A close up of a logo

Description automatically generated

**FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI**

**GROUP 7**

**PROJECT**

**BITS3523 – COMPUTER AUDIT AND RISK MANAGEMENT**

**LECTURER:**

**TS. DR. S.M. WARUSIA MOHAMED BIN S.M.M YASSIN**

**PREPARED BY:**

|  |  |
| --- | --- |
| **NAME** | **NO MATRIC** |
| Suriya A/L Meehondelan | B032110079 |
| Meera Sri A/P Radhakrishnan | B032110292 |
| Fatin Nasuha Binti Mohamed Sabir | B032110289 |
| Siti Aisyah Binti Faizal | B032110155 |
| Ahmad Azri Bin Nasharudin | B032110327 |
| Ahmad Akmal Haziq Bin Zulkifli | B032220002 |

Table of Contents

[**CHAPTER 1: INTRODUCTION** 1](#_Toc170063119)

[1.1 Introduction 1](#_Toc170063120)

[1.2 Company Background 1](#_Toc170063121)

[1.4 Project Objectives 3](#_Toc170063122)

[1.5 Management Risk Organizational Chart 5](#_Toc170063123)

[1.5.1 Organization Role and Description 6](#_Toc170063124)

[1.6 Project Description / Network Diagram 10](#_Toc170063125)

[1.7 ASSETS 11](#_Toc170063126)

[**CHAPTER 2: RISK MANAGEMENT AND METHODOLOGIES** 13](#_Toc170063127)

[2.1: Risk Management Approach Using ISO 31000 framework 13](#_Toc170063128)

[2.2 ISO 31000 14](#_Toc170063129)

[2.3 ISO 31000 Stages 14](#_Toc170063130)

[**CHAPTER 3: RISK ASSESSMENT** 18](#_Toc170063131)

[3.1) Risk Identification 18](#_Toc170063132)

[3.1.1) Assets Identification 18](#_Toc170063133)

[3.2) Risk Analysis 60](#_Toc170063134)

[3.2.1) Impact Analysis 64](#_Toc170063135)

[3.3) Risk Evaluation 69](#_Toc170063136)

[3.3.1) Risk Level of Possible Risks 70](#_Toc170063137)

[**CHAPTER 4: TREATMENT AND RESPONSE** 75](#_Toc170063138)

[4.1 Determine Control 75](#_Toc170063139)

[4.2 Selection of Risk Treatment 83](#_Toc170063140)

[4.3 Risk Treatment Plan 85](#_Toc170063141)

[4.4 Residual Risk 86](#_Toc170063142)

# 

# **CHAPTER 1: INTRODUCTION**

## 1.1 Introduction

This report outlines a thorough structure of risk evaluations related to ISO 31000, specifically designed for the healthcare sector. The framework provides guidance on assessing and managing information security risks, given the large amount of sensitive patient data involved. In order to protect and ensure compliance with privacy regulations regarding this data, hospitals can use ISO 31000's risk assessment processes to identify vulnerabilities, evaluate threats, and implement necessary controls. With proper practices to address new challenges, ISO 31000 can be utilized to maintain the integrity of electronic health records. Additionally, healthcare organizations can combine existing healthcare-related guidelines with this framework to enhance overall governance. By fostering collaboration between various stakeholders, this framework can empower ABC Healthcare to effectively manage resources, overcome new challenges, and stay aligned with the overall strategic direction. This phased implementation approach ensures long-term success through performance monitoring and allows for adjustments. The framework should be adaptable to address unforeseen challenges, and transparency is key to maintaining continued support from the Board and Management.

## 1.2 Company Background

ABC Healthcare is a hospital established in 2020 to serve the residents of Ayer Keroh, Melaka. A team of dedicated healthcare professionals provides high-quality services to the community in this area. ABC Healthcare's mission is to prioritize creating a welcoming environment for patients to receive treatments and health consultations by offering a range of services such as annual checkups and minor injury treatments. Led by the Director, the team consists of healthcare professionals including physicians, nurses, pharmacists, and administrative staff who work together to ensure flawless workflow and coordination to serve patients seamlessly.

As the world evolves with technology, ABC Healthcare does the same by equipping modern IT infrastructure to support overall operations effectively. This includes electronic health record (EHR) systems, telehealth platforms, and administrative software to create seamless communication between the team and the patients. Having a good track record and feedback from clients drive ABC Healthcare to remain committed and provide a safe, secure, and comfortable environment for patients.

1.3 Organizational Chart

A diagram of a medical organization

Description automatically generated

## 1.4 Project Objectives

1) Enhance Patient Data Security

Implement a robust risk management framework to protect patient data from breaches and unauthorized access. By utilizing ISO 31000, ABC Healthcare can establish comprehensive risk assessment and mitigation strategies to secure electronic health records (EHR). This includes identifying potential vulnerabilities, assessing the impact of data breaches, and applying necessary controls to safeguard patient information.

2) Ensure Compliance with Regulatory Standards

Achieve and maintain compliance with relevant healthcare regulations and standards, such as HIPAA or local privacy laws. By adopting ISO 31000, ABC Healthcare can systematically identify and manage compliance risks. This involves continuous monitoring of regulatory changes, assessing compliance gaps, and implementing processes to meet legal and ethical standards, thus avoiding legal penalties and enhancing trust.

3) Improve Operational Resilience

Enhance the resilience of ABC Healthcare's operations to ensure continuity of care during disruptions. ISO 31000's risk management principles can help ABC Healthcare identify potential operational risks, such as IT system failures or natural disasters. By developing and testing business continuity plans, ABC Healthcare can ensure that critical healthcare services remain operational during unforeseen events, minimizing disruption to patient care.

4) Optimize Resource Allocation

Efficiently allocate resources to mitigate risks and improve overall healthcare delivery. Using ISO 31000, ABC Healthcare can prioritize risks based on their likelihood and impact, allowing for more effective allocation of financial, human, and technological resources. This strategic approach ensures that the most critical risks are addressed first, optimizing resource use and improving the quality of care.

5) Foster a Risk-Aware Culture

Promote a culture of risk awareness and proactive risk management among all staff members. Implementing ISO 31000 involves training and engaging staff at all levels in risk management practices. By fostering a risk-aware culture, ABC Healthcare can encourage proactive identification and reporting of risks, leading to early detection and mitigation. This collaborative approach enhances overall risk management and contributes to a safer, more secure healthcare environment.

## 1.5 Management Risk Organizational Chart

A group of people with their heads together

Description automatically generated

### 1.5.1 Organization Role and Description

|  |  |  |
| --- | --- | --- |
| TITLE ROLE | DESCRIPTION | JOB SCOPE AND RESPONSIBILITY |
| Hospital Director | * Oversees entire hospital operations and strategic direction. | * Ensures efficient functioning of all departments. * Develops and implements strategic initiatives. * Maintains regulatory compliance and quality standards. |
| Deputy Medical Director | * Assists Medical Director in medical policies and procedures. | * Provides leadership to medical staff. * Collaborates on strategic decision-making. * Ensures quality patient care delivery. |
| Deputy Managing Director | * Collaborates on strategic initiatives and operational management. | * Assists in developing and executing strategic plans. * Manages administrative functions. * Ensures operational efficiency and compliance. |
| Research | * Oversees research activities and fosters innovation. | * Coordinates research projects and studies. * Facilitates collaboration among researchers. * Ensures ethical and regulatory compliance. |
| Clinical Research Centre | * Conducts clinical trials and research studies. | * Facilitates clinical research activities. * Manages trial protocols and participant recruitment. * Ensures adherence to regulatory standards. |
| Women and Children | * Provides specialized care services for women and children. | * Manages obstetrics, gynaecology, and paediatric services. * Ensures compassionate and comprehensive care. |
| Obstetrics and Gynaecology Department | * Specialized care for women's health needs. | * Provides prenatal care, childbirth, and reproductive health services. * Manages gynaecological conditions and surgeries. |
| Paediatric Department | * Manages healthcare services for children and adolescents. | * Provides diagnosis, treatment, and preventive care. * Supports child and adolescent health and well-being. |
| Surgery | * Oversees surgical services across various specialties. | * Manages surgical procedures and operating rooms. * Coordinates surgical teams and patient care. |
| Anaesthesiology Department | * Provides anaesthesia services for surgical procedures. | * Administers anaesthesia to patients. * Monitors patient safety and comfort during surgery. |
| Neurosurgery Department | * Specialized surgical treatment for neurological conditions. | * Performs surgeries on the brain, spinal cord, and nervous system. * Provides postoperative care and rehabilitation. |
| Clinical Management | * Manages clinical operations and resource allocation. | * Optimizes patient flow and resource utilization. * Ensures quality and safety in clinical care delivery. |
| Medical Mangement Unit | * Coordinates medical services and treatment planning. | * Manages medical staff and patient care processes. * Supports effective treatment planning and coordination. |
| Nursing Unit | * Oversees nursing staff and patient care operations. | * Manages nursing staff and patient assignments. * Ensures adherence to nursing standards and protocols |
| Medical | * Manages medical departments and healthcare services. | * Provides medical care across various specialties. * Supports patient diagnosis, treatment, and management. |
| Psychiatry and Mental Health Department | * Provides psychiatric and mental health services. | * Diagnoses and treats mental illnesses and disorders. * Provides therapy and counselling services. |
| Medical Department | * Oversees medical services and patient care delivery. | * Manages medical staff and clinical operations. * Ensures quality and safety in medical care. |
| IT Department | * Manages information technology systems and infrastructure. | * Maintains hospital IT systems and networks. * Supports healthcare data management and security. |
| Financial Department | * Manages financial planning and accounting functions. | * Oversees budgeting, accounting, and financial reporting. * Ensures fiscal responsibility and compliance. |
| Engineering Department | * Manages facility infrastructure and equipment maintenance. | * Maintains hospital buildings, utilities, and equipment. * Ensures safety and compliance with regulations. |

## 1.6 Project Description / Network Diagram

A diagram of a computer network

Description automatically generated

<https://drdollah.com/hospital-information-system-his/system-architecture/>

1.6 Standard Referred

ISO 31000 risk management framework is referred as a guideline for this project. This is due to its purpose in proposing a guideline for organizations for identifying, evaluating and managing risks which can be customized to suit any organization. This standard is applicable in organizations in multiple different sectors and industries while also covering all types of risk. It is also can be applied in decision making at all levels.

## 1.7 Assets

*Hardware*

* *Databases*
* *Storage device*
* *Switches*
* *Domain controller*
* *Network management system*
* *Printers*
* *PCs*

*Software*

* *Electronic Health Record (EHR)*
* MySQL
* NetApp ONTAP
* Cisco IOS
* *Active Directory Domain Service (AD DS)*
* *SolarWinds* network performance monitor
* *Operating System (Windows 11)*
* *Microsoft Office Suite*

*Human*

* Medical staff
* Administration staff
* Support staff
* IT staff
* Management and leadership

Data and Information

* Patient records
* Financial records
* Research data
* Administrative records
* Operational Data

Physical Assets

* Building and facilities
* Medical equipment
* Furnitures
* vehicles

# **CHAPTER 2: RISK MANAGEMENT AND METHODOLOGIES**

## 2.1: Risk Management Approach Using ISO 31000 framework

A diagram of a risk management process

Description automatically generated

## 2.2 ISO 31000

We proposed ISO 31000 as our main standard. ISO 31000 is an international standard for risk management. It provides guidelines, principles, framework, and a process for managing risks effectively within organizations. ISO 31000 aims to assist organizations in developing a systematic and comprehensive approach to risk management. It helps organizations identify, analyze, evaluate, treat, monitor, and communicate risks, thereby improving decision-making processes and enhancing resilience.

The standard outlines a systematic process for managing risks, which involves identifying risks, assessing the likelihood and consequences of those risks, determining the level of risk tolerance, selecting and implementing appropriate risk treatment options, and monitoring and reviewing the effectiveness of risk management activities.

applicable to all types and sizes of organizations, regardless of their sector or industry. It can be used by public and private sector organizations, as well as non-profit organizations, to manage risks associated with various aspects of their operations, including strategic, operational, financial, and compliance risks.

## 2.3 ISO 31000 Stages

i) communication and consultation

Communication and consultation are efforts to ensure stakeholders understand various types of risks so that decisions made do not harm the organization. By conducting communication and consultation, it is expected to enhance the performance of risk management, making it more planned and smooth. Communication and consultation are carried out with stakeholders so that the organization can provide the necessary data and explanations about the system to be studied.

ii) scope, context, criteria

The purpose of establishing the scope, context, and criteria is to identify and design risk management that aligns with the scope of the organization.

iii) risk assessment

Risk assessment is the process of identifying, analyzing, and evaluating risks. Conducting a risk assessment requires accurate data and information available within the organization.

1. risk identification

Risk identification is a method to search for, find, and explain in detail the risks that hinder an organization. Accurate information is needed to identify risks. Risk identification can be done by interviewing experts in the field of Information Technology (IT Staff). There are several stages involved in identifying risks:

* Identifying information technology within the organization.
* Analyzing potential risks that may arise in the information technology.
* Identifying the impact of the risks.

1. risk analysis

Risk analysis is a method to identify existing risks. The purpose of risk analysis is to provide an overview during risk evaluation so that the risk methods employed can be targeted accurately. A likelihood table is used to determine how often a risk occurs within a certain period.

|  |  |  |  |
| --- | --- | --- | --- |
| Rating | Criteria | description | frequency |
| 1 | rare | the risk almost never occurs | >2 years |
| 2 | unlikely | the risk rarely occurs | 1-2 years |
| 3 | possible | the risk occasionally occurs | 7-12 months/years |
| 4 | Likely | the risk frequently occurs | 4-6 months/years |
| 5 | certain | the risk is certain to occur | 1-3 months/years |

Likelihood table

|  |  |  |
| --- | --- | --- |
| rating | criteria | description |
| 1 | insignificant | Does not disrupt company activities |
| 2 | minor | Company activities are slightly hindered but core activities are not affected. |
| 3 | moderate | Causes disruptions in business processes, hindering some company activities |
| 4 | major | Hinders almost all company activities |
| 5 | significant | Company activities stop due to a total disruption in business processes |

Impact table

1. risk evaluation

Risk evaluation is the decision-making process in risk management. Risk evaluation plays a role in determining whether further action is needed or not. In the risk evaluation stage, a risk matrix is used, which is derived from the results of the risk analysis and then entered into the matrix.

A chart with different colors and text

Description automatically generated with medium confidenceRisk matrix

iv) risk treatment

The purpose of risk treatment is to consider risk treatment options and implement risk management to control risks, reduce the likelihood of losses, and improve organizational performance, organizations have the following options for risk treatment:

1. Changing the likelihood

This is done to prevent the occurrence of risks that have a negative impact on the company and to facilitate the occurrence of positive risks, turning them into advantages for the organization.

1. Changing the impact

Reducing losses that may occur due to unprevented risks and maximizing the benefits of risks that negatively impact the organization.

1. Changing the likelihood and impact

Preventing risks that have a negative impact or triggering risks that have a positive impact, and preparing contingency plans as a precaution if all else fails.

v) monitoring and review

Monitoring and review are carried out to ensure that the risk process has been successfully implemented. Monitoring should always be conducted, and the results should be reviewed. The outcomes of monitoring and review must be incorporated into the organization's activities as performance benchmarks.

vi) recording and reporting

After the risk management process is completed, it is necessary to have documentation that serves as a record of activity implementation, acts as legal evidence in case of issues, and serves as a means for knowledge, both for the development of knowledge management within the company.

# **CHAPTER 3: RISK ASSESSMENT**

## 3.1) Risk Identification

### 3.1.1) Assets Identification

#### **HARDWARE**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| TYPE OF DEVICES | LOCATION | VALUE | PIC | DESCRIPTION | SERIAL NUMBER | MANUFACTURER | WARRANTY (YEARS) |
| Database Server 1 | Data Centre, Rack 2, shelf 1 | RM 50 000 | Emily Thompson (Database Administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | DB123456 | Dell | 3 |
| Database Server 2 | Backup Data Centre, rack 2, shelf 2 | RM 50 000 | Harry Kane (Database Administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | DB654321 | Dell | 3 |
| Storage Device | Data Centre, Rack 1, Shelf 3 | RM 10 000 | John Smith (IT administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | ST098765 | Dell | 5 |
| Switch 1 | Data Centre, network cabinet 1 | RM 10 000 | Lisa (Network Administrator) | Switch 1 serves as the core switch, centrally located in the data center. It connects directly to each of the other switches | SW112233 | Cisco | 1 |
| Switch 2 | Data Centre, network cabinet 1 | RM 5000 | Lisa (Network Administrator) | Switch 2 is positioned adjacent to Switch 1 within the data center. It connects to Switch 1 for access to the core network and directly links to the domain controller, facilitating authentication and directory services for network users. | SW223344 | Cisco | 1 |
| Switch 3 | Data Centre, network cabinet 2 | RM 5000 | Lisa (Network Administrator) | serves as an access switch, providing connectivity for network management systems, such as monitoring and configuration tools, allowing administrators to efficiently manage the network infrastructure. | SW009988 | Cisco | 1 |
| Switch 4 | Radiology Department, Network Cabinet | RM 5000 | Lisa (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW110055 | Cisco | 1 |
| Switch 5 | Radiology Department, Network Cabinet 2 | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW334400 | Cisco | 1 |
| Switch 6 | Neurology Department, Network Cabinet | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW110011 | Cisco | 1 |
| Switch 7 | Pediatrics Department, Network Cabinet | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW666777 | Cisco | 1 |
| Domain Controller | Data centre, Rack 2, Shelf 3 | RM 3000 | Michael (System/network administrator) | Windows Server running Active Directory services. It serves as the central authentication and authorization server for the healthcare system's network. | DC090988 | Windows | 2 |
| Network Management System | Data centre, rack 3, shelf 1 | RM 6500 | Michael (System/network administrator) | a centralized software platform used to monitor, configure, and analyze the healthcare system's network infrastructure. | NM976611 | Solarwind | 2 |
| Printer 1 | Rediology department, office 1 | RM 500 | Mike(IT support) | Printer 1 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents. | PR887788 | HP | 3 |
| Printer 2 | Cardiology department. Office 2 | RM 500 | Mike (office manager) | Printer 2 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents. | PR111100 | HP | 3 |
| Printer 3 | Pediatrics department, reception area | RM 500 | Mike (IT support) | Printer 3 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents. | PR912641 | HP | 3 |
| MRI Machine 1 | Radiology department, Imaging room 1 | RM 5 000 000 | Dr. Robert Thompson (Radiologist) | MRI Machine 1 is a Siemens MAGNETOM Aera 1.5T MRI system. It is used for detailed imaging of internal body structures to diagnose various medical conditions. | MRI090953 | Siemens | 10 |
| PC 1 | Rediology department, office 1 | RM 1 500 | John (IT support) | PC 1 is a Dell OptiPlex 7070 desktop computer. It is used by the radiologist for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC9344334 | Dell | 3 |
| PC 2 | Cardiology department. Office 2 | RM 1 500 | John (IT support) | PC 2 is a Dell OptiPlex 7070 desktop computer. It is used by the cardiologist for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC112291 | Dell | 3 |
| PC 3 | Pediatrics department, reception area | RM 1 500 | John (IT support) | PC 3 is a Dell OptiPlex 7070 desktop computer. It is used by the pediatrician for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC454511 | Dell | 3 |

**SOFTWARE**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TYPE OF DEVICES | LOCATION |  | VALUE | SOFTWARE | PIC | DESCRIPTION | VENDOR | LICENSE EXPIRY DATE | SUPPORT CONTACT |
| Database Server 1 | Data Centre, Rack 2, shelf 1 |  | RM 50 000 | MySQL | Emily Thompson (Database Administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | Oracle Corporation | 10/10/2027 | 00 1 650-506-7000 |
| Database Server 2 | Backup Data Centre, rack 2, shelf 2 |  | RM 50 000 | MySQL | Harry Kane (Database Administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | Oracle Corporation | 10/10/2027 | 00 1 650-506-7000 |
| Storage Device | Data Centre, Rack 1, Shelf 3 |  | RM 10 000 | NetApp ONTAP | John Smith (IT administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | NetAPP | 19/4/2029 | 60 320535139 |
| Switch 1, 2, 3, 4, 5, 6, 7 | Data Centre, network cabinet 1 |  | RM 10 000 | Cisco IOS | Lisa (Network Administrator) | provides essential networking functions including switching and routing, VLAN management, security, QoS, high availability, network management, and automation. These features are crucial for the efficient and secure operation of network infrastructure. | Cisco | 25/12/2025 | 1 800 805880 |
| Domain Controller | Data centre, Rack 2, Shelf 3 |  | RM 3000 | Active directory domain service | Michael (System/network administrator) | supports centralized user and access management, security and compliance, resource management, and enhanced collaboration. It ensures efficient operations, compliance with regulations, and secure management of IT resources, all of which are vital for delivering high-quality patient care. | Microsoft | 10/1/2026 | +603 2777 8888 |
| Network Management System | Data centre, rack 3, shelf 1 |  | RM 6500 | SolarWinds network performance monitor | Michael (System/network administrator) | ensures network health and reliability, supports capacity planning, aids in compliance, and enhances security. By providing real-time monitoring and alerts, performance analysis, and detailed reporting, NPM helps maintain the critical IT infrastructure necessary for delivering high-quality patient care. | SolarWinds | 5/1/2026 | +1-866-530-8040 |
| MRI Machine 1 | Radiology department, Imaging room 1 |  | RM 5 000 000 | Siemens Healthineers: DotGO software | Dr. Robert Thompson (Radiologist) | enhances the efficiency, consistency, and quality of MRI imaging workflows. It automates routine tasks, supports advanced imaging protocols, improves patient experience, and integrates seamlessly with other healthcare systems, making it a valuable tool in modern healthcare settings for delivering high-quality diagnostic imaging services. | Siemens | 1/9/2034 | +60 (3) 7952 5555 |
| PC 1 | Rediology department, office 1.  Cardiology department. Office 2. |  | RM 1 500 | Windows 11 | John (IT support) | contribute to a more efficient, secure, and user-friendly environment in healthcare settings. These improvements can lead to better patient care, streamlined operations, and enhanced collaboration among healthcare professionals. | Microsoft | 20/2/2029 | +603 2777 8888 |
| PC 2 | Cardiology department. Office 2. |  | RM 5000 | EHR | John (IT support) | centralizing patient information, improving care coordination, enhancing patient safety, streamlining workflows, supporting decision-making, engaging patients, enabling data analytics, ensuring regulatory compliance, reducing costs, and promoting continuity of care | Epic System Corporation | 15/3/2028 | +1 608-271-9000 |
| PC 3 | Pediatrics department, reception area. |  | RM 1000 | Microsoft office suite | John (IT support) | Used for clinical documentation, data analysis, communication, collaboration, training, project management, workflow automation, and secure file storage. | Microsoft | 22/8/2025 | +603 2777 8888 |

#### **HUMAN**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NAME | TITLE | DEPARTMENT | SKILLS AND QUALIFICATION | ACCESS LEVEL | AVAILABILITY | REPLACEMENT TIME |
| Dr Alice Lee | Cancer research scientist | Research | Expertise in cancer research, experience with clinical trials and data analysis software (e.g., STATA, R) | Access to research databases and hospital EHR (limited to oncology data). | Full-time, critical role with high impact on absence. | Long due to specialized expertise. |
| Mr. Ben Miller | Research assistant | research | Expertise in biostatistics and data management | Access to research databases with limited access rights. | Full-time, supports Dr. Lee's research and can partially cover during absence. | Moderate, depending on the specific tasks involved |
| Dr Sarah Jones | Board-Certified OB-GYN Physician | Women & Children | Extensive experience in delivering babies and managing high-risk pregnancies. | Full EHR access for obstetrics, restricted access to NICU. | Full-time, critical role with long replacement time | Very long due to specialization |
| Ms. Emily Brown | Registered Nurse (Pediatrics) | Women & Children | Certifications in pediatrics and neonatal care | EHR access for pediatrics, access to general patient wards. | Full-time, provides support to Dr. Jones and can cover some duties during absence | Moderate, depending on the specific role and experience of the replacement nurse |
| Dr David Smith | Cardiothoracic Surgeon | Surgery | Expertise in complex heart and lung surgeries | Full EHR access for surgical procedures | Full-time, critical and irreplaceable role | Very long due to specialization and experience |
| Dr. Michael Chen | Surgical Resident (General Surgery) | Surgery | Broad surgical skills with potential for future specialization. | Full EHR access for surgical procedures | Full-time, can provide some support to Dr. Smith and cover basic surgery during absence | Long for specific surgeries performed by Dr. Smith, but shorter for general surgery coverage |
| Ms. Pamela Johnson | Director of Nursing | Clinical Management | Extensive experience in healthcare administration and clinical workflows. | Broad access to hospital management systems and employee data for HR functions | Full-time, critical role for hospital operations | Long due to experience and leadership qualities |
| Mr. Charles White | Clinical Quality Improvement Specialist | Clinical Management | Background in healthcare data analysis and process improvement | Access to specific hospital management systems for quality monitoring. | Full-time, supports Ms. Johnson and can cover some administrative tasks during absence | Moderate, depending on the specific skills and experience required |
| Dr. Maria Garcia | Board-Certified Internist | Medical | Strong diagnostic skills and experience with a wide range of medical conditions. | Full EHR access for internal medicine patients | Full-time, provides essential medical care | Moderate, depending on the availability of other qualified internists |
| Dr. William Thomas | Part-Time Physician (Geriatric Medicine) | Medical | Expertise in caring for elderly patients. | Full EHR access for geriatric medicine patients. | Part-time, provides additional coverage for specific patient needs. | N/A (part-time role, coverage can be adjusted based on patient needs). |
| Ms. Anna Lopez | Healthcare Finance Manager | Financial | Expertise in medical billing and coding procedures. | Access to financial data systems for patient billing. | Full-time, critical role for managing hospital finances. | Long due to experience and knowledge of complex healthcare billing regulations. |
| Mr. Robert Young | Accounting Assistant | Financial | Strong understanding of financial regulations and reporting. | Access to financial data systems for basic accounting functions. | Full-time, supports Ms. Lopez and can cover some administrative tasks during absence. | Moderate, depending on the specific tasks and experience required. |
| Mr Thomas | Biomedical Equipment Technician | Engineering | Expertise in maintaining and repairing medical equipment. | Access to restricted areas for equipment maintenance. | Full-time, critical role for ensuring equipment functionality. | Moderate, depending on the availability of qualified biomedical equipment technicians. |
| Ms. Elizabeth Brown | Building Maintenance Engineer | Engineering | Expertise in maintaining hospital facilities (HVAC, electrical). | Access to building maintenance systems and restricted areas for repairs. | Full-time, supports Mr. Thomas and ensures proper building operation | Moderate, depending on the specific skills and experience required for building maintenance. |

**DATA**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DATA TYPE | LOCATION | DATA VOLUME | RETENTION PERIOD (YEARS) | DATA OWNER | BACKUP AND RECOVERY PLAN |
| Patient Record | Database 1 | 1 TB | 10 | Medical record department | Daily backups, off-site storage, monthly recovery tests |
| Financial Transactions | Database 2 | 500GB | 7 | Finance department | Hourly backups, cloud replication, weekly recovery tests |
| Staff Information | Database 2 | 300GB | 7 | HR department | Daily backups, off-site storage, monthly recovery tests |
| Medical imaging data | Storage device | 5 TB | 5 | Radiology department | Real-time backups, local and remote storage, quarterly recovery tests |
| Network log | Network management system | 100GB | 1 | IT department | Real-time backups, redundant storage, quarterly recovery tests |
| System access log | Domain controller | 200GB | 1 | IT department | Real-time backups, redundant storage, quarterly recovery tests |

#### **PHYSICAL ASSETS**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ASSET** | **ASSET TYPE** | **QUANTITY** | **LOCATION** | **VALUE** | **MANUFACTURER** | **WARRANTY (years)** |
| Hospital Bed | Medical equipment | 100 | Patients room | 2000 | Hill-rom | 2 |
| Ventilator | Medical equipment | 20 | ICU | 25000 | medtronic | 2 |
| Surgical table | Medical equipment | 10 | Operating rooms | 15000 | STERIS corporation | 3 |
| Patient monitor | Medical equipment | 50 | ICU | 7000 | Philips healthcare | 2 |
| Blood pressure monitor | Medical equipment | 50 | General ward | 500 | Omron | 1 |
| wheelchair |  | 30 | General ward | 300 | Invacare | 1 |
| Ultrasound machine | Medical equipment | 5 | Maternity ward | 50000 | Philips healthcare | 3 |
| Office chair | Furniture | 50 | Administrative office | 200 | Herman miller | 5 |
| Waiting room chair | Furniture | 100 | Main lobby | 100 | Steelcase | 2 |
| sofa | Furniture | 10 | Family waiting area | 800 | La-z-boy | 2 |
| Conference table | Furniture | 5 | Meeting rooms | 2000 | knoll | 5 |
| Bedside table | furniture | 100 | Patient room | 150 | stryker | 3 |
| Ambulance | Vehicle | 15 |  |  |  |  |

3.1.2) Potential Risk Identification.

|  |  |
| --- | --- |
| **ID** | **RISK** |
| R01 | Data loss |
| R02 | Data entry failure |
| R03 | System crash |
| R04 | Slow network |
| R05 | Unable to Obtain IP Address |
| R06 | Data Mismatch |
| R07 | UPS unable to Store Power |
| R08 | Human Error |
| R09 | Lack of Knowledge on EHR Operation |
| R10 | Computer System Hanging/Freezing |
| R11 | Virus |
| R12 | Hardware Damage |
| R13 | Unable to Boot Computer |
| R14 | Power Outage |
| R15 | Natural disaster |
| R16 | Insufficient Access Control (PH) |
| R17 | Mechanical Failure (P) |
| R18 | Display/Readout Failure (P) |
| R19 | Wear and Tear (P) |
| R20 | Inadequate Training (H) |
| R21 | Fatigue or Distraction (H) |
| R22 | Misinterpretation of Data (H) |

3.1.3) Risk Impact Identification

#### HARDWARE TABLE

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TYPE OF DEVICES** | **LOCATION** | **VALUE** | **PIC** | **DESCRIPTION** | **SERIAL NUMBER** | **manufacturer** | **Warranty (years)** | **RISK ID** | **RISK DESCRIPTION** |
| Database Server 1 | Data Centre, Rack 2, shelf 1 | RM 50 000 | Emily Thompson (Database Administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | DB123456 | Dell | 3 | R12  R13 | Hardware damage  Unable to boot device |
| Database Server 2 | Backup Data Centre, rack 2, shelf 2 | RM 50 000 | Harry Kane (Database Administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | DB654321 | Dell | 3 | R12  R13 | Hardware damage  Unable to boot device |
| Storage Device | Data Centre, Rack 1, Shelf 3 | RM 10 000 | John Smith (IT administrator) | The storage device is a Dell PowerVault MD series NAS with 20TB of storage capacity. It serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | ST098765 | Dell | 5 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 1 | Data Centre, network cabinet 1 | RM 10 000 | Lisa (Network Administrator) | Switch 1 serves as the core switch, centrally located in the data center. It connects directly to each of the other switches | SW112233 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 2 | Data Centre, network cabinet 1 | RM 5000 | Lisa (Network Administrator) | Switch 2 is positioned adjacent to Switch 1 within the data center. It connects to Switch 1 for access to the core network and directly links to the domain controller, facilitating authentication and directory services for network users | SW223344 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 3 | Data Centre, network cabinet 2 | RM 5000 | Lisa (Network Administrator) | serves as an access switch, providing connectivity for network management systems, such as monitoring and configuration tools, allowing administrators to efficiently manage the network infrastructure. | SW009988 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 4 | Radiology Department, Network Cabinet | RM 5000 | Lisa (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW110055 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 5 | Radiology Department, Network Cabinet 2 | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW334400 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 6 | Neurology Department, Network Cabinet | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW110011 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Switch 7 | Pediatrics Department, Network Cabinet | RM 5000 | Linda (Network Administrator) | provides connectivity for thick clients, including printers, PCs, and other devices, within the clinic's local network environment. | SW666777 | Cisco | 1 | R12  R13 | Hardware damage  Unable to boot device |
| Domain Controller | Data centre, Rack 2, Shelf 3 | RM 3000 | Michael (System/network administrator) | Windows Server running Active Directory services. It serves as the central authentication and authorization server for the healthcare system's network | DC090988 | Windows | 2 | R12  R13 | Hardware damage  Unable to boot device |
| Network Management System | Data centre, rack 3, shelf 1 | RM 6500 | Michael (System/network administrator) | a centralized software platform used to monitor, configure, and analyze the healthcare system's network infrastructure | NM976611 | Solarwind | 2 | R12  R13 | Hardware damage  Unable to boot device |
| Printer 1 | Rediology department, office 1 | RM 500 | Mike(IT support) | Printer 1 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents | PR887788 | HP | 3 | R12  R13 | Hardware damage  Unable to boot device |
| Printer 2 | Cardiology department. Office 2 | RM 500 | Mike (office manager) | Printer 2 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents | PR111100 | HP | 3 | R12  R13 | Hardware damage  Unable to boot device |
| Printer 3 | Pediatrics department, reception area | RM 500 | Mike (IT support) | Printer 3 is an HP LaserJet Pro M404dn. It is used for printing medical reports, patient records, and administrative documents | PR912641 | HP | 3 | R12  R13 | Hardware damage  Unable to boot device |
| MRI Machine 1 | Radiology department, Imaging room 1 | RM 5 000 000 | Dr. Robert Thompson (Radiologist) | MRI Machine 1 is a Siemens MAGNETOM Aera 1.5T MRI system. It is used for detailed imaging of internal body structures to diagnose various medical conditions. | MRI090953 | Siemens | 10 | R12  R13 | Hardware damage  Unable to boot device |
| PC 1 | Rediology department, office 1 | RM 1 500 | John (IT support) | PC 1 is a Dell OptiPlex 7070 desktop computer. It is used by the radiologist for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC9344334 | Dell | 3 | R12  R13 | Hardware damage  Unable to boot device |
| PC 2 | Cardiology department. Office 2 | RM 1 500 | John (IT support) | PC 2 is a Dell OptiPlex 7070 desktop computer. It is used by the cardiologist for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC112291 | Dell | 3 | R12  R13 | Hardware damage  Unable to boot device |
| PC 3 | Pediatrics department, reception area | RM 1 500 | John (IT support) | PC 3 is a Dell OptiPlex 7070 desktop computer. It is used by the pediatrician for accessing electronic health records (EHR), viewing medical images, and managing patient care. | PC454511 | Dell | 3 | R12  R13 | Hardware damage  Unable to boot device |

#### **SOFTWARE TABLE**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TYPE OF DEVICES** | **LOCATION** | **VALUE** | **SOFTWARE** | **PIC** | **DESCRIPTION** | **VENDOR** | **LICENSE EXPIRY DATE** | **SUPPORT CONTACT** | **RISK ID** | **RISK DESCRIPTION** |
| Database Server 1 | Data Centre, Rack 2, shelf 1 | RM 50 000 | MySQL | Emily Thompson (Database Administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | Oracle Corporation | 10/10/2027 | 03-2299 3600 | R 01  R 02 | Data Loss  Data Entry Failure |
| Database Server 2 | Backup Data Centre, rack 2, shelf 2 | RM 50 000 | MySQL | Harry Kane (Database Administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | Oracle Corporation | 10/10/2027 | 03-2299 3600 | R 01  R 02 | Data Loss  Data Entry Failure |
| Storage Device | Data Centre, Rack 1, Shelf 3 | RM 10 000 | NetApp ONTAP | John Smith (IT administrator) | serves as the primary storage repository for various healthcare system data, including patient records, medical images, and administrative documents. | NetAPP | 19/4/2029 | 0320-535139 | R 01  R 03 | Data Loss  System Crash |
| Switch 1, 2, 3, 4, 5, 6, 7 | Data Centre, network cabinet 1 | RM 10 000 | Cisco IOS | Lisa (Network Administrator) | provides essential networking functions including switching and routing, VLAN management, security, QoS, high availability, network management, and automation. These features are crucial for the efficient and secure operation of network infrastructure. | Cisco | 25/12/2025 | 1-800-805880 | R 04  R 05 | Slow network  Unable to Obtain IP Address |
| Domain Controller | Data centre, Rack 2, Shelf 3 | RM 3000 | Active directory domain service | Michael (System/network administrator) | supports centralized user and access management, security and compliance, resource management, and enhanced collaboration. It ensures efficient operations, compliance with regulations, and secure management of IT resources, all of which are vital for delivering high-quality patient care. | Microsoft | 10/1/2026 | 03-2777 8888 | R07  R 10 | UPS unable to Store Power  Computer System Hanging/Freezing |
| Network Management System | Data centre, rack 3, shelf 1 | RM 6500 | SolarWinds network performance monitor | Michael (System/network administrator) | ensures network health and reliability, supports capacity planning, aids in compliance, and enhances security. By providing real-time monitoring and alerts, performance analysis, and detailed reporting, NPM helps maintain the critical IT infrastructure necessary for delivering high-quality patient care. | SolarWinds | 5/1/2026 | +1-866-530-8040 | R11   R 16 | Virus  Insufficient Access Control |
| MRI Machine 1 | Radiology department, Imaging room 1 | RM 5 000 000 | Siemens Healthineers: DotGO software | Dr. Robert Thompson (Radiologist) | enhances the efficiency, consistency, and quality of MRI imaging workflows. It automates routine tasks, supports advanced imaging protocols, improves patient experience, and integrates seamlessly with other healthcare systems, making it a valuable tool in modern healthcare settings for delivering high-quality diagnostic imaging services. | Siemens | 1/9/2034 | +60 (3) 7952 5555 | R 18 | Display/Readout Failure |
| PC 1 | Rediology department, office 1. | RM 1 500 | Windows 11 | John (IT support) | contribute to a more efficient, secure, and user-friendly environment in healthcare settings. These improvements can lead to better patient care, streamlined operations, and enhanced collaboration among healthcare professionals. | Microsoft | 20/2/2029 | 03-2777 8888 | R 03  R 10 | System crash  Computer System Hanging/Freezing |
| PC 2 | Cardiology department. Office 2. | RM 5000 | EHR | John (IT support) | centralizing patient information, improving care coordination, enhancing patient safety, streamlining workflows, supporting decision-making, engaging patients, enabling data analytics, ensuring regulatory compliance, reducing costs, and promoting continuity of care | Epic System Corporation | 15/3/2028 | +1 608-271-9000 | R 03  R 10 | System crash  Computer System Hanging/Freezing |
| PC 3 | Pediatrics department, reception area | RM 1000 | Microsoft office suite | John (IT support) | Used for clinical documentation, data analysis, communication, collaboration, training, project management, workflow automation, and secure file storage. | Microsoft | 22/8/2025 | +603 2777 8888 | R 03  R 10 | System crash  Computer System Hanging/Freezing |

#### **HUMAN**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NAME** | **TITLE** | **DEPARTMENT** | **SKILLS AND QUALIFICATION** | **ACCESS LEVEL** | **AVAILABILITY** | **REPLACEMENT TIME** | **RISK ID** | **RISK DESCRIPTION** |
| Dr Alice Lee | Cancer research scientist | Research | Expertise in cancer research, experience with clinical trials and data analysis software (e.g., STATA, R) | Access to research databases and hospital EHR (limited to oncology data). | Full-time, critical role with high impact on absence. | Long due to specialized expertise. | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Mr. Ben Miller | Research assistant | research | Expertise in biostatistics and data management | Access to research databases with limited access rights. | Full-time, supports Dr. Lee's research and can partially cover during absence. | Moderate, depending on the specific tasks involved | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Dr Sarah Jones | Board-Certified OB-GYN Physician | Women & Children | Extensive experience in delivering babies and managing high-risk pregnancies. | Full EHR access for obstetrics, restricted access to NICU. | Full-time, critical role with long replacement time | Very long due to specialization | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Ms. Emily Brown | Registered Nurse (Pediatrics) | Women & Children | Certifications in pediatrics and neonatal care | EHR access for pediatrics, access to general patient wards. | Full-time, provides support to Dr. Jones and can cover some duties during absence | Moderate, depending on the specific role and experience of the replacement nurse | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Dr David Smith | Cardiothoracic Surgeon | Surgery | Expertise in complex heart and lung surgeries | Full EHR access for surgical procedures | Full-time, critical and irreplaceable role | Very long due to specialization and experience | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Dr. Michael Chen | Surgical Resident (General Surgery) | Surgery | Broad surgical skills with potential for future specialization. | Full EHR access for surgical procedures | Full-time, can provide some support to Dr. Smith and cover basic surgery during absence | Long for specific surgeries performed by Dr. Smith, but shorter for general surgery coverage | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Ms. Pamela Johnson | Director of Nursing | Clinical Management | Extensive experience in healthcare administration and clinical workflows. | Broad access to hospital management systems and employee data for HR functions | Full-time, critical role for hospital operations | Long due to experience and leadership qualities | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Mr. Charles White | Clinical Quality Improvement Specialist | Clinical Management | Background in healthcare data analysis and process improvement | Access to specific hospital management systems for quality monitoring. | Full-time, supports Ms. Johnson and can cover some administrative tasks during absence | Moderate, depending on the specific skills and experience required | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Dr. Maria Garcia | Board-Certified Internist | Medical | Strong diagnostic skills and experience with a wide range of medical conditions. | Full EHR access for internal medicine patients | Full-time, provides essential medical care | Moderate, depending on the availability of other qualified internists | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Dr. William Thomas | Part-Time Physician (Geriatric Medicine) | Medical | Expertise in caring for elderly patients. | Full EHR access for geriatric medicine patients. | Part-time, provides additional coverage for specific patient needs. | N/A (part-time role, coverage can be adjusted based on patient needs). | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Ms. Anna Lopez | Healthcare Finance Manager | Financial | Expertise in medical billing and coding procedures. | Access to financial data systems for patient billing. | Full-time, critical role for managing hospital finances. | Long due to experience and knowledge of complex healthcare billing regulations. | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Mr. Robert Young | Accounting Assistant | Financial | Strong understanding of financial regulations and reporting. | Access to financial data systems for basic accounting functions. | Full-time, supports Ms. Lopez and can cover some administrative tasks during absence. | Moderate, depending on the specific tasks and experience required. | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Mr Thomas | Biomedical Equipment Technician | Engineering | Expertise in maintaining and repairing medical equipment. | Access to restricted areas for equipment maintenance. | Full-time, critical role for ensuring equipment functionality. | Moderate, depending on the availability of qualified biomedical equipment technicians. | R08  R09 | Human Error  Lack of  Knowledge on EHR |
| Ms. Elizabeth Brown | Building Maintenance Engineer | Engineering | Expertise in maintaining hospital facilities (HVAC, electrical). | Access to building maintenance systems and restricted areas for repairs. | Full-time, supports Mr. Thomas and ensures proper building operation | Moderate, depending on the specific skills and experience required for building maintenance. | R08  R09 | Human Error  Lack of  Knowledge on EHR |

#### **DATA**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **DATA TYPE** | **LOCATION** | **DATA VOLUME** | **RETENTION PERIOD (YEARS)** | **DATA OWNER** | **BACKUP AND RECOVERY PLAN** | **RISK ID** | **RISK DESCRIPTION** |
| Patient Record | Database 1 | 1 TB | 10 | Medical record department | Daily backups, off-site storage, monthly recovery tests | R01  R02 | Data loss  Data entry failure |
| Financial Transactions | Database 2 | 500GB | 7 | Finance department | Hourly backups, cloud replication, weekly recovery tests | R01  R02 | Data loss  Data entry failure |
| Staff Information | Database 2 | 300GB | 7 | HR department | Daily backups, off-site storage, monthly recovery tests | R01  R02 | Data loss  Data entry failure |
| Medical imaging data | Storage device | 5 TB | 5 | Radiology department | Real-time backups, local and remote storage, quarterly recovery tests | R01  R02 | Data loss  Data entry failure |
| Network log | Network management system | 100GB | 1 | IT department | Real-time backups, redundant storage, quarterly recovery tests | R01  R02 | Data loss  Data entry failure |
| System access log | Domain controller | 200GB | 1 | IT department | Real-time backups, redundant storage, quarterly recovery tests | R01  R02 | Data loss  Data entry failure |

#### **PHYSICAL ASSET**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ASSET TYPE** | **QUANTITY** | **LOCATION** | **VALUE** | **MANUFACTURER** | **WARRANTY (years)** | **RISK ID** | **RISK DESCRIPTION** |
| Hospital Bed | 100 | Patients room | 2000 | Hill-rom | 2 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Ventilator | 20 | ICU | 25000 | medtronic | 2 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Surgical table | 10 | Operating rooms | 15000 | STERIS corporation | 3 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Patient monitor | 50 | ICU | 7000 | Philips healthcare | 2 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Blood pressure monitor | 50 | General ward | 500 | Omron | 1 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| wheelchair | 30 | General ward | 300 | Invacare | 1 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Ultrasound machine | 5 | Maternity ward | 50000 | Philips healthcare | 3 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Office chair | 50 | Administrative office | 200 | Herman miller | 5 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Waiting room chair | 100 | Main lobby | 100 | Steelcase | 2 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| sofa | 10 | Family waiting area | 800 | La-z-boy | 2 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Conference table | 5 | Meeting rooms | 2000 | knoll | 5 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |
| Bedside table | 100 | Patient room | 150 | stryker | 3 | R07  R14  R15 | UPS unable to Store Power  Power outage  Natural disaster |

## 3.2) Risk Analysis

The step that is performed after risk identification is risk analysis of the existing risks. These risks will also be analysed based on their impact on the organisation as well as their likelihood of happening.

The scoring scheme for likelihood of occurrence and impact of a specific risk can be calculated through the following scoring scheme:  
  
Likelihood scoring scheme:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood Score | 1 | 2 | 3 | 4 | 5 |
| Description | Rare | Unlikely | Possible | Likely | Almost Certain |
| Frequency (Time frame) | >2 years | 1-2 years | 7-12 months | 4-6 months | 1-3 months |
| Probability (%) | 0 – 20% | 21 – 40% | 41 – 60% | 61 – 80% | 81 – 100% |

Impact Scoring Scheme:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact Score | 1 | 2 | 3 | 4 | 5 |
| Description | Insignificant | Minor | Moderate | Major | Catastrophic |
| Impact Description (general) | Does not affect the organisation’s activities | Slightly hinders activities, but core operations are unaffected | Causes disruption in processes, hindering some activities | Hampers nearly all activities | Stops activities due to total disruptions |
| Probability (%) | 0 – 20% | 21 – 40% | 41 – 60% | 61 – 80% | 81 – 100% |

Use quantitative analysis which using the formula below

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **RISK** | **OCCURENCE PER YEAR** | **LIKELIHOOD (%)** | **LIKELIHOOD SCORE** |
| R01 | Data loss | 1 | 0.14 | 1 |
| R02 | Data entry failure | 150 | 21.37 | 2 |
| R03 | System crash | 250 | 35.60 | 2 |
| R04 | Slow network | 420 | 59.83 | 3 |
| R05 | Unable to Obtain IP Address | 500 | 71.22 | 4 |
| R06 | Data Mismatch | 600 | 85.46 | 5 |
| R07 | UPS unable to Store Power | 50 | 7.12 | 1 |
| R08 | Human Error | 700 | 99.71 | 5 |
| R09 | Lack of Knowledge on EHR Operation | 250 | 35.60 | 2 |
| R10 | Computer System Hanging/Freezing | 420 | 59.83 | 3 |
| R11 | Virus | 50 | 7.12 | 1 |
| R12 | Hardware Damage | 200 | 28.49 | 2 |
| R13 | Unable to Boot Computer | 50 | 7.132 | 1 |
| R14 | Power Outage | 100 | 14.24 | 1 |
| R15 | Natural disaster | 1 | 0.14 | 1 |
| R16 | Insufficient Access Control (PH) | 100 | 14.24 | 1 |
| R17 | Mechanical Failure (P) | 300 | 42.75 | 3 |
| R18 | Display/Readout Failure (P) | 200 | 28.49 | 2 |
| R19 | Wear and Tear (P) | 400 | 56.97 | 3 |
| R20 | Inadequate Training (H) | 100 | 14.24 | 1 |
| R21 | Fatigue or Distraction (H) | 600 | 85.46 | 5 |
| R22 | Misinterpretation of Data (H) | 300 | 42.75 | 3 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Likelihood (%) | Likelihood Score | Impact (%) | Impact Score |
| R01 | Data Loss | 38% | 2 | 48% | 3 |
| R02 | Data Entry Failure | 52% | 3 | 56% | 3 |
| R03 | System Crash | 36% | 2 | 60% | 4 |
| R04 | Slow Network | 64% | 4 | 56% | 3 |
| R05 | Unable to Obtain IP Address | 68% | 4 | 44% | 3 |
| R06 | Data Mismatch | 44% | 3 | 44% | 3 |
| R07 | UPS Unable to Store Power | 40% | 3 | 52% | 3 |
| R08 | Human Error | 52% | 3 | 48% | 3 |
| R09 | Lack of Knowledge on EHR Operation | 40% | 3 | 40% | 3 |
| R10 | Computer System Hanging/Freezing | 52% | 3 | 52% | 3 |
| R11 | Virus | 52% | 3 | 72% | 4 |
| R12 | Hardware Damage | 60% | 4 | 56% | 3 |
| R13 | Unable to Boot Computer | 52% | 3 | 52% | 3 |
| R14 | Power Outage | 44% | 3 | 76% | 4 |
| R15 | Natural Disaster |  | 1 |  | 5 |
| R16 | Insufficient Access Control (PH) |  | 2 |  | 4 |
| R17 | Mechanical Failure (P) |  | 3 |  | 3 |
| R18 | Display/Readout Failure (P) |  | 3 |  | 3 |
| R19 | Wear and Tear (P) |  | 3 |  | 3 |
| R20 | Inadequate Training (H) |  | 3 |  | 4 |
| R21 | Fatigue or Distraction (H) |  | 4 |  | 3 |
| R22 | Misinterpretation of Data (H) |  | 3 |  | 3 |

### 3.2.1) Impact Analysis

This section describes the severity and type of impact on the organisation’s operations, assets, reputation and other critical areas.

|  |  |
| --- | --- |
| Impact Rating | Definition |
| Catastrophic – 5 | Event or circumstance having potentially catastrophic influence on company or large material negative impact on a crucial sector. |
| Major – 4 | Critical incident or scenario that can be tolerated with good management. |
| Moderate – 3 | Significant incident or scenario that can be addressed under regular conditions. |
| Minor – 2 | Event with impacts that can be readily accepted but require organisational effort to reduce the damage. |
| Insignificant – 1 | Some loss but not major; current controls and procedures should deal with the incident or circumstance. |

The Impact Rating Definition table above defines the constitutes of catastrophic, major, moderate, minor and insignificant.

|  |  |
| --- | --- |
| Type of Impact | Impact |
| Harm to Operations | * Disruption in healthcare delivery * Delayed procedures * Low efficiency * Low confidence in delivery * Inability to perform current mission * Misdiagnoses |
| Harm to Assets | * Damage to patient data/IT systems (Hardware & Software)/Medical Equipment * Loss of intellectual properties |
| Harm to Individuals | * Patient safety risks * Identity theft * Privacy breaches * Physical/Psychological mistreatment   + Damage to image/reputation |
| Harm to Other Organisations | * Contract breaches * Direct financial costs * Relational harm that damage to trust/ Reputational damage (future relationship) |

The Impact Type table above identifies the different types of impacts.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Risk Description | Rating | Description |
| R01 | Data Loss | Medium | **Harm to Operations:** Loss of critical patient data could delay treatments.  **Harm to Assets:** Data recovery costs. |
| R02 | Data Entry Failure | Medium | **Harm to Operations:** Incorrect data entries lead to wrong treatments or diagnoses.  **Harm to Individuals:** Potential harm to patient health. |
| R03 | System Crash | Medium | **Harm to Operations:** Disruption in accessing patient records, delaying treatment.  **Harm to Assets:** Cost of system restoration. |
| R04 | Slow Network | Medium | **Harm to Operations:** Reduced efficiency. |
| R05 | Unable to Obtain IP Address | Medium | **Harm to Operations:** Disruption in healthcare delivery. |
| R06 | Data Mismatch | Medium | **Harm to Operations:** Leads to incorrect patient data integration, potentially results misinformed treatment decisions.  **Harm to Individuals:** Potential harm to patient health. |
| R07 | UPS Unable to Store Power | Medium | **Harm to Operations:** Inability to perform current mission causing operational disruptions.  **Harm to Individuals:** Patient safety risks at stake. |
| R08 | Human Error | Medium | **Harm to Operations:** Compromise quality of work and patient safety. |
| R09 | Lack of Knowledge on EHR Operation | Medium | **Harm to Operations:** Undermines trust in the healthcare provider's competence. |
| R10 | Computer System Hanging/Freezing | Medium | **Harm to Operations:** Delay access to patient records. |
| R11 | Virus | High | **Harm to Operations:** Can cause major disruptions to system operations.  **Harm to Assets:** Data breaches, compromises patient confidentiality.  **Harm to Individuals:** Privacy breaches. |
| R12 | Hardware Damage | Medium | **Harm to Operations:** Disruption in healthcare delivery as well as costly repairs and replacements. |
| R13 | Unable to Boot Computer | Medium | **Harm to Operations:** Delays in accessing patient records, leads to low efficiency. |
| R14 | Power Outage | High | **Harm to Operations:** Causes major disruptions might be for critical procedures.  **Harm to Individuals:** Possible physical or psychological mistreatments. |
| R15 | Natural Disaster | Medium | **Harm to Assets:** Costly repairs and loss of medical equipment. |
| R16 | Insufficient Access Control (PH) | Medium | **Harm to Operations:** Unauthorised access to sensitive data/areas, leads to potential sabotage.  **Harm to Assets:** Damage to sensitive patient data.  **Harm to Individuals:** Privacy breaches. |
| R17 | Mechanical Failure (P) | Medium | **Harm to Operations:** Delays treatment of patients.  **Harm to Assets:** Costly repairs and replacement of medical equipment.  **Harm to Individuals:** Patient safety is at risk due to delay in treatments. |
| R18 | Display/Readout Failure (P) | Medium | **Harm to Operations:** Inaccurate data can lead to misdiagnoses.  **Harm to Individuals:** Potential harm to patient’s health safety due to incorrect readings. |
| R19 | Wear and Tear (P) | Medium | **Harm to Operations:** Delayed procedures caused by degradation of equipment’s performance.  **Harm to Assets:** Regular medical equipment maintenance cost |
| R20 | Inadequate Training (H) | High | **Harm to Individuals:** Increased risk of accidents and physical mistreatment.  **Harm to Organisations:** Reputational damage due to lack of standard work culture. |
| R21 | Fatigue or Distraction (H) | Medium | **Harm to Operations:** Reduced productivity and increased likelihood of mistakes.  **Harm to Individuals:** Increased risk of accidents and physical mistreatment.  **Harm to Organisations:** Reputational damage due to lack of standard work culture. |
| R22 | Misinterpretation of Data (H) | Medium | **Harm to Operations:** Low confidence in treatment delivery and possible cause of misdiagnoses.  **Harm to Individuals:** Physical or psychological mistreatment that leads to patient’s safety risks. |

## 

## 3.3) Risk Evaluation

The final step is the risk evaluation which involves decision-making in risk management. The results of the risk evaluation will determine the actions to be taken to address and manage the risks which are identified and categorised into three risk levels (low, medium and high) based on a risk matrix.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RISK EVALUATION MATRIX | | | | | |
| IMPACT  \  LIKELIHOOD | 1  Insignificant | 2  Minor | 3  Moderate | 4  Major | 5  Catastrophic |
| Certain – 5 | Medium | Medium | High | High | High |
| Likely – 4 | Medium | Medium | R04, R05, R12, R21 | High | High |
| Possible – 3 | Low | Medium | R02, R06, R07, R08, R09, R10, R13, R17, R18, R19, R22 | R11, R14, R20 | High |
| Unlikely – 2 | Low | Low | R01 | R03, R16 | Medium |
| Rare – 1 | Low | Low | Low | Medium | R15 |

Once the risk evaluation is completed through the risk evaluation matrix table, there will be an explanation of the 15 potential dangers that match the risk level of each risk based on their likelihood of happening and impact they have on the organisation.

### 3.3.1) Risk Level of Possible Risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Risk Description | Likelihood | Impact | Rating |
| R11 | Virus | 3 | 4 | High |
| R14 | Power Outage | 3 | 4 | High |
| R20 | Inadequate Training (H) | 3 | 4 | High |
| R02 | Data Entry Failure | 3 | 3 | Medium |
| R06 | Data Mismatch | 3 | 3 | Medium |
| R07 | UPS Unable to Store Power | 3 | 3 | Medium |
| R08 | Human Error | 3 | 3 | Medium |
| R09 | Lack of Knowledge on EHR Operation | 3 | 3 | Medium |
| R10 | Computer System Hanging/Freezing | 3 | 3 | Medium |
| R13 | Unable to Boot Computer | 3 | 3 | Medium |
| R17 | Mechanical Failure (P) | 3 | 3 | Medium |
| R18 | Display/Readout Failure (P) | 3 | 3 | Medium |
| R19 | Wear and Tear (P) | 3 | 3 | Medium |
| R22 | Misinterpretation of Data (H) | 3 | 3 | Medium |
| R04 | Slow Network | 4 | 3 | Medium |
| R05 | Unable to Obtain IP Address | 4 | 3 | Medium |
| R12 | Hardware Damage | 4 | 3 | Medium |
| R21 | Fatigue or Distraction (H) | 4 | 3 | Medium |
| R03 | System Crash | 2 | 4 | Medium |
| R16 | Insufficient Access Control (PH) | 2 | 4 | Medium |
| R01 | Data Loss | 2 | 3 | Medium |
| R15 | Natural Disaster | 1 | 5 | Medium |

The table above shows that the outcome of risk evaluation from identified assets such as data, system and hardware, there are two high level risks which are Virus and Power Outage. Overall, there are twelve other medium level risks which are data entry failure, data mismatch, UPS unable to store power, human error, lack of knowledge on SIMRS operation, computer system hang, inability to boot the computer, data loss, system crash, slow network, inability to obtain IP address and hardware damage.

3.3.2) Examples of Identified Risk

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Likelihood Score | Impact Score | Rating | Example Scenario |
| R01 | Data Loss | 2 | 3 | Medium | Loss of critical patient data due to a backup failure, causing delays in treatments. |
| R02 | Data Entry Failure | 3 | 3 | Medium | Incorrect data entries lead to wrong treatments or diagnoses, impacting patient health. |
| R03 | System Crash | 2 | 4 | Medium | System crash leads to disruption in accessing patient records, delaying treatments. |
| R04 | Slow Network | 4 | 3 | Medium | Reduced network efficiency slows down patient care processes. |
| R05 | Unable to Obtain IP Address | 4 | 3 | Medium | Inability to access critical network resources disrupts healthcare delivery. |
| R06 | Data Mismatch | 3 | 3 | Medium | Integration of incorrect patient data leads to misinformed treatment decisions. |
| R07 | UPS Unable to Store Power | 3 | 3 | Medium | Power failure disrupts operations, risking patient safety. |
| R08 | Human Error | 3 | 3 | Medium | Mistakes in procedures compromise patient safety and operational efficiency. |
| R09 | Lack of Knowledge on EHR Operation | 3 | 3 | Medium | Staff unfamiliarity with EHR systems undermines data accuracy and workflow efficiency. |
| R10 | Computer System Hanging/Freezing | 3 | 3 | Medium | System freezes delay access to critical patient information. |
| R11 | Virus | 3 | 4 | High | Malware infection compromises patient data security and privacy. |
| R12 | Hardware Damage | 4 | 3 | Medium | Physical damage to equipment disrupts healthcare services until repairs are made. |
| R13 | Unable to Boot Computer | 3 | 3 | Medium | Computer boot failure delays access to patient records. |
| R14 | Power Outage | 3 | 4 | High | Extended power outage halts critical medical procedures and patient care. |
| R15 | Natural Disaster | 1 | 5 | High | Severe earthquake causes structural damage to the healthcare facility, requiring evacuation of patients and complete shutdown of operations. |
| R16 | Insufficient Access Control (PH) | 2 | 4 | Medium | Former employee exploits lax access controls to steal patient information, leading to legal and reputational consequences. |
| R17 | Mechanical Failure (P) | 3 | 3 | Medium | Life-support machine failure during operation necessitates emergency intervention. |
| R18 | Display/Readout Failure (P) | 3 | 3 | Medium | Monitor failure during surgery complicates monitoring and patient care. |
| R19 | Wear and Tear (P) | 3 | 3 | Medium | Equipment deterioration affects diagnostic accuracy, requiring regular maintenance. |
| R20 | Inadequate Training (H) | 3 | 4 | High | Poorly trained staff make critical errors in patient care due to insufficient EHR system knowledge. |
| R21 | Fatigue or Distraction (H) | 4 | 3 | Medium | Exhausted healthcare provider administers incorrect medication dosages, endangering patient safety. |
| R22 | Misinterpretation of Data (H) | 3 | 3 | Medium | Clinician misinterprets lab results due to unclear EHR data formatting, leading to incorrect diagnoses. |

# **CHAPTER 4: TREATMENT AND RESPONSE**

## 4.1 Determine Control

Determining control involves identifying and implementing measures that can mitigate or eliminate the risks associated with different assets. This section explains the control measures identified for various assets in the ABC healthcare.

#### Hardware

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assets | Require | Risk Description | Control Measure | Effectiveness | Explanation |
| Database Server 1 & Server 2 | High uptime | Data Loss  Power Outage  UPS Unable to Store Power  System Crash  Computer System  Hanging/Freezing  Hardware Damage  Natural Disaster  Insufficient Access Control  Unable to Obtain IP Address  Display/Readout Failure | Regular backups, RAID setup | High | RAID setup and regular backups ensure data redundancy and quick recovery. |
| Storage Device | Data integrity | Regular backups, RAID setup | High | RAID setup and regular backups ensure data redundancy and quick recovery. |
| Switch 1,2,3,4,5,6,7 | Network connectivity | Redundant switches, regular maintenance | High | Redundant switches and regular maintenance ensure high network availability. |
| PC 1,2,3 | User access | Regular software updates, antivirus | Medium | Regular updates and antivirus reduce risk but cannot completely eliminate software-related issues. |
| MRI Machine 1 | Imaging | Regular maintenance, manufacturer support | High | Regular maintenance and manufacturer support ensure high reliability and quick repairs. |
| Printer | High availability | Regular maintenance, spare parts available | Medium | Regular maintenance helps, but some malfunctions might still occur. |
| Domain Controller | Network management | Strong password policies, regular audits | High | Strong policies and regular audits greatly reduce unauthorized access risk. |
| Network Management System | Network performance | Regular monitoring, timely updates | High | Regular monitoring and timely updates ensure high network performance and reliability. |

#### Software

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assets | Require | Risk Description | Control Measure | Effectiveness | Explanation |
| MySQL  (Database 1 & 2) | |  | | --- | |  |   Data Storage | Data mismatch,  Data Entry Failure  Virus | Regular backups, data validation | High | Regular backups and data validation ensure data integrity and quick recovery. |
| NetApp ONTAP | Data storage | |  | | --- | | Regular backups, RAID setup |  |  | | --- | |  | | High | RAID setup and regular backups ensure data redundancy and quick recovery. |
| Cisco IOS | Network management | Regular updates, security patches | High | Regular updates and security patches minimize vulnerabilities. |
| Active Directory | User management | Strong password policies, regular audits | High | Strong policies and regular audits greatly reduce unauthorized access risk. |
| SolarWinds NPM | Network performance | |  | | --- | | Regular monitoring, timely updates |  |  | | --- | |  | | High | Regular monitoring and timely updates ensure high network performance and reliability. |
| Siemens DotGO | Imaging software | Regular updates, manufacturer support | High | Regular updates and manufacturer support ensure high reliability and quick issue resolution. |
| Windows 11 | User access | |  | | --- | | Regular software updates, antivirus |  |  | | --- | |  | | Medium | updates and antivirus provide good protection but cannot eliminate all vulnerabilities. |
| EHR | Data management | Strong encryption, regular security audits | High | Strong encryption and regular audits ensure high data security and integrity. |
| Microsoft Office Suite | Productivity | Regular backups, secure cloud storage | High | Regular backups and secure cloud storage ensure data integrity and availability. |

#### Human:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assets | Require | Risk Description | Control Measure | Effectiveness | Explanation |
| Dr. Alice Lee  Cancer research scientist | Compatible staff | Inadequate Training &  Human Error | Cross-training, documentation | Medium | Cross-training helps cover key functions, but specialized expertise may still be lacking. |
| Mr. Ben Miller  Research assistant | Supervision, support | Regular training, supervision | Medium | Training reduces errors but cannot completely eliminate them. |
| Dr. Sarah Jones  Board-Certified OB-GYN Physician | Backup specialist | Detailed protocols, backup specialist | Medium | Backup specialist helps, but expertise in high-risk cases may be limited. |
| Ms. Emily Brown  Registered Nurse (Pediatrics) | Additional support | Backup nurse, cross-training | Medium | Cross-training ensures some coverage, but not all skills may be replaceable. |
| Dr. David Smith  Cardiothoracic Surgeon | Backup surgeon | Detailed protocols, backup surgeon | Medium | Backup surgeon helps, but specific expertise may still be lacking. |
| Dr. Michael Chen  Surgical Resident (General Surgery) | Supervision, training | Supervision, regular training | Medium | Supervision reduces errors, but inexperience can still cause issues. |
| Pamela Johnson  Director of Nursing | Leadership training | Leadership training, succession planning | High | Leadership training and succession planning ensure continuity in critical roles. |
| Charles White  Clinical Quality Improvement Specialist | Support staff | Support staff, cross-training | Medium | Cross-training ensures some coverage, but critical skills may still be lacking. |
| Maria Garcia  Board-Certified Internist | Backup internist | |  | | --- | | Cross-training, documentation |  |  | | --- | |  | | Medium | Cross-training helps cover key functions, but specialized expertise may still be lacking. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| William Thomas  Part-Time Physician (Geriatric Medicine) | Adjusted coverage |  | Adjusted coverage, backup support | Medium | Adjusted coverage helps, but patient-specific expertise may still be lacking. |
| Anna Lopez  Healthcare Finance Manager | Backup finance manager | Detailed procedures, backup finance manager | Medium | Backup finance manager helps, but knowledge of complex billing regulations may be lacking. |
| Robert Young  Accounting Assistant | Support staff | Support staff, cross-training | Medium | Cross-training ensures some coverage, but critical skills may still be lacking. |
| Thomas  Biomedical Equipment Technician | Backup technician | Regular maintenance, backup technician | Medium | Regular maintenance and backup technician help, but specific expertise may still be lacking. |
| Elizabeth Brown  Building Maintenance Engineer | Backup engineer | Regular maintenance, backup engineer | Medium | Regular maintenance and backup engineer help, but specific expertise may still be lacking. |

Data

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assets | Require | Risk Description | Control Measure | Effectiveness | Explanation |
| Patient Record | Confidentiality & Data integrity | Data loss or corruption | Regular backups, secure storage | High | Regular backups and secure storage ensure data integrity and availability. |
| Financial Transactions |
| Staff Information |
| Medical Imaging Data |
| Network Log |
| System Access Log |

Physical Assets:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Assets | Require | Risk Description | Control Measure | Effectiveness | Explanation |
| Hospital Bed | Patient care | Hardware Damage | Regular maintenance, manufacturer support | High | Regular maintenance ensures the beds are functional and safe for use. |
| Ventilator | High | Regular maintenance and manufacturer support ensure high reliability and quick repairs. |
| Surgical Table | High | Regular maintenance ensures the surgical tables are functional and safe for use. |
| Patient Monitor | High | Regular maintenance ensures the monitors are functional and accurate. |
| Blood Pressure Monitor | High | Regular maintenance ensures the monitors are functional and accurate |
| Wheelchair | High | Regular maintenance ensures the wheelchairs are functional and safe for use. |
| Ultrasound Machine | Imaging | High | Regular maintenance and manufacturer support ensure high reliability and quick repairs. |
| Office Chair | Staff comfort | |  | | --- | |  |  |  | | --- | |  |   Regular maintenance, replacements   |  | | --- | |  |  |  | | --- | |  | | Medium | Regular maintenance helps, but wear and tear can still occur over time. |
| Waiting Room Chair | Patient comfort | Medium |
| Sofa | Medium |
| Bedside table | Patient care | Medium |
| Conference Table | Meetings | Medium |
| Ambulance | Emergency response | Mechanical failure | Regular maintenance, manufacturer support | High | Regular maintenance and manufacturer support ensure high reliability and quick repairs. |

## 4.2 Selection of Risk Treatment

The selection of risk treatment strategies involves choosing the most appropriate actions to manage identified risks. Each risk treatment type aims to mitigate, transfer, accept, or avoid the risk based on its likelihood and potential impact on the organization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Risk Description | Asset | Treatment Type | Explanation for choosing it |
| R01 | Data Loss | Database Server 1 & 2, Storage Device, Patient Record, Financial Transactions, Staff Information, Medical Imaging Data, Network Log, System Access Log | Risk Mitigate | Regular backups and secure storage significantly reduce the risk of data loss. |
| R11 | Virus | SolarWinds NPM, Windows 11, Microsoft Office Suite, Siemens DotGO | Risk Mitigate | Regular updates and antivirus software help to prevent and mitigate virus infections. |
| R14 | Power Outage | MRI Machine , Ventilator, Surgical Table, Hospital Bed, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Ambulance | Risk Transfer | Obtaining insurance and backup power solutions help to transfer the financial impact. |
|  | Inadequate Training | Medical Staff, Administrative Staff, IT Staff | Risk Mitigate | Comprehensive training programs reduce the likelihood of errors due to inadequate training. |
| R02 | Data Entry Failure | Electronic Health Record (EHR) | Risk Mitigate | Enhanced training and data validation processes minimize the risk of data entry errors. |
| R06 | Data Mismatch | MySQL (Database 1 & 2), NetApp ONTAP | Risk Mitigate | Regular data validation checks reduce the likelihood of data mismatches. |
| R07 | UPS Unable to Store Power | Medical Equipment, Office Equipment, Furniture, Vehicles | Risk Transfer | Insurance and regular maintenance transfer the risk and mitigate potential impacts. |
| R03 | System Crash | PC 1, PC 2, PC 3, Network Management System | Risk Mitigate | Regular maintenance and software updates reduce the risk of system crashes. |
| R08 | Human Error | Medical Staff, Administrative Staff, IT Staff | Risk Mitigate | Ongoing training and monitoring help to reduce the frequency of human errors. |
| R10 | Computer System Hanging/Freezing | Domain Controller, PC 1, PC 2, PC 3 | Risk Mitigate | Regular maintenance and software updates help to prevent system freezing. |
| R12 | Hardware Damage | Storage Device, Printer, MRI Machine, Ventilator, Surgical Table, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Office Chair, Waiting Room Chair, Sofa, Bedside Table, Conference Table | Risk Mitigate | Scheduled maintenance checks reduce the likelihood of hardware damage. |
| R13 | Unable to Boot Computer | Active Directory Domain Service (AD DS) | Risk Accept | Regular backups and user training manage the risk and maintain system availability. |
| R15 | Natural Disaster | All physical assets | Risk Transfer | Comprehensive insurance and a disaster recovery plan transfer and mitigate the impact. |
| R16 | Insufficient Access Control | Active Directory, Domain Controller | Risk Mitigate | Strong access policies and controls reduce the likelihood of unauthorized access. |
| R17 | Mechanical Failure | Medical Equipment & Ambulance | Risk Mitigate | Regular maintenance and checks help to prevent mechanical failures. |
| R18 | Display/Readout Failure | Patient Monitor, Medical Equipment | Risk Mitigate | Regular maintenance and checks reduce the likelihood of display/readout failures. |
| R05 | Unable to Obtain IP Address | Network Management System | Risk Mitigate | Monitoring and regular updates  minimize the risk of failing to  obtain IP addresses. |

## 4.3 Risk Treatment Plan

The risk treatment plan is a structured approach to addressing identified risks within an organization. It involves developing specific actions to mitigate or manage risks, assigning responsibilities, and setting timelines for implementing these actions. The goal is to ensure that risks are managed in a way that aligns with the organization's objectives and risk appetite.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Asset | Treatment Type | Action Plan | Responsible Party | Timeline |
| R01 | Data Loss | Database Server 1 & 2, Storage Device, Patient Record, Financial Transactions, Staff Information, Medical Imaging Data, Network Log, System Access Log | Risk Mitigate | Regular backups and secure storage | IT Department | Immediate |
| R11 | Virus | SolarWinds NPM, Windows 11, Microsoft Office Suite, Siemens DotGO | Risk Mitigate | Implement regular updates and antivirus software | IT Department | Immediate |
| R14 | Power Outage | MRI Machine , Ventilator, Surgical Table, Hospital Bed, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Ambulance | Risk Transfer | Obtain insurance and backup power solutions | Facilities Management | Immediate |
|  | Inadequate Training | Medical Staff, Administrative Staff, IT Staff | Risk Mitigate | Implement comprehensive training programs | HR Department | Ongoing |
| R02 | Data Entry Failure | Electronic Health Record (EHR) | Risk Mitigate | Enhance training and data validation processes | EHR System Admin | Immediate |
| R06 | Data Mismatch | MySQL (Database 1 & 2), NetApp ONTAP | Risk Mitigate | Regular data validation checks | Database Admin | Ongoing |
| R07 | UPS Unable to Store Power | Medical Equipment, Office Equipment, Furniture, Vehicles | Risk Transfer | Obtain insurance and ensure regular maintenance | Facilities Management | Immediate |
| R03 | System Crash | PC 1, PC 2, PC 3, Network Management System | Risk Mitigate | Conduct regular maintenance and software updates | IT Department | Immediate |
| R08 | Human Error | Medical Staff, Administrative Staff, IT Staff | Risk Mitigate | Provide ongoing training and monitoring | HR Department | Ongoing |
| R10 | Computer System Hanging/Freezing | Domain Controller, PC 1, PC 2, PC 3 | Risk Mitigate | Conduct regular maintenance and software updates | IT Department | Immediate |
| R12 | Hardware Damage | Storage Device, Printer, MRI Machine, Ventilator, Surgical Table, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Office Chair, Waiting Room Chair, Sofa, Bedside Table, Conference Table | Risk Mitigate | Schedule regular maintenance checks | Maintenance Team | 1 Month |
| R13 | Unable to Boot Computer | Active Directory Domain Service (AD DS) | Risk Accept | Maintain regular backups and provide user training | IT Department | Immediate |
| R15 | Natural Disaster | All physical assets | Risk Transfer | Acquire comprehensive insurance and develop a disaster recovery plan | |  | | --- | | Facilities Management |  |  | | --- | |  | | 1 Month |
| R16 | Insufficient Access Control | Active Directory, Domain Controller | Risk Mitigate | Implement strong access policies | Security Team | Ongoing |
| R17 | Mechanical Failure | Medical Equipment & Ambulance | Risk Mitigate | Regular maintenance and checks | Maintenance Team | 1 Month |
| R18 | Display/Readout Failure | Patient Monitor, Medical Equipment | Risk Mitigate | Regular maintenance and checks | Maintenance Team | Immediate |
| R05 | Unable to Obtain IP Address | Network Management System | Risk Mitigate | Monitoring and regular updates | IT Department | Immediate |

## 4.4 Residual Risk

Residual risk is the amount of risk that remains after risk treatment measures have been applied. Despite implementing various control measures to mitigate risks, some level of risk often persists, which is known as residual risk. It is important for organizations to identify, assess, and manage these residual risks to ensure they do not adversely affect their operations or objectives.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Asset | Initial Risk Level | Treatment Type | Residual Risk Level | Description |
| R01 | Data Loss | Database Server 1 & 2, Storage Device, Patient Record, Financial Transactions, Staff Information, Medical Imaging Data, Network Log, System Access Log | Medium | Risk Mitigate | Low | Regular backups and secure storage significantly reduce the risk, but minor residual risk remains. |
| R11 | Virus | SolarWinds NPM, Windows 11, Microsoft Office Suite, Siemens DotGO | High | Risk Mitigate | Low | Regular updates and antivirus reduce the risk, with minimal residual risk. |
| R14 | Power Outage | MRI Machine , Ventilator, Surgical Table, Hospital Bed, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Ambulance | High | Risk Transfer | Low | Insurance and backup power solutions reduce the impact, with minimal residual risk. |
| R20 | Inadequate Training | Medical Staff, Administrative Staff, IT Staff | High | Risk Mitigate | Medium | Comprehensive training programs reduce the risk, but some residual risk remains. |
| R02 | Data Entry Failure | Electronic Health Record (EHR) | Medium | Risk Mitigate | Low | Training and validation reduce the risk, with minimal residual risk. |
| R06 | Data Mismatch | MySQL (Database 1 & 2), NetApp ONTAP | Medium | Risk Mitigate | Low | Regular validation eliminates most mismatches, with minimal residual risk. |
| R07 | UPS Unable to Store Power | Medical Equipment, Office Equipment, Furniture, Vehicles | Medium | Risk Transfer | Low | Insurance and backup power reduce the financial impact, with minimal residual risk. |
| R03 | System Crash | PC 1, PC 2, PC 3, Network Management System | Medium | Risk Mitigate | Low | Regular updates and monitoring reduce the risk, with minimal residual risk. |
| R08 | Human Error | Medical Staff, Administrative Staff, IT Staff | Medium | Risk Mitigate | Medium | Training reduces errors, but human error cannot be completely eliminated. |
| R10 | Computer System Hanging/Freezing | Domain Controller, PC 1, PC 2, PC 3 | Medium | Risk Mitigate | Low | Regular maintenance and updates reduce the risk, with minimal residual risk. |
| R12 | Hardware Damage | Storage Device, Printer, MRI Machine, Ventilator, Surgical Table, Patient Monitor, Blood Pressure Monitor, Ultrasound Machine, Office Chair, Waiting Room Chair, Sofa, Bedside Table, Conference Table | |  | | --- | | Medium |  |  | | --- | |  | | Risk Mitigate | Low | Regular maintenance reduces the risk, but some minor residual risk remains. |
| R13 | Unable to Boot Computer | Active Directory Domain Service (AD DS) | Medium | Risk Accept | Medium | Regular backups and user training help manage the risk, but some residual risk is accepted. |
| R15 | Natural Disaster | All physical assets | Medium | Risk Transfer | Low | Insurance and disaster recovery plans mitigate the impact, with minimal residual risk. |
| R16 | Insufficient Access Control | Active Directory, Domain Controller | Medium | Risk Mitigate | Low | Strong policies and audits minimize the risk, but some residual risk remains. |
| R17 | Mechanical Failure | Medical Equipment & Ambulance | Medium | Risk Mitigate | Low | Regular maintenance reduces the risk, with minimal residual risk. |
| R18 | Display/Readout Failure | Patient Monitor, Medical Equipment | Medium | Risk Mitigate | Low | Regular maintenance reduces the risk, with minimal residual risk. |
| R05 | Unable to Obtain IP Address | Network Management System | Medium | Risk Mitigate | Low | Monitoring and updates minimize the risk, but some residual risk remains. |

**CHAPTER 5: RISK ACCEPTANCE**

**CHAPTER 6: CONCLUSION**

**CHPATER 7: LIMITATION**

**PREFERENCE**

**APPENDIX**