Sri Lanka Institute of Information Technology

Security Report
Winlanka Hospital (Pvt) Ltd
Group Assignment

IE3052 -Information Security Risk Management

Submitted by:

Student Registration Number	Student Name
IT22230010	UMAYANGA.H.L.A
IT22083678	SAHAN H. P. T
IT22249852	KARUNARATHNA P.M.T. L
IT22121592	HERATH H M C.H. K

Date of submission
02.05.2025

Table of Contents

1.Executive Summary

This report outlines an information security risk assessment of Winlanka Hospital, a private healthcare facility in Sri Lanka employing 165 staff across clinical and administrative roles. The assessment follows the OCTAVE Allegro methodology and is supported by the NIST Cybersecurity Framework for continuous improvement and risk mitigation.

In an increasingly digital healthcare environment, the hospital's reliance on systems such as Electronic Health Records (EHR), Hospital Information Systems (HIS), and medical IoT devices expose it to growing cyber threats. Ensuring the confidentiality, integrity, and availability of sensitive health data is critical for patient trust and service continuity.

The assessment identifies several key vulnerabilities, including outdated device firmware, inadequate access control, lack of network segmentation, and the absence of a formal incident response plan. These pose significant risks under Sri Lanka's Personal Data Protection Act (PDPA), which mandates strong controls over the collection, processing, and storage of personal data, particularly in the healthcare sector.

To strengthen its security posture, Winlanka Hospital must implement multi-factor authentication, role-based access controls, staff awareness training, routine vulnerability scans, and tested disaster recovery procedures. Institutionalizing governance with clear policies and assigned responsibilities will further support compliance with local laws and enhance resilience against threats

1.1 Overview of Hospital Environment

Winlanka Hospital is a mid-sized, privately owned healthcare institution located in Nugegoda, Sri Lanka. With a staff strength of approximately 165 individuals—including clinical, administrative, and technical teams, the hospital delivers 24/7 care to patients from Colombo and surrounding suburbs. It offers a comprehensive range of clinical and diagnostic services with a focus on patient-centered care and operational efficiency.

The hospital's core functions are supported by the following key operational departments:

- **Clinical Services**: Inpatient wards, Intensive Care Units (ICUs), surgical theatres, pediatrics, and outpatient clinics
- **Support Services**: Pharmacy, clinical laboratory, radiology, and biomedical engineering
- **Administrative Functions**: Human resources, finance, procurement, and facilities management
- **IT & Information Security**: Manages EHR, HIS, network infrastructure, backups, and system security
- **Quality & Compliance**: Ensures regulatory compliance, conducts internal audits, and oversee risk mitigation activities

The hospital is led by an executive team comprising the Medical Director, Chief Operations Officer (COO), and Chief Information Officer (CIO), in collaboration with departmental heads. This governance structure promotes both clinical excellence and accountability in operations.

From a technological perspective, Winlanka Hospital heavily relies on integrated digital systems such as the Electronic Health Records (EHR) platform, Hospital Information System (HIS), and Medical IoT devices like patient monitors and infusion pumps. These are supported by the hospital's internal network infrastructure, secure communication systems (email, paging), and basic backup and disaster recovery capabilities. Given the critical nature of its services and sensitive patient data, ensuring confidentiality, integrity, and availability of information systems is fundamental to Winlanka Hospital's commitment to safety, compliance, and public trust.

1.2 Key Information Security Issues

The risk assessment conducted at Winlanka Hospital has revealed several pressing information security issues across its critical systems and operational domains. These issues pose substantial risks to patient safety, data privacy, service continuity, and regulatory compliance if not adequately addressed:

1. Lack of Multi-Factor Authentication (MFA) for Clinical and Administrative Access

Many hospital systems, including the EHR and HIS platforms, rely solely on single-factor authentication methods. This leaves critical accounts vulnerable to credential-based attacks, particularly through phishing, insider misuse, or brute-force techniques. Given the sensitivity of patient health data, this represents a high-risk vulnerability.

2. Inadequate Segmentation of Network Infrastructure

The hospital's internal network lacks sufficient segmentation between administrative, clinical, and IoT zones. This flat network design increases the risk of lateral movement by threat actors once a single device or user account is compromised.

3. Weak Backup Validation and Limited Disaster Recovery Testing

Although Winlanka Hospital maintains routine data backups, the process for validating the integrity of backup files and testing disaster recovery procedures is infrequent and informal. This raises concerns about the hospital's ability to restore systems quickly during a ransomware attack or system failure.

4. Insufficient Logging and Monitoring

Winlanka hospital systems including firewalls, EHR platforms, and communication tools lack centralized logging or real-time monitoring. This limits the ability to detect anomalies, unauthorized access, or potential data exfiltration in a timely manner.

5. Outdated Physical Security Controls

The current CCTV systems and RFID access controls used across sensitive areas such as ICUs, pharmacies, and data centers are outdated and lack modern tamper detection or monitoring integrations. Physical security weaknesses may result in unauthorized access to restricted spaces or equipment.

6. Limited Cybersecurity Awareness Among Staff

Medical and administrative staff demonstrate varied levels of cybersecurity awareness. Social engineering, phishing, and improper data handling remain common risks due to a lack of structured training and simulated attack exercises.

These issues collectively expose Winlanka Hospital to a variety of cyber threats that could jeopardize patient safety, operational integrity, and legal standing. Addressing these concerns with a combination

of technical controls, policy enforcement, and awareness programs is critical to fortifying the hospital's security posture.

7. Absence of a Documented Incident Response Plan (IRP)

Currently, Winlanka Hospital lacks a formal, structured incident response plan that outlines escalation procedures, stakeholder roles, communication protocols, and recovery steps in the event of a cybersecurity incident. Without a tested IRP, the hospital is at risk of delayed containment, uncoordinated responses, and regulatory non-compliance during breaches. The absence of such a plan could exacerbate the impact of incidents, especially those involving ransomware, patient data theft, or operational system failure.

1.3 Recommendations

Based on the identified vulnerabilities and gaps, the following recommendations are proposed to enhance the security posture of Winlanka Hospital. These measures align with best practices from the NIST Cybersecurity Framework and healthcare-specific standards such as ISO 27799 and the Sri Lanka Personal Data Protection Act (PDPA).

1. Enforce Multi-Factor Authentication (MFA) for All Critical Systems

Implement phishing-resistant MFA (e.g., authenticator apps or FIDO2 hardware tokens) across all clinical, administrative, and IT platforms including EHR, HIS, and email systems. Avoid SMS-based MFA where possible. Use centralized Identity and Access Management (IAM) for consistent enforcement.

2. Implement Robust Network Segmentation

Redesign the internal network to segment clinical systems, administrative platforms, IoT devices, and guest access. Use VLANs, access control lists (ACLs), and internal firewalls to restrict lateral movement. Enforce least privilege access to reduce attack surface.

3. Formalize and Automate Backup Validation and Recovery Testing

Upgrade backup systems to include encrypted, automated, and versioned backups. Schedule monthly validation and simulated recovery exercises. Ensure that both on-site and off-site (cloud-based) backups follow geo-redundancy principles.

4. Deploy Centralized Logging and Real-Time Monitoring

Integrate Security Information and Event Management (SIEM) tools to collect logs from EHR, HIS, firewalls, and servers. Use tools like Microsoft Sentinel or Elastic Stack to monitor anomalies, privilege misuse, and unauthorized access attempts.

5. Upgrade in Physical Security Systems

Modernize CCTV and RFID systems with real-time monitoring, tamper detection, and audit logging. Conduct periodic physical security assessments and limit access to high-risk zones such as the server room, pharmacy, and ICU.

6. Develop and Deliver Continuous Cybersecurity Awareness Training

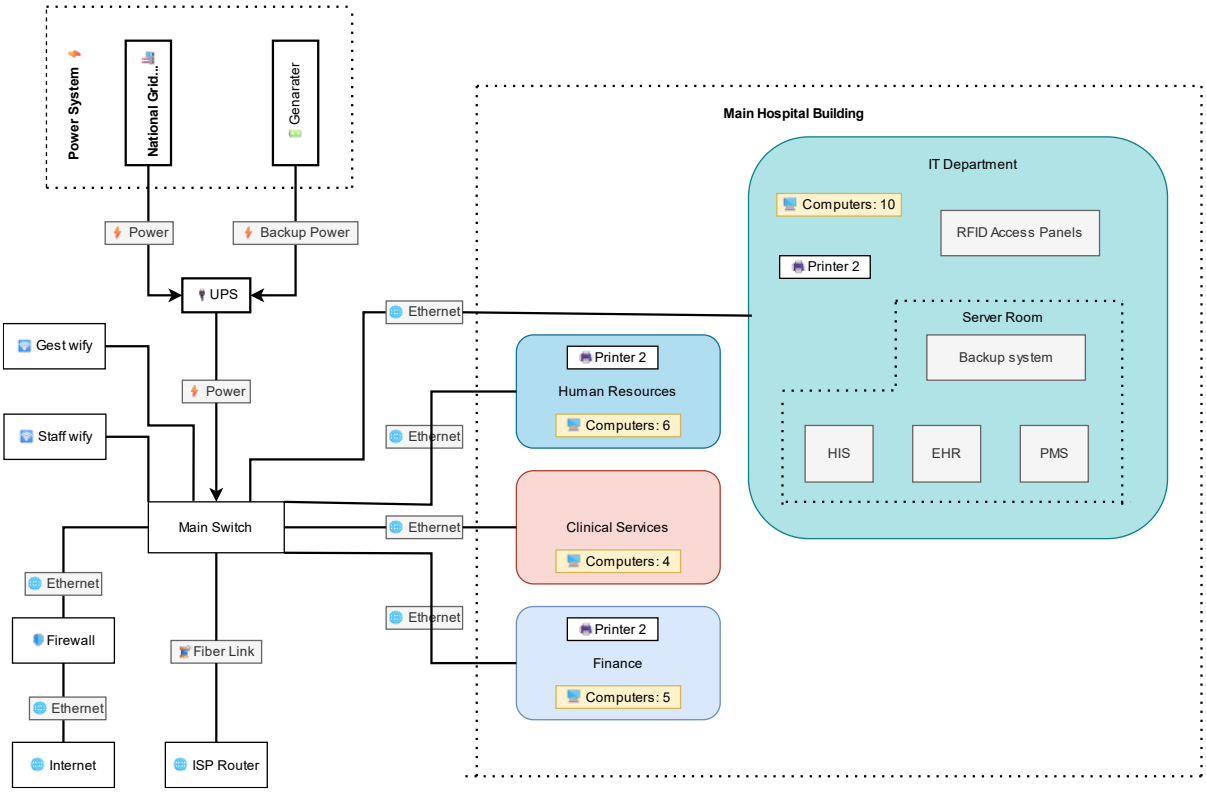
Launch an annual cybersecurity training program tailored to healthcare staff. Include modules on phishing, safe data handling, and reporting suspicious activity. Supplement with simulated phishing campaigns and scenario-based exercises.

7. Establish a Documented Incident Response Plan (IRP)

Develop a formal IRP outlining detection, escalation, containment, communication, and recovery procedures. Define clear roles for IT, clinical, and administrative staff. Conduct quarterly tabletop exercises and integrate the plan into business continuity frameworks.

By implementing these recommendations, Winlanka Hospital can significantly reduce its exposure to cyber threats, ensure regulatory compliance, and safeguard patient safety and trust. Each initiative should be accompanied by measurable KPIs to evaluate effectiveness and inform continuous improvement.

2. Asset Identification: OCTAVE Methodology



2.1 Methodology for Risk Identification

Winlanka Hospital is a privately owned healthcare institution with approximately 165 employees, providing a wide range of medical, surgical, and diagnostic services to patients in the Colombo region. The hospital operates with a blend of on-premises infrastructure including servers, internal network systems, and Medical IoT devices and cloud-based services used for records storage and administrative functions.

To assess the hospital's cybersecurity posture, we applied the OCTAVE Allegro risk assessment framework, which is particularly well-suited for healthcare institutions due to its structured, asset-centric, and flexible approach. The assessment was conducted in April 2025 and involved a combination of interviews, departmental consultations, system analysis, and workflow reviews.

The following departments participated in the assessment:

1. Clinical Services
2. IT & Information Security
3. Administration & Human Resources
4. Finance
5. Health Informatics

By leveraging OCTAVE Allegro, we followed a systematic process to:

1. Identify critical information assets supporting clinical care and operations
2. Assess threats and vulnerabilities to those assets, both digital and physical
3. Evaluate risk impact and likelihood, including patient safety, legal compliance
4. Recommend appropriate mitigation strategies to achieve an acceptable level of risk

This is the first formal security assessment conducted at Winlanka Hospital. Through a structured methodology and cross-departmental collaboration, we identified 5 critical assets essential to the hospital's operations:

1. Hospital Information System (HIS)
2. Internal Network Infrastructure
3. Backup and Disaster Recovery Systems
4. Communication Platforms
5. Physical Security Systems (CCTV, RFID Access)

We also identified the following key impact areas relevant to the hospital:

1. Patient Safety and Trust
2. Operational Continuity
3. Regulatory and Legal Compliance
4. Financial Stability
5. Reputation and Public Confidence

All findings were documented using OCTAVE Allegro Worksheet No. 8 and No.10, forming the foundation for our risk evaluation and treatment plan. These worksheets detail asset profiles, threat sources, impact ratings, and recommended controls offering a repeatable approach for future assessments.

2.2 Stakeholder Involvement & Scope

The cybersecurity risk assessment at Winlanka Hospital involved key stakeholders from clinical, administrative, and technical departments to ensure an accurate, real-world understanding of system dependencies and risks.

Key Stakeholders:

- Medical Director
- Health Informatics Unit
- HR and Finance
- IT Team
- Department Heads (HODs)

Scope of Assessment:

- Patient care systems
- Core infrastructure
- Data protection
- Communication systems

Third-party vendor systems and external hosting infrastructure were excluded from the current scope and may be assessed in future phases. This collaborative approach ensured a complete and practical view of cybersecurity risks within the hospital environment.

3. Analysis of Security Risks

3.1 Identification of Critical Assets

Critical Assets	Reasoning	Description	Security Requirement
Hospital Information System (HIS)	Core system for managing clinical workflows, patient admissions, billing, lab orders, and discharge summaries. Any compromise affects care delivery.	Software platform supporting hospital operations across departments; integrated with labs, pharmacy, and external partners via APIs.	Confidentiality, Integrity, Availability
Internal Network Infrastructure (Switches, Routers, VLANs, Firewalls)	Backbone of the hospital's digital ecosystem. Improper segmentation or insecure configurations may lead to widespread disruption or compromise.	Network devices and logical segmentation managing data flow across EHR, HIS, IoT, guest Wi-Fi, and external services. Includes firewall and IDS/IPS components.	Availability, Integrity, Confidentiality
Backup and Disaster Recovery Systems	Ensures data recovery and service continuity after cyber incidents or technical failures. Vital to prevent permanent data loss.	On-site and off-site backup systems for patient records, HIS/EHR databases, and imaging systems. Includes disaster recovery plans and testing protocols.	Availability, Integrity
Communication Platforms (Email, Paging)	Essential for internal coordination and emergency alerts. Exploits like phishing or misused paging systems can lead to operational breakdown.	Email services for clinical/admin use and intercom/paging systems used in patient alerts and emergency broadcasting. Some systems may use VoIP or unencrypted channels.	Confidentiality, Integrity, Availability
Physical Security Systems (CCTV, RFID Access)	Prevents unauthorized physical access to sensitive zones like server rooms, ICUs, and pharmacy. Misuse can result in data theft or safety violations.	Network-connected surveillance and access control systems monitoring physical spaces. Includes RFID-based entry, IP-CCTV, and video archive storage.	Availability, Confidentiality, Integrity

Following the creation of asset profiles, we proceeded to assess vulnerabilities associated with those assets. This evaluation was carried out using the Allegro framework's Phase 1, specifically processes 3 and 4, which are designed to identify vulnerabilities and threats in order to develop a threat profile for each threat targeting critical assets. To accomplish this task, we utilized Allegro Worksheet No. 10. The completed threat profiles can be found in the appendix section (C. Worksheet 10 – Identifying Information Asset Risk (Threat and risk profiles)). Below, you will find a summary of each threat profile, organized according to their corresponding critical assets.

3.1.1 Hospital Information System (HIS)

Privilege Misuse by Internal Staff

Threat Profile:

The Hospital Information System (HIS) is accessible by various hospital departments including administration, finance, and clinical staff. We observe that several accounts have excessive permissions, with staff in non-clinical roles having access to sensitive modules such as lab results or patient discharge summaries. This creates the potential for intentional data misuse or accidental exposure. Given that healthcare staff frequently multitask across terminals, this threat has a high probability of exploitation, especially in absence of proper access reviews.

Impact Assessment:

- Unauthorized access may lead to exposure of sensitive health or billing information.
- Patients may lose trust in the hospital's ability to safeguard their personal data.
- May result in violations of PDPA (Sri Lanka) or international healthcare compliance standards.

Mitigation Approach:

- Implement role-based access control (RBAC) to ensure staff only access modules relevant to their job.
- Conduct quarterly access reviews to detect and remove excessive privileges.
- Log all access to sensitive modules and audit user behavior analytics (UBA) for anomaly detection.

Lack of Multi-Factor Authentication (MFA) for Clinical and Administrative Access

Threat Profile:

Winlanka Hospital's clinical and administrative systems lack Multi-Factor Authentication (MFA), relying solely on single-factor authentication methods such as passwords. This makes it easier for attackers to gain unauthorized access using stolen or compromised credentials. With healthcare systems storing sensitive patient data and critical operational information, this vulnerability poses significant risks to confidentiality, integrity, and availability.

Impact Assessment:

- Unauthorized access to patient records, medical histories, and other sensitive data could lead to privacy violations and regulatory non-compliance

- Attackers could modify critical patient data, leading to incorrect diagnoses, treatments, or medication errors, which directly endanger patient safety.

Mitigation Approach:

- Enforce MFA for all clinical and administrative accounts, especially those with privileged access. Preferred methods include FIDO2 security keys or authenticator apps
- Use an IAM solution to enforce consistent authentication policies across all systems, ensuring that MFA is mandatory for all critical accounts.

3.1.2 Internal Network Infrastructure (Switches, Routers, VLANs, Firewalls)

Flat Network Exposure to East-West Lateral Movement

Threat Profile:

Winlanka Hospital's internal LAN environment lacks effective segmentation between critical assets and general-use devices. Systems like EHR, medical IoT, and admin PCs share common broadcast domains, allowing east-west traffic without restriction. A threat actor compromising a single endpoint (e.g., via phishing) could easily move laterally across the network, probing or attacking adjacent systems, a well-documented technique used in modern healthcare-targeted ransomware campaigns.

Impact Assessment:

• Attackers could gain unauthorized access to clinical data servers, lab systems, or storage appliances.
• Threats like Conti or Ryuk ransomware could traverse flat networks and rapidly encrypt data across departments.
• Critical services could become unavailable, affecting patient safety and business continuity.

Mitigation Approach:

• Implement 802.1Q VLAN segmentation with inter-VLAN firewalls.
• Enforce east-west micro segmentation using internal firewalls or SDN-based ZTNA.
• Restrict inter-zone communication using firewall policies, host-based ACLs, and traffic profiling.

Default SNMP Strings and Telnet on Core Switches

Threat Profile:

Network switches and routers deployed in the hospital were found using default SNMPv2c community strings (“public”), and Telnet was enabled for remote administration. These configurations expose the network to device takeover, packet sniffing, and route poisoning. Attackers with internal access (even on guest Wi-Fi) could use common scanning tools like SNMPwalk or Nmap scripts to discover and manipulate network infrastructure.

Impact Assessment:

• Malicious reconfiguration or shutdown of switch ports can disrupt EHR access, VoIP communication, or medical IoT sensors.

• MitM attacks may allow credential theft or manipulation of live traffic.
• Could lead to total compromise of network trust boundaries and data in transit.

Mitigation Approach:

• Disable Telnet; enforce SSHv2-only access with key-based authentication.
• Change default SNMP community strings and upgrade to SNMPv3 with encryption.
• Use Access Control Lists (ACLs) and management VLANs to isolate control-plane traffic.

Overly Permissive Firewall ACLs and Blind IDS Zones

Threat Profile:

Our team found out that Winlanka Hospital's perimeter and internal firewalls revealed default-allow rules, wide-open port ranges, and unused legacy rules still active. In addition, IDS/IPS sensors are not deployed on lateral traffic paths (e.g., between admin VLAN and HIS/EHR segments). This creates blind spots that modern malware, APTs, or botnets can exploit without triggering alerts a known tactic seen in breaches like Anthem (2015) or SingHealth (2018).

Impact Assessment:

• Lack of visibility enables stealthy persistence, data exfiltration, or command-and-control (C2) channels.
• Poorly tuned firewalls can fail to block unauthorized services, like exposed RDP or SMBv1.
• Post-incident forensics may lack packet-level insight due to absence of inline monitoring.

Mitigation Approach:

• Conduct a firewall rulebase cleanup using policy reviews and shadow rule analysis.
• Deploy intrusion sensors (e.g., Suricata, Zeek, or commercial IDS) on internal VLAN interlinks.
• Integrate firewall and IDS logs with a central SIEM and configure alerts for anomaly-based patterns.

3.1.3 Backup and Disaster Recovery Systems

Outdated or Weak Backup Encryption

Threat Profile:

Winlanka Hospital performs scheduled backups of critical systems like EHR, HIS, and imaging databases. However, a review of the disaster recovery setup revealed that some backup archives use outdated encryption methods or no encryption at all, especially for legacy storage on NAS devices. This creates a serious confidentiality risk in case of physical theft or remote compromise. The probability of exploitation is medium, but the impact is critical in a healthcare environment where patient data sensitivity is high.

Impact Assessment:

- Attackers accessing unencrypted backup files may steal or leak sensitive patient information.
- Legal and regulatory consequences under PDPA and health sector privacy regulations.
- Reputational loss due to breach disclosure and erosion of patient trust.

Mitigation Approach:

- Transition to AES-256 encryption for all backup archives—both at rest and in transit.
- Enforce encryption during the entire backup lifecycle, including during staging and restoration.
- Store encryption keys securely, using hardware security modules (HSMs) or centralized key management systems.

Lack of Regular Validation and Recovery Testing

Threat Profile:

Although Winlanka Hospital performs daily and weekly backups, the IT department lacks a formal process to test restoration of backups. A recent simulated recovery attempt revealed that a key EHR backup was incomplete due to silent corruption. Without regular validation, the hospital is at risk of relying on unusable data during emergencies. This threat has a medium to high probability due to common human and technical error.

Impact Assessment:

- Inability to restore critical patient records could delay treatments, especially in emergency wards or ICUs.
- Loss of data may interrupt billing, pharmacy, or insurance workflows.
- Prolonged system downtime affects both clinical operations and administrative continuity.

Mitigation Approach:

- Perform monthly test restores of randomly selected backups to validate data integrity.
- Use automated backup validation tools that can report anomalies or failures.
- Include backup validation and restoration drills as part of the hospital's Business Continuity Plan (BCP).

3.1.4 Communication Platforms (Email, Paging)

Phishing and Business Email Compromise (BEC)

Threat Profile:

Email is a primary communication tool at Winlanka Hospital for internal coordination, patient updates, lab results, and external interactions with suppliers or insurance firms. However, the hospital currently lacks a dedicated phishing protection solution, and several email accounts are protected only by single-factor authentication. This opens up a high-probability threat of phishing or Business Email Compromise (BEC), where attackers impersonate doctors or finance staff to steal data or redirect payments.

Impact Assessment:

- Successful phishing attacks can lead to exposure of patient information or financial fraud.
- Staff may unintentionally download malware or ransomware from malicious links or attachments.

- Compromised hospital emails could erode trust with patients and partners, especially if misused.

Mitigation Approach:

- Enforce multi-factor authentication (MFA) for all email accounts.
- Deploy email security gateways with sandboxing for attachments and real-time link inspection.
- Conduct simulated phishing training quarterly to improve staff vigilance.
- Implement DMARC, SPF, and DKIM for email domain authentication and spoofing prevention.

Unsecured Intercom and Paging Systems

Threat Profile:

Winlanka Hospital uses overhead paging and intercom systems for urgent care calls, shift coordination, and emergency alerts. However, these systems are not encrypted, and access control is minimal, with several physical paging terminals left unattended. In some zones, these systems run over IP networks without segmentation, making them vulnerable to signal injections or denial-of-service attacks. The probability of misuse is medium, but the operational impact is significant during emergencies.

Impact Assessment:

- Attackers or pranksters could issue false emergency alerts, causing panic or workflow disruption.
- Critical communications may be interrupted or hijacked, delaying emergency response.
- Unmonitored terminals could allow insiders to misuse the announcement system for unauthorized messages.

Mitigation Approach:

- Enforce physical access control for all paging terminals (e.g., RFID locks, keypad access).
- Upgrade to secure VoIP paging systems with encrypted channels (e.g., SIP over TLS).
- Segment paging system traffic onto a dedicated VLAN, separate from other clinical or admin networks.
- Maintain event logs and audio records for sensitive broadcast zones.

3.1.5 Physical Security Systems (CCTV, RFID Access)

Unsecured IP-Based CCTV Systems

Threat Profile:

Winlanka Hospital uses IP-based CCTV cameras across wards, corridors, server rooms, and entry points for surveillance and incident documentation. However, several cameras are deployed with default admin

credentials, and video feeds are accessible via unencrypted web interfaces. Without proper network isolation, attackers could gain access to live feeds or tamper with recordings, leading to privacy violations or compromised investigations. The likelihood is medium to high, especially from internal actors or external attackers who gain network access.

Impact Assessment:

- Exposure of CCTV footage could violate patient confidentiality and dignity, especially in ICU or pediatric wards.
- Attackers may disable or erase surveillance data, hindering forensic investigations after physical or cyber incidents.
- Could lead to non-compliance with healthcare security regulations and civil liabilities.

Mitigation Approach:

- Enforce unique credentials and disable unused services on all CCTV devices.
- Enable TLS encryption for accessing CCTV interfaces and configure centralized logging.
- Place CCTV infrastructure on a dedicated VLAN, separated from clinical and admin systems.
- Store recordings in tamper-proof, access-controlled archives, backed by regular integrity checks.

RFID Access Misuse and Credential Cloning

Threat Profile:

Access to sensitive hospital zones such as the server room, pharmacy, and ICU is controlled via RFID badge systems. However, multiple staff share access badges, and lost/stolen cards are not always revoked promptly. Moreover, older-generation RFID systems are vulnerable to cloning attacks using low-cost tools. The threat of unauthorized physical access is therefore medium to high, particularly from insiders or determined attackers.

Impact Assessment:

- Unapproved entry to critical areas can lead to data theft, tampering with medical systems, or medication theft.
- Potential sabotage or insider threat scenarios where attackers gain proximity to networking or backup devices.
- Violations of internal policy and potential compromise of confidential records or systems.

Mitigation Approach:

- Upgrade RFID infrastructure to smartcards with encryption and anti-cloning technology (e.g., MIFARE DESFire).
- Implement badge monitoring software that logs access by date, time, and user ID.
- Enforce lost card reporting policies and allow immediate card deactivation via central system.
- Combine RFID with biometric verification or PIN for high-risk areas

4.Summary of Recommendations

This report presents the results of a comprehensive cybersecurity risk assessment conducted for Winlanka Hospital, a leading healthcare service provider in Sri Lanka. Using the OCTAVE Allegro methodology and mapped against the NIST Cybersecurity Framework, the assessment aimed to identify critical information assets, assess threats and vulnerabilities, and recommend mitigation strategies aligned with industry best practices.

The evaluation revealed several high-risk issues across core systems, including the Hospital Information System (HIS), Internal Network Infrastructure, Backup and Disaster Recovery mechanisms, Communication Platforms, and Physical Security Systems. These vulnerabilities, if left unaddressed, could result in unauthorized data access, service disruptions, reputational damage, and regulatory violations.

Key issues identified include excessive user privileges, absence of multi-factor authentication (MFA), flat network architecture, unencrypted or outdated backups, phishing susceptibility, and unsecured physical access systems. The hospital's infrastructure lacked consistent enforcement of critical security controls such as segmentation, backup validation, and access logging.

While Winlanka Hospital has basic IT security practices in place, it had not conducted a structured risk assessment prior to this exercise. As a result, several systems operate with outdated configurations or insufficient protections. Backup systems were vulnerable due to weak encryption and lack of recovery testing. Communication systems lacked phishing protection and email domain authentication. Physical access systems were outdated, exposing critical areas to misuse.

To improve resilience, the hospital should implement RBAC, MFA, VLAN segmentation, AES-256 encryption, phishing defenses, and regular backup recovery testing. Enhancing governance, training staff, and integrating logs into a centralized SIEM will further improve incident visibility and reduce exposure to modern threats.

5. References

• Carnegie Mellon University – SEI (2007). *OCTAVE Allegro: Improving Information Security Risk Assessments*. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

• National Institute of Standards and Technology (NIST) (2018). *Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework v1.1)*. Available at: https://www.nist.gov/cyberframework

• ISO (2016). *ISO/IEC 27799: Health Informatics – Information Security Management in Health Using ISO/IEC 27002*. Available at: https://www.iso.org/standard/62777.html

• National Institute of Standards and Technology (NIST) (2020). *Digital Identity Guidelines: SP 800-63B*. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html

• National Institute of Standards and Technology (NIST) (2005). *SP 800-58: Security Considerations for VoIP Systems*. Available at: https://csrc.nist.gov/publications/detail/sp/800-58/final

• Sri Lanka Parliament (2022). *Personal Data Protection Act No. 9 of 2022*. Available at: https://www.icta.lk/personal-data-protection

6.Security Planning OCTAVE

6.1Appendices

6.1.1 Worksheet 8 – Identification of Critical Assets

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Hospital Information System (HIS)	Core to clinical and administrative operations. Enables patient registration, billing, lab processing, discharge.	Integrated platform for managing hospital workflows, connecting with departments like pharmacy, labs, radiology, and external systems via APIs.
(4) Owner(s) *Who owns this information asset?*		
IT Department and Hospital Administration		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: **Medical staff, Administrative staff , IT administrators**	**High**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: **Medical staff, IT administrators**	**High**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: This asset must be available for **24** hours, **7** days/week**, 52** weeks/year.	**High**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: **ISO 27001, NIST, GDPR, and SOC 2**.	**Medium**
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	✓ Availability ❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Internal Network Infrastructure	Backbone of all hospital communication. Any compromise can lead to widespread data breaches, service downtime, and attack propagation.	Physical and virtual network components that manage internal and external traffic, including VLANs, firewall rules, routing, and switch
(4) Owner(s) *Who owns this information asset?*		
Network Security Team and IT Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: **IT administrators, Network engineers**	**High**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: **IT administrators, Network engineers**	**High**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: This asset must be available for **24** hours, **7** days/week**, 52** weeks/year.	**High**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: **ISO 27001, NIST, GDPR, and SOC 2**.	**Medium**
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	✓ Availability ❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Backup and Disaster Recovery Systems	Ensures continuity of operations during system failures, cyberattacks, or data loss. Critical for restoring patient and hospital data.	Systems responsible for backing up electronic health records (EHR), HIS, imaging data, and operational databases, including both on-site and off-site storage and disaster recovery procedures.
(4) Owner(s) *Who owns this information asset?*		
IT Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: **Medical staff, Administrative staff, IT administrators**	**High**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: **Medical staff, IT administrators**	**High**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: This asset must be available for **24** hours, **7** days/week**, 52** weeks/year.	**High**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: **PDPA Sri Lanka 2022,ISO 27001, NIST, GDPR, and SOC 2**.	**Medium**
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	✓ Availability ❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Communication Platforms (Email, Paging)	Critical for operational coordination, emergency responses, and sharing medical updates. Exploitable by phishing or misuse.	Includes internal and external email systems, paging/intercom systems, and broadcast tools used for daily operations, clinical updates, and emergencies.

(4) Owner(s) *Who owns this information asset?*
IT Department and Hospital Operations Team

(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: **Medical staff, Administrative staff, IT administrators**	**High**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: **Medical staff, Administrative staff, IT administrators**	**High**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: This asset must be available for **24** hours, **7** days/week**, 52** weeks/year.	**High**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: **Sri Lanka's PDPA, ISO 27001, ISO 27799, NIST Cybersecurity Framework, and GDPR**	**High**

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	✓ Integrity	❑ Availability	❑ Other

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Physical Security Systems (CCTV, RFID Access)	Controls physical access to critical hospital areas such as server rooms, ICUs, pharmacies, and admin offices. Prevents unauthorized entry and protects evidence trails.	Includes IP-based CCTV surveillance systems and RFID badge readers used for staff access control. Often integrated with internal networks and storage systems.
(4) Owner(s) *Who owns this information asset?*		
Facilities Security Team and IT Security Department		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows: **Medical staff, Administrative staff, IT administrators**	**High**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows: **IT administrators, Facilities Security Team**	**High**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows: This asset must be available for **24** hours, **7** days/week**, 52** weeks/year.	**High**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows: **ISO 27001, NIST, GDPR, and SOC 2**.	**Medium**
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	✓ Availability	❑ Other

6.2.1 Identified Vulnerabilities and Threat Sources

Asset	Vulnerability	Definition & Description
Hospital Information System (HIS)	Privilege Misuse by Internal Staff	Excessive access rights allow non-clinical staff to view or modify sensitive health records, increasing risk of unauthorized access or data leakage.
	Lack of Multi-Factor Authentication (MFA)	HIS access is protected only by passwords, making it vulnerable to credential theft and brute-force attacks, especially for privileged roles.
Internal Network Infrastructure (Switches, Routers, VLANs, Firewalls)	Flat Network Exposure to East-West Lateral Movement	Lack of proper VLAN segmentation allows attackers to move laterally between departments and systems once inside, increasing attack impact.
	Default SNMP Strings and Telnet on Core Switches	Use of default SNMP community strings (e.g., "public") and Telnet allows attackers to access and manipulate network devices without encryption.
	Overly Permissive Firewall ACLs and Blind IDS Zones	Firewall rules allow too much access and intrusion detection systems lack visibility into lateral traffic, leaving threats undetected.
Backup and Disaster Recovery Systems	Outdated or Weak Backup Encryption	Backup archives use deprecated or no encryption, exposing sensitive data to compromise if storage is accessed physically or remotely.
	Lack of Regular Validation and Recovery Testing	Backups are not periodically tested, which may lead to failed restorations during real incidents, risking data loss and service outages.
Communication Platforms (Email, Paging)	Phishing and Business Email Compromise (BEC)	Email accounts lack anti-phishing protections and MFA, making them vulnerable to impersonation, credential theft, or financial fraud.
	Unsecured Intercom and Paging Systems	Paging systems are accessible without proper controls or encryption, allowing unauthorized broadcasts or disruption of emergency communication.
Physical Security Systems (CCTV, RFID Access)	Unsecured IP-Based CCTV Systems	Cameras use default credentials and unencrypted interfaces, making live feeds and stored footage vulnerable to interception or tampering.
	RFID Access Misuse and Credential Cloning	Staff RFID cards are shared or unprotected against cloning, enabling unauthorized individuals to enter restricted zones such as server rooms or pharmacies.

6.2.3 Worksheet 10 – Information Asset Risk Evaluation

Risk Probability

Probability	Value	Description
Critical	76% - 100%	This risk has a high likelihood of occurring daily and demands immediate attention.
High	56% – 75%	Risk can occur once or more in a month and required immediate attention.
Medium	26% - 55%	Risk occurrence is moderate. It does not appear as frequently.
Low	0 -25%	Risk occurrence is low. It is highly unlikely to happen but there is a small possibility.

Impact values

Impact	Value	Description
Critical	100	Impact can lead to organizational shut down, loss or severe damage to human lives and mostly unrecoverable from the damage if the threat happens.
High	75	Recoverable, but severe damage and expenses of assets, reputation, and organization's functions.
Medium	50	Impact is not severe and can be controlled by implementing controls to affected areas.
Low	25	Manageable threat. Does not seriously affect assets or functions of the organization. It can be mitigated locally.

The maximum tolerable risk level for Winlanka Hospital is defined as a relative risk score of 75.

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Hospital Information System (HIS)		
	Area of Concern	Several non-clinical staff have excessive access to patient data and administrative modules, increasing the likelihood of intentional or accidental misuse of sensitive information within the HIS.		
	(1) Actor	Internal Staff (Administrative, Non-clinical)		
	(2) Means *How would the actor do it? What would they do?*	Staff members with excessive privileges may access lab results, discharge summaries, or billing records not relevant to their role. Misuse may be intentional or accidental, often going undetected without proper logging or access control enforcement.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate or Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Access to HIS should be tightly controlled through Role-Based Access Control (RBAC). Only clinical and authorized admin staff should access relevant modules. Implement: • Access auditing and log analysis (UBA) • Quarterly access reviews • Principle of least privilege enforcement		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Loss of patient trust due to breach of confidentiality can damage reputation and customer relationships, while also leading to financial penalties under PDPA Sri Lanka and potential patient lawsuits	Reputation & Customer Confidence	75 × 75%	56.25
	Financial	75 × 75%	56.25
Staff may need to repeat work if errors occur or access is abused, impacting productivity, while indirect safety and health risks may arise if incorrect data is accessed or modified	Productivity	50 × 50%	25
	Safety & Health	75 × 60%	45

	Violation of PDPA and hospital policies	Fines & Legal Penalties	50 × 25%	12.25
		User Defined Impact Area	50 × 50%	25
			Relative Risk Score	**219.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	✓ **Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
User Access Management System & HIS Role-Based Access Configuration	**-** Enforce Role-Based Access Control (RBAC) with clear role definitions - Enable access logging and integrate with User Behavior Analytics (UBA) - Restrict access to admin terminals in sensitive locations **Post-Mitigation Score**: 50 x 50% + 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% = 75 **Residual Risk: 75 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Hospital Information System (HIS)		
	Area of Concern	HIS access is currently protected only by usernames and passwords. Accounts with elevated privileges are exposed to credential theft or brute-force attacks, leaving sensitive systems vulnerable.		
	(1) Actor	External Attacker or Insider with stolen credentials		
	(2) Means *How would the actor do it? What would they do?*	Exploiting password-only login mechanisms through phishing, credential stuffing, or brute force. Once inside, attacker may view, delete, or alter patient records, or interrupt hospital workflows		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Modification**	✓ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	HIS access should be protected with **Multi-Factor Authentication (MFA)** for all privileged users. • Use secure MFA methods (FIDO2, authenticator apps) • Apply consistent authentication policies across all systems • Enforce MFA via central IAM solution		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A breach leading to unauthorized access or leakage of records can result in a loss of trust, damaging reputation and customer relationships, while also incurring financial consequences such as regulatory penalties and incident recovery costs	Reputation & Customer Confidence	75 × 75%	56.25
	Financial	75 × 55%	41.25
Disruption of hospital operations and delays in care can impact productivity; while posing significant	Productivity	30 × 50%	15

	safety and health risks, as altered patient records could potentially endanger lives	Safety & Health	75 × 75%	56.25
	Violation of PDPA and hospital policies	Fines & Legal Penalties	75 × 60%	45
		User Defined Impact Area	30 × 50%	15
			Relative Risk Score	**228.75**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	✓ **Mitigate**	✓ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Identity and Access Management (IAM) System	**-** Create and enforce a mandatory MFA policy - Configure IAM policy rules across HIS and related systems - Establish MFA awareness training for users **Post-Mitigation Score**: 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% = 75 **Residual Risk: 75 — Acceptable**

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Communication Platforms (Email, Paging)		
	Area of Concern	Email accounts are only protected with single-factor authentication and lack phishing protection, making the hospital vulnerable to Business Email Compromise (BEC), spoofing, and malware delivery.		
	(1) Actor	External Threat Actor (cybercriminals, phishing groups)		
	(2) Means *How would the actor do it? What would they do?*	The attacker sends phishing emails that impersonate hospital executives or suppliers. Victims may unknowingly share credentials, download malware, or follow fraudulent payment instructions. These campaigns often target finance or HR teams and exploit lack of MFA and email gateway filtering.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Modification**	❑ **Destruction** ✓ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• Enforce MFA for all staff email accounts • Deploy email security gateway with URL/link sandboxing • Implement DMARC, SPF, and DKIM email policies • Conduct phishing simulation training regularly		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
False alerts may erode public confidence, impacting reputation and customer trust, with minimal direct financial loss but a potential for significant reputational damage.	Reputation & Customer Confidence	75 × 75%	56.25
	Financial	50 × 25%	12.5
Disruption of hospital workflows or emergency protocols can hinder productivity, potentially leading to delayed emergency care or miscommunication, which poses significant safety and health risks	Productivity	50 × 50%	25
	Safety & Health	75 × 55%	41.25

	Could violate internal safety regulations	Fines & Legal Penalties	25 × 25%	12.25
		User Defined Impact Area	50 × 50%	25
			Relative Risk Score	**172.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Email System and Identity Access Management (IAM)	**-** Develop and enforce a Phishing Protection Policy - Create incident response SOPs for phishing attempts - Restrict access to shared workstations used for email access via timeout policies **Post-Mitigation Score**: 40 × 50% + 25 × 50% + 25 × 50% + 20 × 50% + 20 × 50% = 62 **Residual Risk: 62 — Acceptable**

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Unsecured Intercom and Paging Systems		
	Area of Concern	Paging systems are accessible without authentication and operate over unsecured IP networks. Attackers or insiders can inject signals, issue false alerts, or disrupt emergency coordination.		
	(1) Actor	Insider Threat		
	(2) Means *How would the actor do it? What would they do?*	Paging terminals are left unattended, and legacy paging infrastructure lacks authentication or encryption. Attackers may use signal spoofing tools or physically access terminals to broadcast unauthorized messages or disrupt alerts.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• Replace legacy intercom with VoIP paging over TLS • Create VLAN segmentation for communication traffic • Monitor and log paging activity, especially in sensitive areas		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
False alerts may erode public confidence, resulting in minimal direct financial loss but potentially significant reputational damage	Reputation & Customer Confidence	50 × 45%	22.5
	Financial	50 × 25%	12.5
Disruption of hospital workflows or emergency protocols can reduce productivity and lead to delayed emergency care or miscommunication, posing serious safety and health risks	Productivity	50 × 50%	25
	Safety & Health	75 × 50 %	37.5
Could violate internal safety regulations	Fines & Legal Penalties	25 × 25%	12.25

		User Defined Impact Area	50 × 50%	25
			Relative Risk Score	**134.75**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	✓ **Mitigate**	✓ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Physical Paging Terminals & Network Segment for Intercom Systems	**-** Upgrade to VoIP paging over encrypted channels - Train staff in reporting misuse or anomalies - Maintain paging logs and activity tracking **Post-Mitigation Score**: 50 x 50% + 25 × 50% + 25 × 50% + 20 × 50% + 20 × 50% =70 **Residual Risk: 70 — Acceptable**

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Backup and Disaster Recovery Systems		
	Area of Concern	Backup archives especially those on legacy NAS devices—are either using outdated encryption or none at all, exposing sensitive patient data to compromise during a breach or theft.		
	(1) Actor	Insider or External Attacker		
	(2) Means *How would the actor do it? What would they do?*	An attacker with physical access (e.g., stolen NAS device) or remote access (via network vulnerability) can retrieve backup data. If encryption is outdated (e.g., DES, 3DES) or absent, files can be easily exfiltrated or reconstructed.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• Migrate all backups to AES-256 encryption • Encrypt during backup, transfer, and restore • Use secure Key Management Systems (KMS) or HSMs • Apply role-based access control on backup storage		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Major damage to reputation and customer trust due to PHI exposure can also result in significant financial consequences, including regulatory fines under PDPA.	Reputation & Customer Confidence	75 × 75%	56.25
	Financial	75 × 70%	52.25
Staff may revert to manual workflows, impacting productivity, while also facing the risk of indirect harm to safety and health if critical data is lost or modified.	Productivity	50 × 60%	30
	Safety & Health	25 × 25%	6.25

	Non-compliance with data security mandates	Fines & Legal Penalties	75 × 60%	45
		User Defined Impact Area	-	-
			Relative Risk Score	**190**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Backup Storage Systems	- Develop and enforce Backup Encryption Policy - Migrate to AES-256 encryption for all new and archived backups - Enforce TLS 1.3 for backup transfers - Secure on-prem backup devices in locked server rooms **Post-Mitigation Score**: 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% = 75 **Residual Risk: 75 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Backup and Disaster Recovery Systems		
	Area of Concern	Backup integrity isn't validated through regular testing. A corrupted backup may only be discovered during an actual disaster, making recovery unreliable.		
	(1) Actor	Insider (IT operations team)		
	(2) Means *How would the actor do it? What would they do?*	Lack of restoration testing and anomaly detection tools results in silently corrupted or incomplete backups. These are only discovered during a live incident, causing recovery delays or failures.		
	(3) Motive *What is the actor's reason for doing it?*	Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	• Monthly tests restore procedures • Use automated backup verification tools • Incorporate into BCP/DR drills • Maintain a lot of validation results for audit readiness		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Perceived operational failure can damage reputation and customer trust, while also incurring financial costs due to extended downtime and staff overtime.	Reputation & Customer Confidence	75 × 75%	56.25
	Financial	50 × 25%	12.5
Disrupted workflows across hospital services can hinder productivity, leading to delays in clinical care and treatment plans, which pose significant safety and health risks.	Productivity	50 × 50%	25
	Safety & Health	25 × 25%	6.25
Breach of SL data protection guidelines	Fines & Legal Penalties	50 × 25%	12.25
	User Defined Impact Area		
		Relative Risk Score	**112.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Backup Scheduling System & DR Process Framework	**-** Create monthly restore test schedule - Use automated validation tools (e.g., checksum verification) - Set failure alerts for missed or failed restore attempts **Post-Mitigation Score**: 50 × 30% + 25 × 40% + 25 × 40% + 25 × 30% + 25 × 30% = 56 **Residual Risk: 56 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Internal Network Infrastructure		
	Area of Concern	Lack of proper VLAN segmentation allows attackers to move laterally between departments and systems once inside, increasing attack impact.		
	(1) Actor	External threat actor, possibly internal		
	(2) Means *How would the actor do it? What would they do?*	An attacker compromises a single endpoint and uses tools like PsExec, BloodHound, or RDP to laterally move to higher-value targets. Can easily scan and exploit adjacent systems due to lack of segmentation.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Implement 802.1Q VLANs with inter-VLAN firewalling, enforce east-west micro-segmentation, apply host-based ACLs, and use ZTNA strategies.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	○ **Medium**	○ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

Lack of proper VLAN segmentation allows attackers to move laterally between departments and systems once inside, increasing attack impact.

Company suffered severe reputational and customer damage due to a publicized ransomware attack, alongside major financial losses from the ransom, recovery efforts, and operational downtime.

Ransomware attack disrupted EHR, scheduling, and diagnostics services, severely impacting productivity, while potentially life-threatening delays in care delivery compromised safety and

Violation of PDPA and hospital policies.

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	100 *0.80	80
Financial	75 *0.75	56.25
Productivity	75 *0.75	56.25
Safety & Health	25 *0.30	7.5
Fines & Legal Penalties	75 *0.65	48.75
User Defined Impact Area	-	-

Relative Risk Score **248.75**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Internal LAN Segmentation and VLAN Routing Infrastructure	- Implement network zoning policies - Deploy 802.1Q VLAN segmentation - Enforce inter-VLAN firewall rules and host-based ACLs **Post-Mitigation Score**: 50 x 50% + 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% = 75 **Residual Risk: 75 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Internal Network Infrastructure		
	Area of Concern	Use of default SNMP community strings and Telnet allows attackers to access and manipulate network devices without encryption.		
	(1) Actor	Malicious insider or attacker on internal Wi-Fi		
	(2) Means *How would the actor do it? What would they do?*	Uses SNMPwalk, Nmap, or Metasploit to discover devices, extract configs, or manipulate routing/switching behavior.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Disable Telnet, enforce SSHv2 with key auth, use SNMPv3 with encrypted strings, and isolate management traffic using ACLs/VLAN		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Service disruptions can undermine customer confidence, harm an organization's reputation, and cause significant financial costs due to downtime in EHR or communication systems.	Reputation & Customer Confidence	75 *0.75	56.25
	Financial	75 *0.75	56.25
Network-level disruptions, including VoIP and medical IoT, hinder operational productivity and may delay critical communications, jeopardizing patient safety and health.	Productivity	75 *0.70	52.5
	Safety & Health	50 *0.50	25
Inadequate device hardening could lead to compliance violations, incurring substantial fines and legal penalties.	Fines & Legal Penalties	50 *0.50	25
	User Defined Impact Area	-	-
		Relative Risk Score	**215**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	✓ **Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Core Network Infrastructure	- Apply device hardening policies - Document and enforce SNMPv3 standard use - Disable Telnet and enable only SSHv2 with key-based login - Restrict physical access to network gear **Post-Mitigation Score**: 50 x 50% + 25 × 50% + 25 × 40% + 25 × 40% + 25 × 60% = 72 **Residual Risk: 72 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Internal Network Infrastructure		
	Area of Concern	Firewall rules allow too much access and intrusion detection systems lack visibility into lateral traffic, leaving threats undetected.		
	(1) Actor	External attacker or APT actor maintaining persistence		
	(2) Means *How would the actor do it? What would they do?*	Exploits legacy firewall rules to access critical systems, uses blind spots to exfiltrate data or maintain command/control.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Conduct rulebase cleanup, deploy IDS (Suricata/Zeek) in internal zones, integrate with SIEM, alert on anomalous traffic.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	✓ **Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Loss of trust, media coverage, and regulatory concern can damage an organization's reputation and erode customer confidence, while potential fines and breach mitigation efforts lead to substantial financial costs.	Reputation & Customer Confidence	75 *0.75	56.25
	Financial	75 *0.70	52.5
Undetected malware can gradually degrade operations, reducing productivity, and while immediate safety risks are minimal, delays in diagnosing threats could impact health outcomes.	Productivity	50 *0.60	30
	Safety & Health	25 *0.25	6.25
A breach may trigger mandatory reporting requirements and result in significant fines.	Fines & Legal Penalties	75 *0.60	45
	User Defined Impact Area	-	-
		Relative Risk Score	**190**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Firewall Management Console & IDS/IPS Infrastructure	- Develop firewall rule governance policies - Deploy IDS/IPS sensors across lateral VLANs (e.g., Zeek, Suricata) - Schedule monthly firewall rule base reviews - implement backup storage protection for logs **Post-Mitigation Score**: 50 × 60% + 25 × 40% + 25 × 40% + 25 × 40% + 25 × 40% =75 **Residual Risk: 72 — Acceptable**		

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	Physical Security Systems		
	Area of Concern	Cameras use default credentials and unencrypted interfaces, making live feeds and stored footage vulnerable to interception or tampering.		
Threat	(1) Actor	External attackers or internal malicious users		
	(2) Means *How would the actor do it? What would they do?*	Attackers exploit default login credentials or sniff unencrypted video streams to gain access. They may monitor sensitive areas, disable cameras, or delete footage.		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Destruction** ❑ **Modification** ✓ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Enforce strong, unique credentials, encrypt camera feeds, segment CCTV network, and implement secure, tamper-proof storage with access logging..		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Leaked surveillance data erodes trust and violates healthcare/surveillance laws, risking hefty fines and legal claims.	Reputation & Customer Confidence	100 *0.85	85
	Financial	75 *0.75	56.25
Breach costs include notifications, legal claims, and upgrades, while investigations and reconfiguration delay operations.	Productivity	50 *0.70	35
	Safety & Health	25 *0.25	6.25
Leaks may hinder emergency forensics or enable intrusions, risking safety in healthcare settings.	Fines & Legal Penalties	75 *0.60	45
	User Defined Impact Area	-	-
		Relative Risk Score	**227.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	**✓ Mitigate**	✓ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
CCTV Camera Network and Video Management System (VMS)	**-** Enforce CCTV configuration baseline (change default credentials, periodic reviews) - Maintain access logs and video audit trail policy - Enforce TLS encryption for all web interfaces - Restrict physical access to CCTV control rooms **Post-Mitigation Score**: 50 x 30% + 25 × 40% + 25 × 30% + 25 × 30% + 25 × 30% = 55 **Residual Risk: 62 — Acceptable**		

Allegro - Worksheet 10		Information Asset Risk Worksheet			
Information Asset Risk	Information Asset	**Physical Security Systems**			
	Area of Concern	Staff RFID cards are shared or unprotected against cloning, enabling unauthorized individuals to enter restricted zones such as server rooms or pharmacies.			
	Threat	(1) Actor	Internal staff, insiders with malicious intent, or attackers with access to cloning tools		
		(2) Means *How would the actor do it? What would they do?*	Misuse of shared badges, failure to revoke lost cards, or cloning of unprotected RFID signals to gain unauthorized access.		
		(3) Motive *What is the actor's reason for doing it?*	Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Upgrade to encrypted RFID implement logging and badge monitoring, enforce immediate deactivation of lost cards, and enable multi-factor entry for critical zones.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**
			Reputation & Customer Confidence	100 *0.85	85

	Unauthorized access may reduce patient confidence if publicized, while theft, sabotage, or security upgrades incur financial losses.	Financial	75 *0.75	56.25
	Investigating incidents and restoring security disrupts productivity. Unauthorized access to critical systems or medications poses significant	Productivity	50 *0.70	35
		Safety & Health	25 *0.25	6.25
	Potential non-compliance with physical security standards or health data laws may lead to fines and legal issues.	Fines & Legal Penalties	75 *0.65	48.75
		User Defined Impact Area	-	-
Relative Risk Score				**231.25**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
✓ **Accept**	✓ **Defer**	✓ **Mitigate**	✓ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
RFID Access Control System (Controllers + Badge Management Software)	- Enforce Lost Badge Reporting Policy with immediate revocation - Conduct quarterly access audits for sensitive zones - Upgrade to encrypted smartcards (MIFARE DESFire EV2) **Post-Mitigation Score**: 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% + 25 x 50% = 75 **Residual Risk: 62 — Acceptable**

7.Risk Monitoring & Response Plan – NIST

This section outlines how Winlanka Hospital (Pvt) Ltd will implement and continuously monitor cybersecurity risk mitigation strategies using the NIST Cybersecurity Framework (CSF). The plan is structured around the five core functions: Identify, Protect, Detect, Respond, and Recover, ensuring alignment with international best practices and Sri Lanka's Personal Data Protection Act (PDPA).

7.1 Identify

Objective: Develop an organizational understanding to manage cybersecurity risk to hospital systems, assets, data, and capabilities.

Key Activities:

- Maintain a real-time inventory of critical hospital assets including HIS, EHR, backup systems, IP-based CCTV, network infrastructure, and cloud platforms.
- Conduct periodic cybersecurity risk assessments using structured frameworks such as OCTAVE Allegro.
- Classify hospital data based on sensitivity and criticality (e.g., patient health data, financial records).
- Define acceptable risk levels, critical service thresholds, and prioritization criteria for mitigation.

Tools and Methods:

- Asset management platforms
- Data classification templates
- Risk registers and threat modeling reports

7.2 Protect

objective: Implement appropriate safeguards to ensure uninterrupted healthcare delivery and secure system operations.

Implementation Measures:

- Enforce Multi-Factor Authentication (MFA) on HIS, EHR, email, and administrator-level systems.
- Secure code repositories, backup archives, and network appliances using role-based access controls (RBAC).
- Apply regular firmware and software updates across clinical systems and IoT devices using automated patching tools.
- Encrypt sensitive data at rest and in transit using industry-standard algorithms .
- Segment internal networks using VLANs and apply east-west micro-segmentation for added control.

Ongoing Monitoring:

- Audit IAM policies and user access logs quarterly
- Validate encryption configurations and backup procedures
- Monitor compliance against security baselines

Tools and Platforms:

- Azure/AWS IAM, Microsoft Intune
- GitHub/Azure DevOps for secure repositories
- Configuration Management Tools

7.3 Detect

Objective: Develop and implement appropriate activities to identify the occurrence of cybersecurity events.

Monitoring Strategy:

- Enable centralized log collection from HIS, EHR, firewalls, and CCTV systems using platforms like Azure Monitor or WS CloudTrail.
- Deploy real-time threat detection using tools such as Microsoft Defender for Endpoint, Amazon GuardDuty, and open-source EDR solutions.
- Correlate security events and logs using a Security Information and Event Management (SIEM)tool such as Splunk or **Microsoft Sentinel.

Detection Enhancements:

- Define alerts for abnormal login behaviors, privilege escalation, and lateral movement.
- Conduct routine log reviews and security audits.
- Monitor changes in device configurations and access to sensitive assets.

7.4 Respond

Objective: Take appropriate actions when cybersecurity incidents are detected to contain, mitigate, and recover effectively.

Response Measures:

- Develop a documented Incident Response Plan (IRP) outlining roles, escalation paths, and communication protocols.
- Train key IT and clinical staff with tabletop exercises simulating breach scenarios such as ransomware or insider misuse.
- Automate isolation of infected endpoints using EDR tools and predefined response playbooks.

Key Controls:

- Retain system and network logs for forensic analysis
- Configure alerts and dashboards for incident tracking
- Establish escalation procedures to inform hospital executives and legal teams

7.5 Recover

Objective: Maintain resilience and restore any capabilities or services that are impaired due to a cybersecurity incident.

Recovery Procedures:

- Perform scheduled test restorations of patient data and critical system backups.
- Use geo-redundant storage for offsite copies of medical records, imaging archives, and business continuity data.
- Document all lessons learned after incidents, and feed results into improvement cycles.
- Provide regular updates to staff, regulatory bodies, and patients on recovery progress during major incidents.

Tools and Platforms:

- Veeam, Acronis, or cloud-native backup solutions
- Business Continuity Plans (BCP) and Disaster Recovery (DR) frameworks

7.6 Performance Metrics & Continuous Improvement

Tracking Mechanisms:

- Define Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) for each of the five NIST CSF functions.
- Monitor dashboards for trends in phishing attempts, patch compliance, and alert response times.
- Conduct annual red team vs. blue team assessments to simulate real-world attack-defense scenarios.

Review Cycle:

- Perform quarterly security reviews with IT and executive stakeholders
- Implement feedback loops based on incident reports and post-event evaluations
- Refresh risk assessments and technical controls annually using the OCTAVE Allegro framework