

## Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

**To be completed by the student(s) prior to final submission:**

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	2286790
----------------------------------	---------

**To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:**

<b>Date set</b>	11/12/2022
<b>Submission date (excluding extensions)</b>	by 12:00pm (UK time)
<b>Submission guidance</b>	To be submitted electronically via Tabula
<b>Late submission policy</b>	<p>If work is submitted late, penalties will be applied at the rate of <b>5 marks per University working day</b> after the due date, up to a <b>maximum of 10 working days</b> late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means <b>after the submission deadline time as well as the date</b> – work submitted after the given time even on the same day is counted as 1 day late.</p> <p>For <b>Postgraduate</b> students only, who started their <b>current course before 1 August 2019</b>, the daily penalty is <b>3 marks</b> rather than 5.</p>

<b>Resubmission policy</b>	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

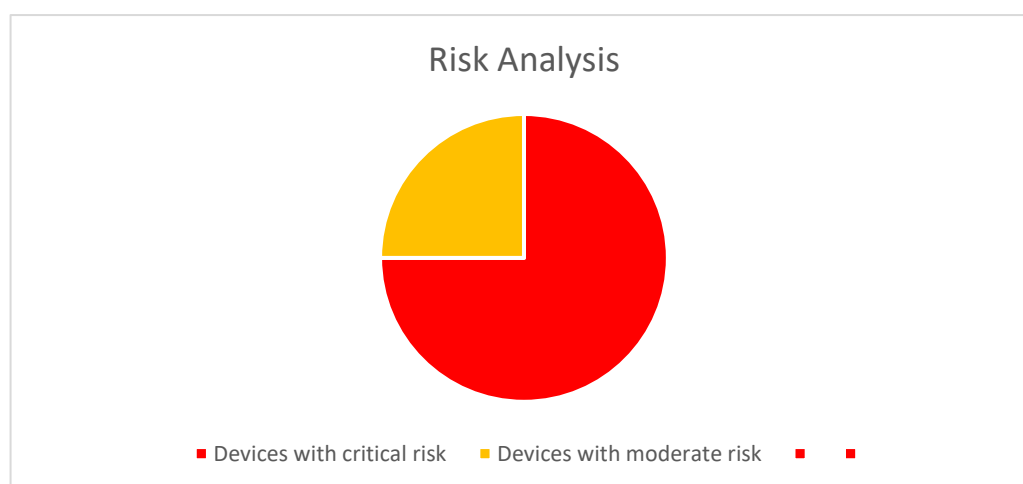
To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

<b>Module title &amp; code</b>	Managing Cyber Risk, Audit and Compliance (WM9C4-15)
<b>Module owner</b>	HS Lallie
<b>Module tutor</b>	HS Lallie
<b>Assessment type</b>	HS Lallie
<b>Weighting of mark</b>	100%

<b>Executive Summary .....</b>	<b>4</b>
<b>Background .....</b>	<b>4</b>
<b>Scope.....</b>	<b>4</b>
<b>Risk Standards Used.....</b>	<b>5</b>
<b>Risk, Threat and Vulnerability Analysis .....</b>	<b>6</b>
<b>Risk Mitigation Strategy .....</b>	<b>10</b>
<b>IOMT Device Management Lifecycle .....</b>	<b>10</b>
<b>Recommendations .....</b>	<b>11</b>
<b>Appendices.....</b>	<b>12</b>

## Executive Summary

Healthcare.com says that The WannaCry global ransomware attack that hit 595 GP practices and 80 hospital trusts in England was an eyeopener for all the healthcare service providers under the NHS in 2017. Although Remote Patient Monitoring and Treatment are both possible for doctors because of smart medical devices, but there is always a possibility of the devices being vulnerable to a cyber-attack, and if GDPR (General Data Protection Regulation) compliance is not achieved, the loss anticipated for data loss could reach 17.5 million pounds, or 4% of annual revenue and higher if there is a casualty. This can be avoided by an initial investment of Two Million Eight Hundred Eighty-Seven Thousand Pounds. If the hospital does not take measures accordingly, there is a good chance of cyber-attack happening soon.



## Background

This security risk assessment is being performed after the NHS's notification about the amendment of the NHS Digital Clinical Safety standard (DCB0160) for additional requirement of Cyber Security for the IOMT devices. The hospital is more than 12 years old, and this is the first audit that has ever been performed. The hospital makes extensive use of IoMT devices, and a technology specialist in each department has the freedom to select and purchase these devices according to the needs of the department. The hospital is at level 1 **Ad hoc security maturity** as the maintenance and supply is the responsibility of individual in every department. Refer Appendix 1 for more information.

## Scope

The complete security management of IOMT devices used in the hospital and are listed below in table 2 is covered by this assessment.

The scope of this risk assessment is limited to:

- Applicable Standards and framework used to estimate the risks
- Risk analysis (Risk Matrix and Risk Register) with an IOMT device management cycle.
- Methods of mitigating the risks related to these medical devices.
- Recommendations for the hospital for the continued use of the medical devices

## Risk Standards Used

Standards	Description
<b>ISO/IEC 27001</b>	This international standard uses a risk-based approach to manage information security. It offers instructions on how to recognise, evaluate, and control risks to information security. It promotes patient safety, the protection of personal information, and compliance with applicable laws and regulations. <sup>1</sup>
<b>The UK's National Cyber Security Centre (NCSC) Cyber Security Standard</b>	Its objectives include managing a security risk, preventing cyberattacks, detecting cyber security events, responding to attacks, and recovering from them. It can be used by the organisation itself or by an external third party. It provides instructions for designing, creating, running, and maintaining medical IoT networks and devices in a secure manner. <sup>2</sup>
<b>NIST SP 800-30</b>	It provides guidance step-bystep for Risk framing, risk assessment, risk response, and risk monitoring for the risk management processes. It also provides different approaches for risk analysis of appropriate risk assessment methods based on organisation's need and resources. <sup>3</sup>
<b>ISO/IEC 27005</b>	ISO/IEC 27005 is a risk management standard that provides guidance for the implementation of an information security management system (ISMS) based on ISO/IEC 27001. It outlines how to identify and assess risks and to provide direction for developing a risk management plan. <sup>4</sup>
<b>OCTAVE</b>	OCTAVE as this method provides a process complete with guidelines, and process. It is an open qualitative method which can be used by small teams in large organizations. OCTAVE covers physical and cyber security. It offers a complete set of procedures for evaluating the networks and IT systems security of an organisation. <sup>5</sup>

*Table 1 Table of Suitable Standards*

Since this is the first audit in 12 years, no earlier records can be consulted. Also, as the hospital stated that these IOMT devices are of high value for them as they make, they can monitor and diagnose patients effectively and remotely, so the main purpose of this risk assessment is to analyse, prioritise, and mitigate all the risks the IOT systems possess accordingly.

The UK's NCSC Cyber Security Standard provides guidance about risk management, controls and incident response. In short, it provides and measures and controls to identity threats and protect the systems from a cyber-attack. It is not just specific to IOT devices, it provides baseline measures and does not specifically work

<sup>1</sup> ISO. (2022). ISO/IEC 27001 and related standards — Information security management. [online] Available at: <https://www.iso.org/isoiec-27001-information-security.html>

<sup>2</sup> Ncsc.gov.uk. (2022). CAF - Principles and guidance. [online] Available at: <https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance>

<sup>3</sup> Blank, R. and Gallagher, P. (2012). *Guide for Conducting Risk Assessments NIST Special Publication 800-30* [online] Available at: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>.

<sup>4</sup> for, O. (2022). ISO/IEC 27005:2022. [online] ISO. Available at: <https://www.iso.org/standard/80585.html>

<sup>5</sup> Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003). *Introduction to the OCTAVE ® Approach*. [online] Available at: <https://www.itgovernance.co.uk/files/Octave.pdf>.

with streamlined scope (like IOMT devices) . Also, the standard is relatively new and is upgraded frequently, so the hospital will have to keep up with the latest advances.

OCTAVE on the other hand can be useful when the evaluation of physical security of the information systems is concerned. It provides guidance about policies and procedures for asset management, personnel security, and physical security. Also, it is useful for small organisations, but here the hospital has more than 12000 employees.

Furthermore, NIST SP 800-30 and ISO 27001 are two of the most widely used standards for information security risk management.

ISO 27001 provides us with frameworks for establishing, implementing, and managing the IT security. It also focusses more on organisation's security, so the scope is huge, but for this audit the scope is limited.

Also implementing ISO 27001 or ISO 27005 will be time-consuming and the standard is complex, so it will be difficult to maintain.

Finally, NIST SP 800-30 provides in detail guidance for performing a risk assessment, which is the main aim of this audit and will be followed throughout the report. Moreover, NIST SP 800-30 can be used in this situation because it places strong emphasis on evaluating the risks related to malicious actors, data security and privacy, and device vulnerabilities rather than controls and incident response. In addition to lowering the risk, it can be used to create a proper security controls and defences.

### Risk, Threat and Vulnerability Analysis

Serial Number	List of Assets (Software)	CVE ID	Version	Vulnerability	Threats
S1	Welch Allyn Service Tool	CVE-2021-27408 CVE-2021-27408	1	1. Out-of-bounds write 2. Out-of-bounds read	<ul style="list-style-type: none"> <li>• Device Impersonation (Node Cloning)</li> <li>• Data Eavesdropping</li> <li>• Device Failure</li> <li>• Malicious Input</li> </ul>
S2	Welch Allyn Connex Central Station (CS) v1.1		1.1		
S3	Philips Healthcare Tasy Electronic Medical Record (EMR) 3.06	CVE-2021-39376	3.06	1. SQL Injection	<ul style="list-style-type: none"> <li>• Data Tampering</li> <li>• Insecure API</li> <li>• Sensitive Information</li> <li>• Medical Device Tracking</li> </ul>
S4	Synaptive Medical Clear Canvas ImageServer 3.0	CVE-2022-8788	3	1. Cross -Side Scripting Vulnerability	<ul style="list-style-type: none"> <li>• Malicious Input</li> <li>• Device Tampering</li> </ul>
S5	Clinic's Patient Management System v1.0	CVE-2022-35117	1	1. SQL Injection	<ul style="list-style-type: none"> <li>• Side – Channel Attack</li> <li>• Device Tracking</li> <li>• Device Type Determination</li> <li>• Data Tampering and Modification</li> <li>• Replay Attack</li> </ul>
S6	Source Codester Medical Hub Directory Site 1.0	CVE-2022-28533	1	1. SQL Injection	<ul style="list-style-type: none"> <li>• Malicious Input</li> <li>• Device Failure/ Malfunctioning</li> <li>• Device Tampering</li> </ul>
S7	Source Codester Electronic Medical Records System	CVE-2022-2676	N/A	1. SQL Injection	<ul style="list-style-type: none"> <li>• Sensitive Data Exposure</li> <li>• Running Malicious Scripting</li> <li>• Tampering Medical Records</li> </ul>
S8	Medical Store Management System v1.0	CVE-2022-25394	1	1. SQL Injection	<ul style="list-style-type: none"> <li>• Device Failure</li> <li>• Corrupting the system</li> <li>• Loss of access to the system</li> </ul>

Code	List of Assets (Hardware)	CVE ID	Versions	Vulnerability	Threats
H1	Hamilton Medical AG,T1-Ventillator	CVE-2020-27282 CVE-2020-27278 CVE-2020-27290	2.2.3	1. Hard – coded credentials 2. XML validation vulnerability 3. Systems fails to thoroughly verify checksums for configuration logs.	<ul style="list-style-type: none"> <li>• Network Compromise</li> <li>• Device Failure</li> <li>• Data Tampering</li> <li>• Insecure API</li> <li>• Loss of Life</li> </ul>
H2	Baxter PrismaFlex	CVE-2020-12035 CVE-2020-12036 CVE-2020-12037	2	1. No Encryption during Data Transmission 2. No Authentication required during Data Transmission 3. Hard – coded credentials used	<ul style="list-style-type: none"> <li>• Man-in-the-Middle</li> <li>• SQL Injection</li> <li>• XSS Injection</li> <li>• User Impersonation</li> </ul>
H3	Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	CVE-2017-12725 CVE-2017-12722 CVE-2017-12718 CVE-2017-12720 CVE-2017-12724 CVE-2017-12721 CVE-2017-12723	1.1 1.5 1.6	1. Buffer Copy without checking the input size 2. Out of bound read 3. Hard - Coded credentials used for FTP server 4. Improper Access Control 5. Hard - Coded credentials used for default network configuration 6. Hard - Coded password used for Telnet 7. Improper Certificate Validation 8. Password is stored in config files by the pump	<ul style="list-style-type: none"> <li>• Device Failure</li> <li>• DDOS</li> <li>• Log Deletion</li> <li>• Battery Drain Attack</li> <li>• Device Tampering</li> <li>• User Impersonation</li> <li>• Network Compromise</li> </ul>
H4	Medtronic Paradigm wireless insulin pump	CVE-2019-10964	512 522 712 722	1. Improper Access Control	<ul style="list-style-type: none"> <li>• Replay Attack</li> <li>• Injection Attack</li> <li>• Modification of Data</li> <li>• Sealing Information</li> <li>• Network Compromise</li> </ul>

Table 2 Vulnerability and Threat<sup>6</sup>

<sup>6</sup> <sup>6</sup> Nist.gov. (2022). *NVD - Home*. [online] Available at: <https://nvd.nist.gov/>.

Device Number	Risks	Risk Narrative	Threat Actor	Mitigation	Likelihood	Impact	Risk Seviorty	Recommendations	Cost Benefit Analysis
S1	<ul style="list-style-type: none"> <li>Information Disclosure</li> <li>Loss of Reputation</li> </ul>	A threat actor can remotely chain the out of bound write vulnerability with arbitrary code execution and can cause information leakage.	<ul style="list-style-type: none"> <li>Cyber-Criminal</li> <li>Hacktivists</li> </ul>	<ul style="list-style-type: none"> <li>Update to the newest version.</li> </ul>	Moderate	Moderate		<ul style="list-style-type: none"> <li>Input Validation (Create a accept or reject list)</li> <li>Use a language that provides appropriate memory abstractions</li> </ul>	<ul style="list-style-type: none"> <li>Update is free.</li> <li>Accept List needs no money.</li> </ul>
S2									
S3	<ul style="list-style-type: none"> <li>Information Disclosure</li> <li>Loss of Reputation</li> </ul>	A threat actor can remotely add SQL query as input to be interpreted as ordinary user data or send malicious payload to get into the system.	<ul style="list-style-type: none"> <li>Cyber-Criminal</li> <li>Hacktivists</li> </ul>	<ul style="list-style-type: none"> <li>Update to the latest version</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Using persistence layers such as Hibernate of Enterprise, Java Net Beans against SQL injection.</li> <li>Parameterisation between code and data</li> <li>Use strict allow list</li> </ul>	<ul style="list-style-type: none"> <li>Update is free.</li> <li>Hibernate of Enterprise Java is free (open source)</li> </ul>
S4	<ul style="list-style-type: none"> <li>Loss of Integrity</li> <li>Loss of Reputation</li> <li>Loss of Access Control</li> </ul>	The threat actor can perform an XSS attack and send malicious request to a website on behalf of the victims (Pretend to be Users)	<ul style="list-style-type: none"> <li>Cyber-Criminal</li> <li>Hacktivists</li> </ul>	<ul style="list-style-type: none"> <li>Patch Management required</li> <li>To mitigate XSS against session cookie, set it to Httponly.</li> <li>Using firewalls</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Use frameworks like Microsoft's Anti XSS library, OWASP ESAPI module, encoding wicket.</li> </ul>	<ul style="list-style-type: none"> <li>Microsoft Anti XSS and OSASP ESAPI are <b>free</b>.</li> <li>Hiring Professional may cost 30000£ x 5 professionals = 1500000£.</li> </ul>
S5	<ul style="list-style-type: none"> <li>Loss of Sensitive Data</li> <li>Loss of Reputation</li> </ul>	The threat actor, in some circumstances can run arbitrary code on the database and compromise all the data or maybe even sell it.	<ul style="list-style-type: none"> <li>Cyber-Criminals</li> <li>Hacktivists</li> </ul>	<ul style="list-style-type: none"> <li>Firewall</li> <li>Input Encoding</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Use vetted library</li> <li>For security checks on the client side, perform a check on server side.</li> </ul>	<ul style="list-style-type: none"> <li>2 CISCO firewall can be 500£ x 2 = 1000£.</li> <li>Vetted Library needs no money.</li> </ul>
S6	<ul style="list-style-type: none"> <li>Loss of Sensitive Information</li> </ul>	The threat actor can send malicious payload over the network and access confidential Information.	<ul style="list-style-type: none"> <li>Cyber-Criminals</li> <li>Hacktivists</li> </ul>	<ul style="list-style-type: none"> <li>Create isolated accounts with limited privileges that are only used for a single task.</li> <li>Output Encoding</li> <li>Firewall</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Fuzz tester for automatic dynamic analysis</li> <li>Database scanners</li> <li>Create a DMZ for devices and services that deal with sensitive information.</li> <li>Input Validation</li> </ul>	<ul style="list-style-type: none"> <li>DMZ feature is available with CISCO firewall appliance.</li> <li>Run Zero is a free database scanner.</li> </ul>
S7	<ul style="list-style-type: none"> <li>Loss of Access Control</li> </ul>								
S8	<ul style="list-style-type: none"> <li>Loss of Reputation</li> </ul>								



Table 4 Risk Register for Hardware

Device Number	Risks	Risk Narrative	Threat Actor	Mitigation	Likelihood	Impact	Risk Seviarity	Recommendations	Cost Benefit Analysis
H1	<ul style="list-style-type: none"> <li>Loss of Life</li> <li>Loss of Reputation</li> <li>Device Failure</li> </ul>	A threat actor can remotely extract sensitive information and cause a DOS attack, and this can affect patient's life.	Cyber-Criminal Hacktivists Insider Threat	<ul style="list-style-type: none"> <li>Input Validation</li> <li>VPN</li> <li>Necessary updates</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Increase the physical Security</li> <li>Grant Limited access to the device</li> <li>Monitor the Notification, alerts</li> </ul>	<ul style="list-style-type: none"> <li>Update is free.</li> <li>Physical Security may cost 26000£ x 10 personnel = 260000£</li> </ul>
H2	<ul style="list-style-type: none"> <li>Loss of Reputation</li> <li>Device Failure</li> </ul>	A threat actor can observe, modify, and change the sensitive information along with the device settings resulting in device failures.	Cyber-Criminal Hacktivists Insider Threat	<ul style="list-style-type: none"> <li>Upgrade to PrisMaxv3</li> <li>Network segmentation</li> </ul>	Moderate	Moderate		<ul style="list-style-type: none"> <li>Limiting inbound and outbound connection</li> <li>Password Policy</li> <li>Network Segmentation</li> <li>Training and Awareness</li> </ul>	<ul style="list-style-type: none"> <li>Training can cost 20£ x 12000 employees = 240000£</li> </ul>
H3	<ul style="list-style-type: none"> <li>Loss of Life</li> <li>Loss of Reputation</li> <li>Device Failure</li> <li>Loss of Data</li> </ul>	A threat actor can remotely gain unauthorised access and disrupt the pump's intended operation that can affect patients' life.	Cyber-Criminal Hacktivists Insider Threat	<ul style="list-style-type: none"> <li>Assign IP addresses</li> <li>Keep an eye out for rogue DNS and DHCP servers on your network.</li> <li>VLAN or VPN</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Password Policy</li> <li>Access to medical personnel only</li> <li>Unused ports can be closed</li> <li>Micro-segmentation of network</li> <li>Firewall</li> </ul>	<ul style="list-style-type: none"> <li>Network Monitoring can be done with Firewall.</li> </ul>
H4	<ul style="list-style-type: none"> <li>Loss of Life</li> <li>Loss of Reputation</li> <li>Loss of Access Control</li> </ul>	A threat actor can gain access to one of the affected insulin pump models and inject, replay, modify, and/or intercept data, as well as change pump settings and control insulin delivery.	Cyber-Criminal Hacktivists Insider Threat	<ul style="list-style-type: none"> <li>Change all the models with these specifications with the latest variant.</li> </ul>	High	High		<ul style="list-style-type: none"> <li>Increase physical security</li> <li>Disconnect devices when not in use</li> <li>Monitor all the notifications, alerts</li> </ul>	<ul style="list-style-type: none"> <li>Cost of new Insulin Pump = 2000£ x 1118 pumps = 2,236,000£.</li> </ul>

Qualitative Analysis values can be: High &gt; Moderate &gt; Low

COLOUR TABLE				
		SEVERITY (IMPACT)		
		LOW	MODERATE	HIGH
LIKELIHOOD	HIGH			
	MODERATE			
	LOW			

Table 5 Colour Table




	Critical Risk. Must be <b>treated</b> Immediately. Impact can cease the main functionality of the hospital.
	Important Risk. Must be <b>treated</b> as soon as possible. This risk can be accepted with regular monitoring.
	Considerable Risk. This kind of risk can be <b>transferred</b> and can be treated eventually according to the finance.

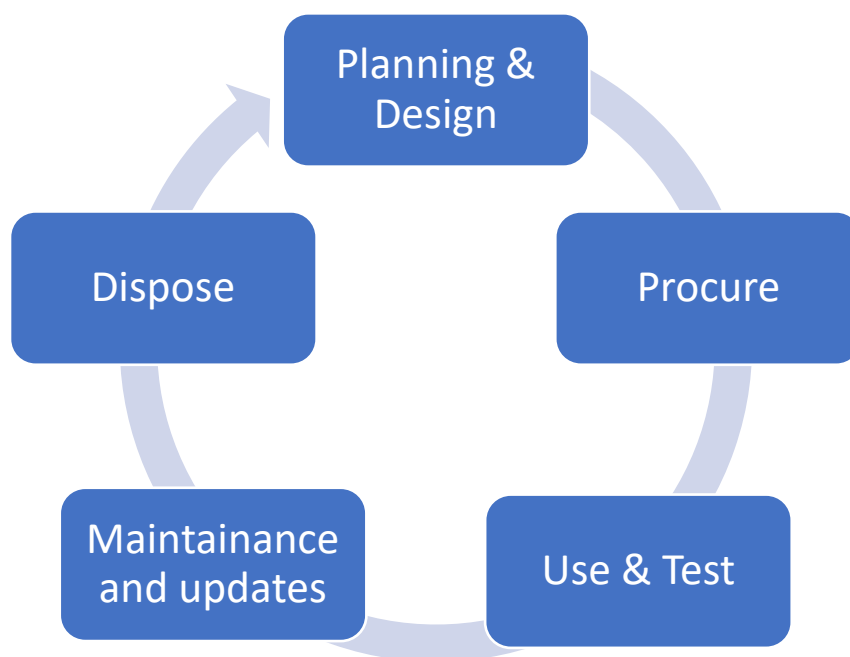
Table 6 Risk Matrix Explanation

## Risk Mitigation Strategy

The Risk Register Concludes that there are 9 severe risks and three moderate risks. The total amount that is needed to mitigate all the risks will be **2,887,000 £** (Two Million Eight Hundred Eighty-Seven Thousand Pounds). Accepting and implementing the recommendations and mitigations is an initial, significant investment that will guarantee there is no disruption of primary services while also strictly adhering with frameworks and policies to avoid significant fines like 17.4 million pounds or 4% of annual income, whichever is larger, if GDPR compliance is not achieved.

The hospital must prioritise the mitigations and recommendations suggested for all the devices which are critical and marked Red. The loss predicted after an attack is huge, so these risks must be treated immediately within 3 months. And after that work on the moderate risks in the coming 6 months. Proper recommendations for all the controls to reduce risks are provided below in recommendations.

## IOMT Device Management Lifecycle



- **Planning & Design:** Plan the IOMT device according to the required specifications.
- **Procure:** Order sufficient IOMT devices for the smooth operation of hospital.
- **Use & Test:** Use and test the devices against possible cyber-attacks.
- **Maintenance and Update:** Regular Patch Management and updates must be ensured.
- **Dispose:** After a certain period replace or dispose the device.

## Recommendations

To ensure efficient operation, the hospital needs to follow these suggestions apart from those that are mentioned above specifically for each device in the risk register:

Recommended Controls	Description
➤ <b>Network</b>	<ul style="list-style-type: none"> <li>➤ Firewall along with Network Intrusion Detection System must be deployed.</li> <li>➤ DMZ (Network Segmentation) must be created to secure and isolate the network used by IOMT devices.</li> <li>➤ Backup and Maintenance must be monitored by the cyber team.</li> <li>➤ Encryption software, patch management must be done regularly.</li> </ul>
➤ <b>Access</b>	<ul style="list-style-type: none"> <li>➤ Environment Hardening by using lowest privilege and least access required to do the tasks.</li> <li>➤ Audit Logs for authorised changes.</li> </ul>
➤ <b>Authentication</b>	<ul style="list-style-type: none"> <li>➤ Password Policies must be maintained.</li> <li>➤ Multi-Factor Authentication must be used.</li> <li>➤ Biometrics access will provide better security.</li> </ul>
➤ <b>Encryption</b>	<ul style="list-style-type: none"> <li>➤ Password must be hashed and salted and must be stored in different database for increased security.</li> <li>➤ <b>SSL</b> and <b>TLS</b> protocols must be used between client and server.</li> </ul>
➤ <b>Errors</b>	<ul style="list-style-type: none"> <li>➤ Ensure the generic errors encountered by a network is displayed.</li> </ul>
➤ <b>Software</b>	<ul style="list-style-type: none"> <li>➤ Anti- Malwares like Malwarebytes can be used which provides protection against malwares.</li> <li>➤ Auto updates of the IOMT devices.</li> </ul>
➤ <b>Cyber Security training and Awareness for the staff</b>	<ul style="list-style-type: none"> <li>➤ Introduce Cyber Security procedures since the recruitment process.</li> <li>➤ Regular Cyber Security Briefing.</li> <li>➤ Live Fire training exercises and simulations can help them be more aware of a cyber-attack.</li> <li>➤ Written or Verbal commitment can be done mandatory to avoid Unintentional or intentional 'Insider threat'.</li> </ul>
➤ <b>Physical</b>	<ul style="list-style-type: none"> <li>➤ Data and Physical Access can be provided according to the governance of the hospital after biometric check.</li> <li>➤ 24-hours physical surveillance around the IOMT devices.</li> </ul>

Table 7 Table of Recommendations

## Appendices

### Glossary

- **Ad-hoc security Maturity - Level 1** – Processes for information security may be unstructured and disorganised. Success is not thought to be repeatable or scalable and is likely to depend on individualised efforts. This is due to the fact that processes would not be sufficiently outlined and documented to permit replication.
- **SSL and TLS** – These are transport layer and secure socket layer protocols which allows establishing encrypted data transfers between clients and server.
- **IOMT (Internet Of Medical Things)** – These are smart devices which are used to monitor the patients' health remotely.