting of 6,000 nurses, midwives, allied professionals and care workers. The health board is led by the chair, non-executive directors, the chief executive and other executive directors. The board is supported by the senior management team (Aneurin Bevan University Health Board, 2020).

Healthcare organisations are at a high risk of cyber attacks as they possess large amounts of valuable data, including sensitive patient information such as medical records, insurance details and personal identifiers. During the pandemic there were signs of a hiatus of attacks on health organisations, however this seems to have changed (Milmo, 2022).

In 2022 a ransomware attack on an NHS software supplier targeted multiple systems within the NHS including the Aneurin Bevan University Health Board. The attack caused widespread outages and effected services including patient referrals, ambulance dispatch out-of-hours appointment bookings, mental health services and emergency prescriptions (Hicks, 2022).

**2. Organisational context**

**Business objectives**

|  |  |
| --- | --- |
| Objective 1 | Improving public health and reducing health inequalities by working with  our partners to promote healthy lifestyles and ensure there is access to  preventative services, particularly for those in areas of greatest need. |
| Objective 2 | Actively engaging patients, carers and communities |
| Objective 3 | Building strong partnerships to ensure services focus on need |
| Objective 4 | Providing and commissioning services that focus on the needs of the patient, in their homes, communities and where necessary hospital settings. |
| Objective 5 | Ensuring safety, excellence and quality in all our services at all times. |
| Objective 6 | Improving the efficiency and effectiveness of our services. |
| Objective 7 | Focusing on prudent and value-based healthcare to ensure clinical value and value for money is delivered. |
| Objective 8 | Driving excellence through innovation and research which is embedded in practice. |
| Objective 9 | Trusting and supporting our staff to make the right decisions for patients and to improve care. |

(Aneurin Bevan University Health Board, 2020)

**Assets**

|  |  |
| --- | --- |
| Medical Facilities | Hospitals, clinics, medical centres |
| Medical Equipment | MRI machines, X-ray machines, surgical tools, patient monitoring devices |
| IT Assets | Servers, computers, networking devices, printers, security software’s |
| Healthcare Information Systems | Electronic Health Records (EHR), medical imaging systems, laboratory information systems |
| Pharmaceuticals | Medications, vaccines, medical supplies |
| Healthcare Professionals | Doctors, nurses, technicians, administrators |
| Partnerships and contracts | Vendor Contracts, Partnerships, healthcare providers |
| Patient Data | Personal health information, medical history, treatment plans, personal Identifiable information |

**Roles within the organisation**

|  |  |
| --- | --- |
| Chair | Provides strategic direction, ensuring effective governance, and safeguarding the organization's values. |
| Chief Executive | They oversee the overall operations, financial management, and quality of care provided by the organization. |
| Vice Chair | They coordinate activities, facilitate communication between different departments, and provide leadership in the absence of the chairperson. |
| Medical Director | Their primary role involves providing medical expertise and guidance to ensure the delivery of high-quality patient care. |
| Executive Director of Public Health and Strategic Partnerships | Entails developing and implementing policies and programs aimed at promoting public health, preventing diseases, and addressing health disparities within the community. |
| Executive Director of Nursing | They are responsible for strategic planning, policy development, budget management, staffing, and ensuring high-quality patient care. |
| Director of Workforce and Organisational Development | This role includes recruitment, training, performance management, employee engagement, and fostering a positive organizational culture. |
| Executive Director of Therapies and Health Science | This includes managing clinical departments such as physical therapy, occupational therapy, speech therapy, and other allied health services. |
| Chief Operating Officer | This includes managing various departments like facilities, patient care, and administrative services, while aligning strategies with the organization's goals. |
| Executive Director of Finance and Procurement | They manage budgeting, financial reporting, and strategic financial planning to ensure the organization's fiscal health. |
| Director of Strategy, Planning and Partnerships | They are responsible for analysing market trends, identifying growth opportunities, and formulating strategic plans to improve the organization's competitive position and financial performance. |
| Director of Digital | Oversees the implementation and management of digital technologies and strategies |
| Director of Corporate Governance | Oversees the development and implementation of policies, procedures, and practices to ensure compliance with regulatory requirements, ethical standards, and best practices. |

**Justification for ISMS**

Aneurin Bevan Health Board collects and stores a lot of sensitive patient information. Implementing an ISMS ensures the confidentiality, integrity and availability of the data, protecting patient privacy and complying with data protection regulations such as GDPR.

The availability and reliability of healthcare information systems are critical for delivering timely and effective patient care. An ISMS helps mitigate the risk of cyber threats ensuring the continuity of healthcare services.

The health board is subject to various regulatory requirements related to patient and data security. Implementing an ISMS helps demonstrate compliance with these regulations, reducing the risk of legal consequences.

Patients trust healthcare providers to safeguard their sensitive medical records. Implementing an ISMS will demonstrate a commitment to protecting patient privacy.

**3. Risk Assessment: Risk Identification**

To assist with the process of completing the risk management process an ISO 27001 ISMS information risk register was completed (see appendix item 1).

The purpose of risk identification is to recognise and document potential risks that could affect an organisation. By identifying risks strategies can be developed to mitigate, avoid or transfer these risks effectively.

The medical health record database poses a significant risk due to the sensitive and confidential nature of the information it contains, including patient health records, treatment histories and personal data. This database could be a target for cyber attacks which can compromise patient privacy. An ISMS is essential to address these risks effectively. It provides a systematic approach to managing sensitive data, identifying vulnerabilities and implementing controls to protect against unauthorised access, data loss and compliance violations.

An ISMS implements the risk management process by systematically identifying, assessing and mitigating risks to the organisation’s information assets. Initially the ISMS conduct a comprehensive risk assessment to identify potential threats, vulnerabilities and impacts to information assets. This involves analysing the organisations infrastructure, systems, processes and data to pinpoint areas of weakness or exposure. Subsequently, the ISMS evaluates the likelihood and potential impact of each identified risk to prioritise them based on their significance. Following this assessment, the ISMS devises and implements risk mitigation strategies, which may involve implementing security controls, safeguards or countermeasures to reduce risk to an acceptable level.

Risk assessments can follow a risk assessment process as seen in figure 1 below:

A diagram of a risk management process

Description automatically generated

(Aneurin Bevan University Health Board, 2024)

**4. Risk Assessment: Risk Analysis**

|  |  |  |  |
| --- | --- | --- | --- |
| Threat type | Threat | Vulnerability | Asset type |
| Data breach  (T1) | Ransomware attack:  To encrypt files containing protected health information (PHI) or lock users out of their system until a ransom is paid to the attacker. | Weak endpoint security measures  Lack of data backup | Patient Data  Healthcare Information Systems |
| Data breach  (T2) | Phishing attacks: Attackers send deceptive emails pretending to be from legitimate sources containing malicious links or asking to disclose sensitive information | Lack of multi-factor authentication  Lack of email filtering  Lack of staff training | Patient Data  Healthcare Information Systems |
| Data breach  (T3) | Denial of service (DoS) attack:  Attackers could disrupt essential services causing systems to become unresponsive | Lack of network segmentation  Lack of intrusion detection systems | Patient Data  Healthcare Information Systems |
| Data breach  (T4) | Proliferation of medical device:  Healthcare professionals use these in various settings, increasing the risk of cyber attacks | Lost or stolen devices  Lack of security audits  Lack of employee training | Patient Data  Healthcare Information Systems  Medical Facilities  Partnerships and contracts |
| Insider threat  (T5) | Malicious insider:  Intentionally misuse their access privileges to steal sensitive data, disrupt operations or sabotage systems | Individuals recruited by external threat actors.  Disgruntled employees | Healthcare Professionals  Healthcare Information Systems  Patient Data |
| Insider threat  (T6) | Negligent insider:  Inadvertently compromises security through carless or uninformed actions | Sharing credentials  Mishandling sensitive data  Lack of staff training | Healthcare Professionals  Healthcare Information Systems  Patient Data |
| Insider threat  (T7) | Compromised insider:  Have had their credentials or access privileges compromised by external threat actors | Phishing attack  Social engineering  Malware | Healthcare Professionals  Healthcare Information Systems  Patient Data |
| Exposure to cyber attacks  (T8) | Third party risks:  Dependency on third-party vendors for services increases the risk of a cyber-attack. | Inproper vendor assessment  Lack of security requirements in contracts  Lack of monitoring and oversight of third parties | Medical Equipment  Medical Facilities  Healthcare Information Systems  Patient Data |
| Exposure to cyber attacks  (T9) | Supply chain risks:  Reliance on a vast network of suppliers for various goods and services increases the risk of a cyber-attack | Inproper supplier management/assessment  Lack of security requirements  Lack of monitoring | Medical Equipment  Medical Facilities  Healthcare Information Systems  Patient Data |
| Weak authentication and access controls  (T10) | Weak authentication | Lack of password policies  Reused passwords  Default credentials.  Lack of MFA | Healthcare Professionals  Patient Data  Healthcare Information Systems |
| Weak authentication and access controls  (T11) | Weak access controls | Excessive privileges  Inadequate role-based access controls | Healthcare Professionals  Patient Data  Healthcare Information Systems |
| Human error  (T12) | Lack of security awareness and training | Lack of comprehensive training programs  Lack of role-based training.  Lack of incident reporting  Lack of regular “refresher” courses | Healthcare Professionals  Patient Data |
| Natural disaster  (T13) | Fires, floods, etc | Lack of resilient infrastructure  Lack of training and awareness  Lack of recovery plan | Medical Facilities  Medical Equipment  Patient Data |

**5. Risk Assessment: Risk Evaluation**

The scores for the risk evaluation have been calculated using the Five-point Scale for Likeness (See appendix Item 1).

|  |  |  |
| --- | --- | --- |
| Score | Likelihood | Impact |
| 0-1 | Low | Low |
| 2-3 | Medium | Medium |
| 4-5 | High | High |

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Likelihood | Impact | Reason |
| T1 | 2 | 5 | A ransomware attack takes a high level of skill meaning that there is a medium chance of it happening. However, Aneurin Bevan University Health Board experienced a ransomware attack in 2022 meaning it is at the high end of medium. The impact would be high due to the attacker potentially gaining access to the health boards medical DB. |
| T2 | 4 | 5 | Phishing attacks have a high chance of happening due to the lack of technical skills it requires to execute. The impact would be high due to the attacker potentially gaining access to the health board's medical DB. |
| T3 | 1 | 5 | A DOS attack is unlikely to happen due to the health board storing its medical records database on a selected third-party cloud platform. However, the impact of a DOS attack would be high. |
| T4 | 1 | 4 | Although unlikely due to the high skill required, the proliferation of medical devices such as wearable devices and sensors in healthcare raises cyber security issues. The impact of this would be high. |
| T5 | 1 | 4 | Although it is an unlikely scenario to have a malicious insider within a healthcare organisation the impact would be high due to the worker having access to sensitive information and the medical DB |
| T6 | 3 | 4 | There is a medium risk of having a negligent insider within the health board due to a potential lack of training or the mishandling of sensitive data. The impact of this risk would be high due to sensitive information being misused. |
| T7 | 3 | 5 | There is a medium risk of having a compromised insider within an organisation due to the likelihood a phishing attack could occur. The impact of this risk would be high. |
| T8 | 1 | 4 | The likelihood of this risk would be low due to the health board selecting a trusted third-party vendor. The impact of the risk would be high due to an attacker potentially gaining sensitive information. |
| T9 | 1 | 4 | The likelihood of this risk would be low due to the health board selecting trusted vendors within the supply chain. The impact of the risk would be high due to an attacker potentially gaining sensitive information. |
| T10 | 2 | 5 | There is a medium likelihood of this risk occurring due to some people in the organisation having weak passwords or still using their default credentials. The impact of the risk would be high due to an attacker gaining access to the health boards system |
| T11 | 3 | 5 | The likelihood of this risk is high due to the information an attacker could steal however there is a high level of skill required to elevate a user’s privilege. The impact of this risk would be high due to the attacker gaining elevated privileges and having access to the health boards DB |
| T12 | 3 | 3 | A lack of security awareness and training has a medium likeness as some members of staff would have little cyber security knowledge. The impact of the risk would be medium due to the chance this would lead to a cyber attack |
| T13 | 1 | 3 | A natural disaster such as a flood or a fire is quite unlikely to happen. It would however have a high financial loss because of the damage to infrastructure it would cause meaning the impact of the risk would be medium. |

**6. Risk Treatment Plan**

The scores for the risk treatment plan have been calculated using the table for Acceptance Criteria (See appendix item 2). Any risk that falls within green would be considered acceptable whereas any risk that falls outside the green would require treatment.

|  |  |
| --- | --- |
| Tolerate (1-3) | Accept the risk with no further action |
| Treat (4-10) | Take action to reduce likelihood or impact |
| Transfer (9-15) | Pass the risk to someone else, for example by outsourcing to a third-party or purchasing insurance to mitigate the risk |
| Terminate (16-25) | Stop performing the activity that results in the risk |

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Control | ISO 27001 Control | Risk treatment |
| T1 | Regular backups- set up automated regular backups of all system files.  Access controls- implement strict access controls to limit who can access PHI and critical system files. | A.6  A.16.1  A.12.2  A.13  A.18.1 | Transfer |
| T2 | Employee training- conduct regular phishing awareness training sessions for employees. These sessions would include simulated phishing attacks. | A.6  A.8.2.3  A.9.2  A.13.2 | Terminate |
| T3 | Traffic monitoring- deploy intrusion detection systems to monitor network traffic and detect DoS attacks. | A.6  A.12.6  A.12.7  A.13.1 | Treat |
| T4 | Inventory management- establish an inventory of all medical devices connected to the network. Monitor the lifecycle of medical devices including procurement, deployment, maintenance and decommissioning. | A.8.1.1  A.8.1.2  A.9.1.2  A.9.4  A.12.6  A.16.1 | Treat |
| T5 | User activity monitoring- deploy user activity monitoring solutions to track employees’ actions within the health boards IT systems | A.7.1.1  A.7.2.2  A.7.3.1  A.9.2.1  A.9.2.3  A.12.4  A.12.5  A.16.1 | Treat |
| T6 | Role-based access control: implement to ensure that employees only have access to the level of access required to perform their job functions. | A.7.2.1  A.8.1.3  A.9.2.2  A.12.5  A.7.2.3 | Transfer |
| T7 | User behaviour analytics- use user behaviour analytics to identify deviations from normal behaviour and flag potentially compromised accounts for further investigation. | A.9.4  A.12.4  A.12.5  A.16.1  A.7.2 | Transfer |
| T8 | Contractual agreements- include specific cybersecurity requirements and expectations in vendor contracts and service level agreements. Define minimum security standards, data protection measures and incident response procedures | A.6.1.5  A.15.1  A.12.1  A.12.6  A.18.1  A.16.1 | Treat |
| T9 | Contractual agreements- include specific cybersecurity requirements and expectations in vendor contracts and service level agreements. Define minimum security standards, data protection measures and incident response procedures | A.6.1.5  A.15.1  A.18.1  A.12.1  A.12.6  A.16.1 | Treat |
| T10 | Password policies- enforce strong password policies to ensure that staff create a complex and unique password. | A.9.1.1  A.9.2.1  A.9.2.3  A.13.2.1  A.12.4  A.12.6  A.16.1 | Transfer |
| T11 | Principle of least privilege- only grant users the minimum level of access necessary to perform their job functions | A.9.1  A.9.2  A.9.4  A.12.4  A.12.6  A.16.1 | Transfer |
| T12 | Security awareness training program- develop a training program tailored to the organisation’s specific security risks.  Role based training- customise security awareness training specific for the roles of different employees within the organisation. | A.7.2  A.7.2.2  A.16.1  A.18.2  A.9.2.3 | Transfer |
| T13 | Emergency response planning- develop emergency response procedures that outline the steps to take in the event of a natural disaster.  Physical security measures- implement physical security measures to protect facilities and assets from damage caused by natural disasters | A.11.1  A.14.1  A.17.1  A.17.2  A.18.1 | Tolerate |

**7. Monitoring and Communication**

Effective monitoring of an Information Security Management System (ISMS) can be ensured by implementing a structured approach that encompasses continuous assessment and active engagement throughout the organisation. This involves establishing clear roles and responsibilities for monitoring activities, including regular audits, vulnerability assessments and compliance checks. Automated tools can be used to allow data collection and analysis, enabling real time monitoring of key security indicators. Regular reviews of security policies and procedures ensure alignment with industry awareness and accountability through training programs communication channels encourages staff participation in monitoring efforts. By integrating monitoring into daily operations and leveraging technology and human resources effectively, the health board can maintain safeguarding sensitive information and mitigating security risks.

In the event of an incident, the health board will undertake a series of measures aimed at minimising impact. This will include activating an incident response team composed of key personnel from various departments to assess the situation and coordinate a timely response. Immediate steps may involve containing the incident, preserving evidence and notifying relevant stakeholders such as affected individuals, regulatory authorities and law enforcement, in compliance with legal and regulatory requirements. Concurrently the health board will initiate efforts to mitigate further damage, restore affected systems and data and implement controls to prevent a similar incident from recurring. Post-incident analysis and documentation are crucial for identifying root causes, evaluating response effectiveness and refining incident response procedures for future incidents. Additionally, communication strategies are essential to maintain transparency, manage stakeholder expectations and rebuild trust in the health board’s ability to address security concerns.

**8. Critical analysis**

The first step of this ISMS process was to establish a brief outline of the organisation selected for the report. This included the organisations objectives, assets, roles that exists and also to justify why an ISMS would be important. This led to a more comprehensive understanding of the organisation, making the later stages of the report seem more achievable.

Using the risk management process, I initially identified and described a variety of risks relevant to the organisation. Given the inherent multitude of risks associated with any health board, this task proved challenging. Consequently, it became important for the report to focus on the most significant risks in depth. The application of the Five-Point Scale for Likelihood proved valuable, enabling the grading of each risk on a scale from 1 to 5 based on both likelihood and impact. This process was crucial in aiding the last stage of the risk management process which is mitigation. By consolidating the scores from the Likelihood Scale, I established acceptance criteria for each risk, thus formulating a risk treatment plan for the organisation. Furthermore, consulting ISO 27001 for relevant controls was essential in determining how to appropriately manage each risk.

If I have an opportunity to complete a similar piece of work, I will certainly leave more time to complete more extensive research on the organisation to allow for a more comprehensive understanding of the associated risks. Although I do believe the risks, I identified were relevant to the organisation, they are slightly vague. I am convinced that conducting further research would have unearthed more pertinent risks specifically tailored to the needs of the health board.

**9. Conclusion**

The completion of this report has underscored the importance of an ISMS report. It offers a structured framework for managing and safeguarding sensitive information, aiding in the identification, assessment and mitigation of information security risks. This is particularly crucial for organisations like the Aneurin Bevan University Health Board, which handle large volumes of sensitive patient data. The preservation of confidentiality, integrity and availability of such data is especially important. Moreover, the recent cyber-attack targeting the organisation likely reduced trust in its security measures. Therefore, completing an ISMS can play a pivotal role in restoring any lost trust by demonstrating a commitment to enhancing information security practises.

**10. References**

‘Aneurin Bevan.png’ (2022) *Digital Health and Care Wales*. 17 August 2022 [online]. Available from: https://dhcw.nhs.wales/images/national-data-resource-ndr/aneurin-bevanpng/ [Accessed 6 May 2024].

Aneurin Bevan University Health Board (2020) *Board Assurance Framework*. March 2020 [online]. Available from: https://abuhb.nhs.wales/files/key-documents/governance-and-assurance/board-assurance-framework-pdf/ [Accessed 28 March 2024].

Aneurin Bevan University Health Board (2020) *Home - Aneurin Bevan University Health Board* *Nhs.wales*. 2020 [online]. Available from: https://abuhb.nhs.wales/ [Accessed 28 March 2024].

Aneurin Bevan University Health Board (2024) *Risk Management Framework*. 25 January 2024 [online]. Available from: https://abuhb.nhs.wales/files/key-documents/risk-management/risk-management-framework-pdf/ [Accessed 28 March 2024].

Calder, A. (2023) *ISO 27001/ISO 27002 - A guide to information security management systems*. IT Governance Ltd.

Hicks, T. (2022) *Aneurin Bevan Health board warns no quick fix to cyber attack* *Caerphilly Observer*. 12 September 2022 [online]. Available from: https://caerphilly.observer/news/1012105/nhs-cyber-attack-aneurin-bevan-health-board/ [Accessed 28 March 2024].

Milmo, D. (2022) *NHS ransomware attack: what happened and how bad is it?* *the Guardian*. 11 August 2022 [online]. Available from: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it [Accessed 28 March 2024].

**Appendix**

**Item 1:**

[ISO27k\_ISMS\_Information\_risk\_register Samuel James.xlsm (sharepoint.com)](https://uweacuk-my.sharepoint.com/:x:/r/personal/samuel5_james_live_uwe_ac_uk/_layouts/15/Doc.aspx?sourcedoc=%7B8EC4449D-BF90-4BB1-9342-F83AE976031C%7D&file=ISO27k_ISMS_Information_risk_register%20Samuel%20James.xlsm&action=default&mobileredirect=true)

**Item 2:**

A table with numbers and text

Description automatically generated

(Calder, 2023)

**Item 3:**

A table of numbers and their names

Description automatically generated with medium confidence

(Calder, 2023)