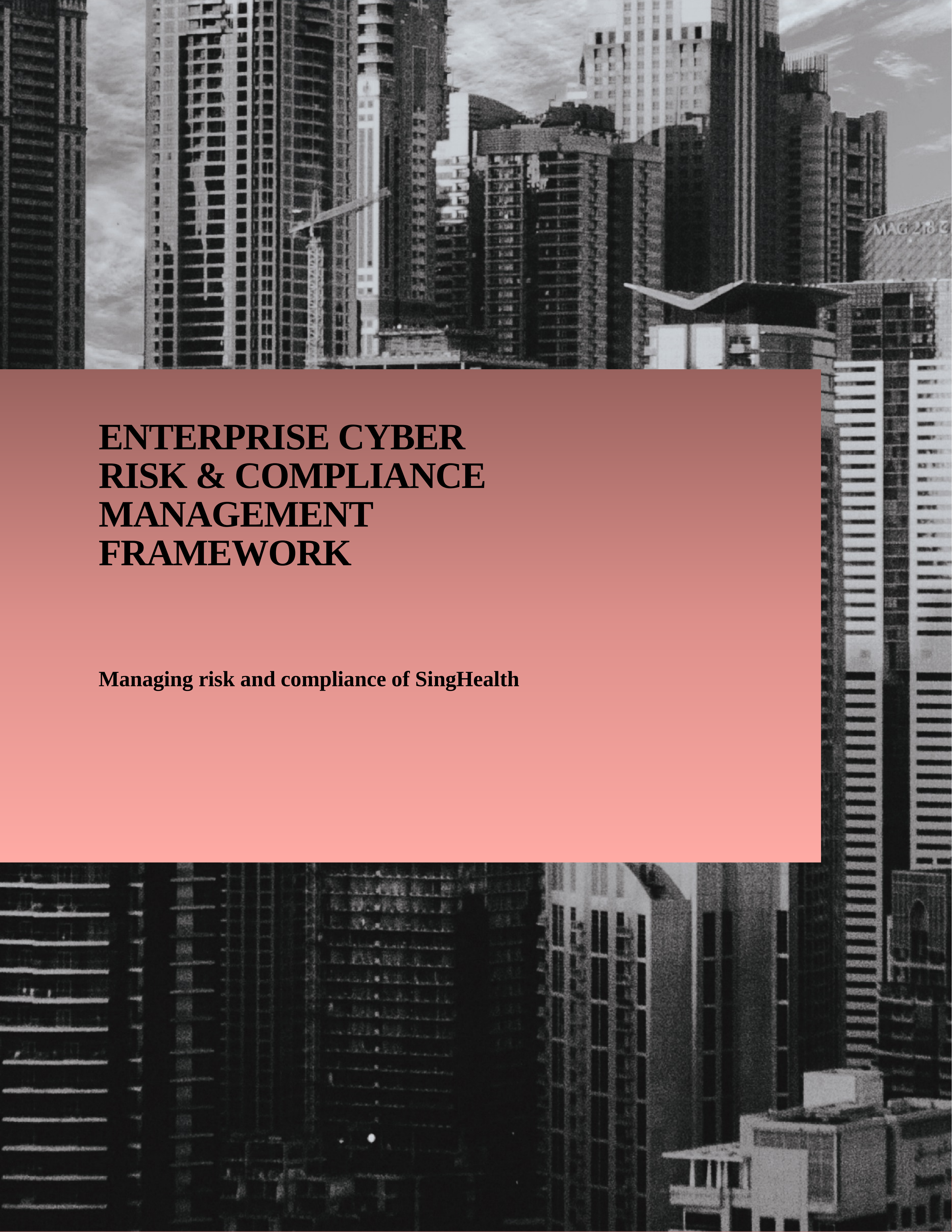

ENTERPRISE CYBER RISK & COMPLIANCE MANAGEMENT FRAMEWORK

Managing risk and compliance of SingHealth

Executive Summary

SingHealth is Singapore's largest public healthcare cluster that has hospitals, clinics and research centers included in its entity list [1]. It holistically provides safe and timely patient care which depends on confidentiality, integrity and availability (C.I.A) of digital health information throughout its interconnected clinical systems [1], [2], [3]. This risk management and compliance report uses ISO 31000 (establish context → identify → analyse → evaluate → treat → monitor) [4] alongside **NIST CSF 2.0** [5] outcomes and **ISO/IEC 27002** [6] control themes on three different but vitally important assets, electronic medical record and PHI data warehouse, radiology PACS and imaging modalities, and hospital building management system. We score inherent and residual risk via a qualitative risk analysis method, compare risks and regulatory compliance associated with SingHealth, and set some treatments, with a 12-month roadmap with KRIs, RACI [7] which are all compliant with Singapore's regulatory requirements.

Assumptions and Scope

- Scope covers SingHealth's core clinical services, hospitals, and enabling facilities and supply chain and vendor access
- A 5x5 qualitative method is used for risk assessment of assets [7]
- SingHealth faced a breach in 2018 [8], but we will assume for this scenario, SingHealth has a model typical health sector exposure in Singapore
- Risk appetite can be medium, but High/Critical residual risk for assets is not tolerated

Introduction

SingHealth is singapore's largest public healthcare provider and has many institutions under it such as hospitals, clinics, etc. It's core clinical platforms include enterprise Electronic Medical Record (EMR/EHR) systems and a PHI data warehouse; radiology PACS facilities with site-level archives; and a Hospital Building Management System (HBMS) for alarms, operating theatres, ICUs, etc [1].

1.1 Primary Business Processes

These include patient registration, identification, treatment, medication management, documentation, billing, diagnostics of people and systems; supporting processes include biomedical engineering and device lifecycle, facilities management like HVAC, alarms, data analytics of care quality and research, interoperability of GPs, labs, national systems and finally security operations [1].

1.2 Why Cyber Risk Management is Vital for SingHealth

Healthcare combines highly sensitive personal/health information (PHI/PII) with critical and real time operations. Failures in confidentiality of data create direct privacy harm, integrity failure can cause failure in clinical decisions, and availability failure can cause delay of critical care. The attack surface for assets is expanded via cloud EMR, remote vendor access, connected devices, and the very nature of patient data being a critical asset (more on this later). Threat actors monetize ransomware driven disruption, data exfiltration and supply-chain compromise. Business, regulatory and operational challenges are present [12] such as:

- Business pressure: constrained cyber defense budgets, where assets have to be risk evaluated and prioritized in budget
- Regulatory Compliance: PDPA obligations for Singaporean companies [9], Cybersecurity Act obligations for Critical Information Infrastructure (CII) [10] and more
- People and Operational Challenges: vendor managed appliances, legacy protocols, thousands of employees with varying identity access management requirements, and more [11]

A structured cyber risk framework aligned with governance, appetite, controls and monitoring is required to enable prioritization of risks across assets and subsidiary institutions, sites, vendors and traceability of risk and treatment with continuous improvement via KRI exercises – all tailored to Singapore's regulatory requirements [12].

Regulatory and Compliance Context

We assess SingHealth's cyber-risk obligations against applicable compliance requirements with selected standards and sector guidance:

- **Personal Data Protection Act (PDPA, Singapore) + data breach notification:** rules for collection, use, disclosure, retention and protection of personal data; assessment of data breaches to individuals, shareholders and the PDPC [9]
- **Cybersecurity Act (Singapore):** CII for designated critical systems with obligations for cybersecurity measures, incident reporting, and more [10]
- **MOH sector guidance and policies:** Ministry of Health cybersecurity expectations, health-sector security requirements for healthcare systems and devices [13]
- **PCI DSS v4.0:** security and storage of card-holder data, vulnerability management, logging, etc
- **ISO/IEC 27001/27002:** Risk-based management system with comprehensive controls spanning access, operations, incident response and documentation [6]

Law / Standard	Selected obligations	Risk categories influenced
PDPA (Singapore)	Lawful collection/use; reasonable security; breach assessment & **timely notification**	**Confidentiality of PHI**, **legal/regulatory risk**, **incident response**, **third-party data sharing**, **records management**
Cybersecurity Act (CII)	Baseline cybersecurity measures; incident reporting; audits; resilience for designated CIIs	**Availability & resilience**, **governance & assurance**, **monitoring & reporting**
MOH sector guidance	Identity/access discipline, secure configurations, supplier oversight, device/OT governance	**Access control & identity**, **ops/OT security**, **supplier risk**, **auditability**
PCI DSS v4.0 (if/where in scope)	CDE **segmentation**, encryption, strong authentication, **logging**, secure updates, third-party controls	**Payment integrity**, **network security**, **malware/tamper prevention**, **supplier risk**, **availability**
ISO/IEC 27001/27002	Risk-based ISMS; policy→standard→procedure; organisational & technical controls	**Governance**, **policy & assurance**, **change control**, **backup/restore**, **continuity**

Table 1: Obligation → risk-category mapping [6], [9], [10], [13]

Compliance-driven control themes include:

- **Identity and Access:** unique named accounts, least privilege, MFA, emergency access, identity segregation
- **Data Protection:** PHI classification, encryption in transit/rest
- **Logging and Monitoring:** centralized, tamper-evident audit across EMR, PACS, BMS in real time

- **Network and Platform Security:** segmentation of clinical networks (PACS), BMS, recorded remote access, code-signed updates
- **Supplier Management:** contractual security clauses, timely patching, due diligence
- **Continuity and IR:** immutable backups and restore tests, breach response playbooks, system fallbacks [14]

Non-compliance implications for a public healthcare cluster include:

Dimension	What it looks like in practice
Legal & Regulatory	PDPC investigations/enforcement; civil penalties; mandated remediation; CII non-compliance actions; restrictions on integrations if conditions apply.
Financial	Forensics, notification, credit monitoring; rebuilds; overtime/locum backfill; chargebacks/penalties (PCI); cyber insurance impacts; throughput/revenue loss from cancellations.
Operational	Theatre closures, diversions, appointment backlogs, imaging/reporting delays, degraded clinician trust in records, disruption to remote maintenance for modalities/BMS.
Reputational	Loss of public trust; media scrutiny; strained professional partnerships; recruitment/retention challenges; long-term brand erosion.

Table 2: Non-compliance with similar institutions [15]

These obligations translate directly into our business context and ISO 31000 risk framework: PDPA underpins confidentiality for EMR/PHI (R1); Cybersecurity Act/MOH guidance drive availability and integrity for PACS and BMS (R2–R3); PCI DSS applies where payments occur. We operationalize them via NIST CSF and ISO/IEC 27002 control themes, apply to the asset risks in Sections 3–5 (e.g., least-privilege/KMS/DLP, segmentation, etc), and make them evidence-based through KPI/KRI/KCI thresholds in Section 6. Compliance matters as meeting obligations drives excellence in PHI protection, segmentation and access for PACS and BMS, monitoring and audit, supplier assurance and more.

Identification of Assets, Threats, Vulnerabilities and Risk

3.1.1 Information assets — sensitivity classification (CIA + sensitivity tier)

Sensitivity tiers:

- **Restricted (R):** PHI/PII, credentials, crypto keys, security configs.
- **Confidential (C):** clinical workflows, internal financials, vendor contracts.
- **Internal (I):** non-public operating docs.
- **Public (P):** approved public information.

Information Asset Class	**Examples (SingHealth)**	**Sensitivity Tier**	**C**	**I**	**A**	**Justification / Framework Basis**
Patient Health Information (PHI) in EMR/EHR	demographics, notes, meds, allergies, care plans	**R**	**Very High**	High	High	Privacy harm + clinical decision reliance; ISO 27002 information classification; PDPA duties
Clinical Imaging & Reports	PACS studies, radiology reports	**R**	**High**	**Very High**	**Very High**	Diagnostic integrity + care timeliness; NIST CSF PR.DS/PR.AC themes
Laboratory & Pathology Results	LIS results, microbiology	**R**	**High**	**Very High**	**Very High**	Treatment decisions depend on correctness; safety impact
Medication & e-Prescribing Data	eMAR, CPOE, formularies	**R**	**High**	**Very High**	**Very High**	Risk of dosing/interaction errors if tampered
PHI Analytics / Data Warehouse	longitudinal PHI, quality metrics	**R**	**Very High**	High	High	Contains large PHI aggregates; re-

						identification risk
Identity & Access Data	user directories, roles, tokens	**R**	**High**	**High**	High	Keys to the kingdom; zero trust dependency
Secrets & Key Material	KMS keys, API secrets	**R**	**High**	**High**	High	Compromise escalates to systemic breach
Billing & Claims Data	patient billing, insurer info	**C/R**	**High**	High	High	Financial exposure; personal data elements
Supplier & Contract Data	security terms, SLAs	**C**	High	Medium	Medium	Legal/commercial sensitivity
Operational Logs & Audit Trails	EMR/PACS access logs	**C**	High	Medium	High	Forensics and compliance evidence
Configuration & Infrastructure Data	IaC, device configs	**C**	Medium	High	High	Integrity of configs directly affects resilience
Research Data (de-identified)	clinical studies	C/I	Medium	Medium	Medium	Re-identification risk varies
Policies/Procedures/Training	SOPs, IR playbooks	I	Medium	Medium	Medium	Internal use; operational dependency
Public Communications	websites, press releases	P	Low	Low	Medium	Controlled disclosure only

Table 3: IT asset classification tiered based on C.I.A and Sensitivity [1], [3], [5], [6]

3.1.2 Non-information IT assets — functional classes, criticality, loss impact & replacement value

Non-Information IT Class	**Examples**	**Function/Criticality**	**Loss Impact (C.I.A)**	**Indicative Replacement Value**	**Indicative RTO / RPO**	**Justification / Framework Basis**
Clinical Apps (Core)	EMR/EHR, eMAR/CPOE, Oncology, ICU systems	**Safety-critical**	**A & I**	High	RTO: hours / RPO: minutes-hours	Patient safety & care continuity; NIST CSF ID.AM/PR.AC
Diagnostic Platforms	PACS/RIS, LIS, cardiology	**Safety-critical**	**A & I**	High	RTO: hours / RPO: minutes-hours	Diagnostics drive treatment decisions
Enterprise Apps	ERP/finance, HRIS, rostering	Business-critical	A	Medium-High	RTO: < 1–2 days / RPO: hours	Operational continuity & payroll
Networking	core/distribution/access, firewalls, Wi-Fi	**Clinically significant**	**A**	High	RTO: minutes-hours / RPO: n/a	Real-time care flows; segmentation
Endpoints & Mobility	clinician workstations, COWs, tablets	Clinically important	A	Medium	RTO: hours / RPO: n/a	Point-of-care access

Medical Devices (connected)	monitors, pumps, modalities	**Safety-critical**	**A & I**	High	RTO: hours / RPO: n/a	Direct patient impact; vendor-managed
OT/ICS Controls	BMS, PLCs, SCADA	**Safety-critical**	**A & I**	Medium-High	RTO: hours / RPO: n/a	Theatre/ICU environment safety

Table 4: Non-IT asset classification tiered based on C.I.A and Impact [1], [3]

3.1.3 Non-IT assets — business-critical classification

Non-IT Asset Class	**Examples**	**Business Criticality**	**Loss Impact**	**Justification**
People	clinicians, residents, nurses, SOC analysts, facilities engineers	**Essential**	Service & safety	Identity/process dependency; insider risk dimension
Facilities & Utilities (including OT/ICS controls)	theatres, wards, ICU rooms, UPS, generators	**Essential**	Safety & availability	Environment for safe procedures
Processes & SOPs	IR playbooks, change control, clinical SOPs	**Essential**	Integrity & availability	Process controls underpin consistent practice
Physical Records & Media	legacy charts, backup tapes	Important	Confidentiality	Residual PHI risk; restore dependency
Pharmaceuticals & Supplies	meds, sterile packs	Essential	Availability	Direct care dependency
Brand & Trust	reputation, public confidence	Essential	Strategic	Affected by privacy breaches / outages

Table 5: Non-IT asset business classification tiered based on criticality to business and Impact [1], [3]

Three assets from tables 3-5 were selected because they are on the critical path of care and together cover the full spectrum of the estate—information (EMR/PHI), clinical IT platforms (PACS/Modalities), and OT/ICS (BMS). The EMR/PHI concentrates the most sensitive data and directly informs clinical decisions (privacy and integrity risk). PACS/Modalities is the diagnostic bottleneck for ED, ICU, and theatres, where availability or integrity issues immediately translate into delays or harm. The BMS underpins safe surgical and ICU environments; compromise can force theatre closures and breach infection control. **Importantly,** OT/ICS controls are also a part of **facilities & utilities** asset which is also a business-critical asset and is essential for day-to-day business. Collectively they align to the highest regulatory exposures (e.g., PDPA security and breach readiness, safety/continuity expectations) and represent prevalent threat paths.

3.2 Threats & Vulnerabilities Mapping

External Threat Actors: ransomware groups, data brokers, supply-chain attackers

Internal Threat Actors: malicious insider, over-privileged account, careless user, third-party vendor access

A) EMR & PHI Data Warehouse (Information Asset)

Threat Source	Threat Action	Key Vulnerabilities	Plausible Causes / Conditions	Existing Controls (typical)	Exploitability (qual.)
External (criminal)	Cloud data exfiltration	Misconfigured storage, exposed keys/tokens, over-broad IAM	Rapid cloud change; weak guardrails; legacy ETL	MFA for admins; baseline guardrails; encryption at rest	**Medium-High**
External (phishers/IABs)	Credential theft / session hijack	MFA fatigue, token replay, SSO misconfig	Social engineering; legacy MFA prompts	Conditional access; anti-phishing training	**Medium**
Internal (malicious/curious)	Inappropriate access/browse	Excess privileges; weak SoD	Role creep; poor access reviews	Quarterly access	**Medium**

				reviews; DLP alerts	
Third-party (integrations)	API abuse / over-collection	Weak API scopes; poor contract terms	Rapid partner onboarding; shadow APIs	API gateway; legal clauses; rate limiting	**Medium**

Table 6: Threat Assessment of EMR Asset [1], [14], [16]

B) Radiology PACS & Imaging Modalities (Non-Information IT Function Asset)

Threat Source	**Threat Action**	**Key Vulnerabilities**	**Plausible Causes / Conditions**	**Existing Controls**	**Exploitability**
External (ransomware group)	Lateral movement to PACS	Flat VLANs; weak ACLs; legacy SMB/RDP	Unsegmented imaging networks	VLANs; AV/EDR on gateways	**Medium-High**
Supply chain (vendor)	Malicious/compromised update	Unsigned updates; default creds	Vendor process gaps; legacy modality	Change windows; vendor contracts	**Medium**
Internal (IT ops error)	Misconfig breaks ingest	Fragile routing; weak change control	Manual config; poor rollback	CAB; backups of configs	**Medium**
Insider (imaging staff)	Data export misuse	Broad export rights; weak audit	Ad-hoc sharing pressure	Audit logs; SOC queries	**Low-Medium**

Table 7: Threat Assessment of PACS Non-IT Asset [1], [14], [16]

C) BMS for Theatres & ICUs (Non-Information OT/ICS Business-Critical/Function Asset)

Threat Source	**Threat Action**	**Key Vulnerabilities**	**Plausible Causes / Conditions**	**Existing Controls**	**Exploitability**
External (ransomware group)	IT→OT pivot to BMS	Poor IT/OT segmentation; shared creds	Flat networks; contractor VPN bypass	Firewalled jump hosts; approvals	**Medium-High**
Third-party (contractor)	Unauthorized parameter change	Shared accounts; no session recording	On-call urgent access; weak oversight	Manual logs; basic approvals	**Medium**
Internal (accidental)	Mis-set setpoints	Weak change procedures; no 4-eyes	Time pressure; limited training	Paper procedures; periodic checks	**Medium**

Table 8: Threat Assessment of HBMS System Infrastructure Asset [1], [14], [16]

3.3 Development of Risk Scenarios

Structure used: *Asset/Context → Threat Source/Action → Vulnerability → Event (what goes wrong) → Consequences → Affected Objectives → Existing Controls → Inherent L×I → Residual L×I → Owner → Treatment → Early Indicators (KRIs) [17]*

Scenario 1 — EMR & PHI Data Warehouse (Information Asset)

Component	**Detail**
Asset / Context	Central EMR and PHI warehouse supporting care pathways and analytics
Threat Source / Action	External criminal exfiltration via cloud misconfig + over-privileged service accounts

Vulnerability	Misconfigured storage policies; exposed keys/tokens; excessive IAM roles
Event	Unauthorized bulk access/exfiltration of PHI
Consequences	Privacy harm; PDPA breach notifications; trust erosion; potential clinical decision risk if data integrity affected
Affected Objectives	Compliance, reputation, clinical safety, operations
Existing Controls	MFA for admins; baseline guardrails; encryption at rest; basic DLP; periodic access reviews
Inherent Risk (L×I)	4 × 4 = **16** (High)
Residual Risk (L×I)	3 × 4 = **12** (Medium-High)
Risk Owner	Group Chief Data Officer
Treatment (summary)	Least privilege & SoD; JIT access; **KMS rotation**; stricter guardrails; **DLP/UEBA**; API scope minimization
Early Indicators (KRIs)	Spike in PHI DLP alerts; anomalous service-account usage; failed guardrail checks

Risk statement 1
Because of cloud/storage misconfigurations and over-privileged service accounts, there is a risk that PHI in the EMR/data warehouse is exfiltrated or manipulated, which could trigger PDPA notifications, erode patient trust, and mislead clinical decisions, affecting our objective to protect privacy and support safe clinical care.

Scenario 2 — Radiology PACS & Imaging Modalities (Non-Information IT Function Asset)

Component	Detail
Asset / Context	PACS/RIS with site archives; modalities (CT/MRI/US) feeding urgent diagnostics
Threat Source / Action	External ransomware group pivots into PACS; vendor update channel abused
Vulnerability	Unsegmented imaging VLANs; unsigned updates; default vendor creds; weak ACLs

Event	Malware/tamper on PACS or gateways; study ingest failures/corruption
Consequences	Delayed/incorrect diagnoses; theatre cancellations; ED backlog; reputational harm
Affected Objectives	Clinical safety, availability, quality
Existing Controls	VLANs; vendor patch cadence; limited FIM/EDR on gateways; on-call admins
Inherent Risk (L×I)	3 × 5 = **15** (Medium-High)
Residual Risk (L×I)	3 × 4 = **12** (Medium-High)
Risk Owner	Director, Imaging IT
Treatment (summary)	**Segmentation (deny-by-default)**; allow-listing on gateways; **code-signed updates**; FIM/EDR; privileged access governance
Early Indicators (KRIs)	Study ingests failure rate; FIM deviations; unsigned update attempts; anomalous east-west traffic

Risk statement 2
Due to unsegmented PACS networks and insecure modality update paths, there is a risk that malware or unauthorized changes disrupt imaging or corrupt studies, which could delay diagnoses and force procedure cancellations, impacting our objective to deliver timely, high-quality patient care.

Scenario 3 — BMS for Theatres & ICUs (Non-Information OT/ICS Business-Critical/Function Asset)

Component	Detail
Asset / Context	Building Management System managing theatre pressure/air changes and ICU climate
Threat Source / Action	External ransomware group pivots IT→OT; contractor mis-uses remote access
Vulnerability	Poor IT/OT segmentation; shared contractor accounts; lack of session recording; legacy protocols

Event	Unauthorized parameter changes or controller outage
Consequences	Theatre closures; infection-control breaches; patient-safety incidents; service cancellations
Affected Objectives	Safety, availability, compliance
Existing Controls	Firewalled jump hosts; access approvals; weekly backups; change control
Inherent Risk (L×I)	3 × 4 = **12** (Medium-High)
Residual Risk (L×I)	2 × 4 = **8** (Medium)
Risk Owner	Facilities Director
Treatment (summary)	**IT/OT segmentation**; brokered remote access (MFA, session recording); unique contractor IDs; passive OT monitoring; offline config backups & drills
Early Indicators (KRIs)	Setpoint change alerts; unbrokered remote sessions; OT anomaly detections; failed restore tests

Risk statement 3
Because IT/OT segmentation is insufficient and contractor remote access is weakly controlled, there is a risk that BMS setpoints are tampered with or controllers are disabled, which could close theatres, breach infection control, and raise patient-safety risks, undermining our objective to maintain safe, continuous clinical environments [4], [17].

Risk Analysis & Evaluation (Qualitative 5×5)

4.1 Scoring Scales (Operationalized)

Likelihood	Score	Definition
Rare	1	≤ once in 10 years given current controls
Unlikely	2	Possible but not expected this year
Possible	3	Credible within 12–24 months
Likely	4	Expected within 12 months
Almost Certain	5	Multiple times per year

Table 9: Likelihood Scale of Risk (Qualitative)

Impact	**Score**	**Definition**
Minor	1	No patient impact; <4h local delay
Moderate	2	Local delay; no safety risk
Significant	3	Backlog; near-miss safety
Major	4	Cancelled theatre lists/diversions; privacy harm
Severe	5	Patient-safety incident; multi-site outage; major privacy event

Table 10: Impact Scale of Risk (Qualitative)

L×I	**Level**	**Colour**	**Appetite**
1–5	Low	Green	Within
6–10	Medium	Yellow	Within
12–15	Medium-High	Orange	**Breaches**
16–25	High	Red	**Breaches**

Table 11: Appetite Color Band of Risk (Qualitative)

4.2 Risk Analysis using Heat-Map (Qualitative) and Risk Register

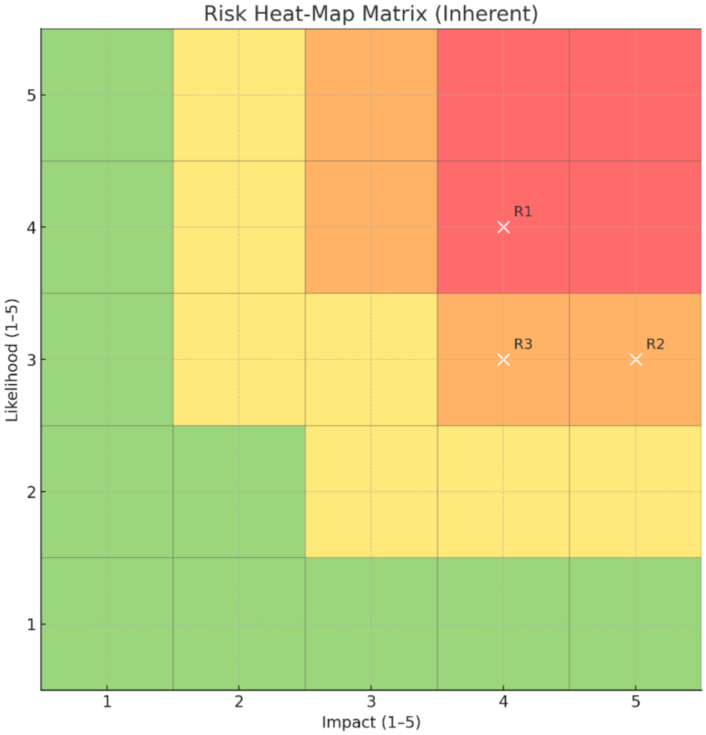

Figure 1: Risk Heat-Map Matrix of Inherent Risk (Qualitative) [18]

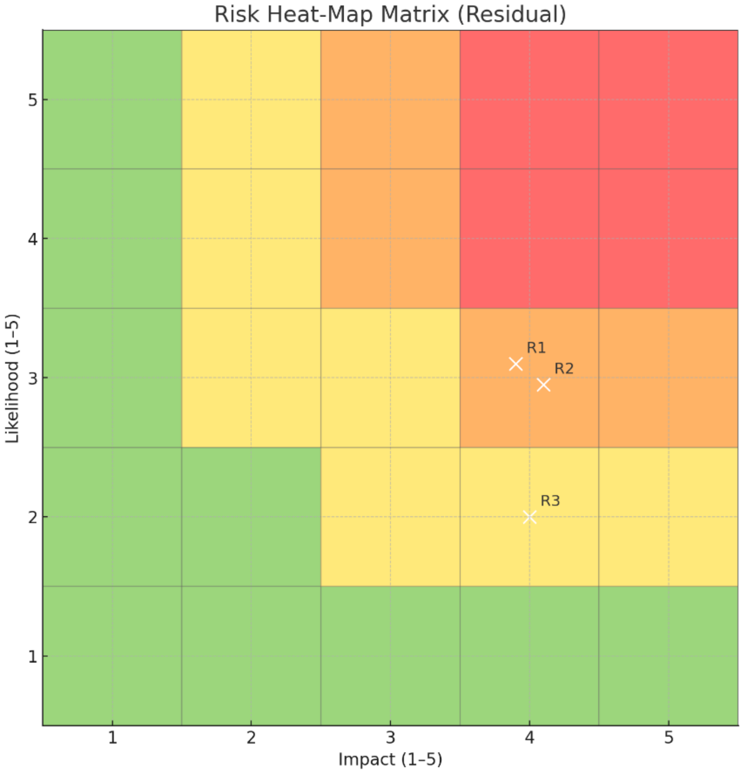

Figure 2: Risk Heat-Map Matrix of Residual Risk (Qualitative) [18]

Risk ID	Asset	Scenario Summary	Inherent L	Inherent I	Residual L	Residual I	Owner	Treatment Summary
R-1	EMR & PHI Data Warehouse	Misconfig/privilege → PHI exfil/manipulation	4	4	3	4	Group CDO	KMS + least-privilege + DLP/UEBA
R-2	Radiology PACS/Modalities	Segmentation/update gaps → tamper/malware	3	5	3	4	Dir. of Imaging IT	Segmentation + allow-listing + FIM/EDR
R-3	BMS (Theatres/ICUs)	Weak IT/OT separation → control tampering	3	4	2	4	Facilities Director	IT/OT segmentation + brokered access

Table 12: Risk Register of Assets

Figure 1 shows the inherent heat map of risk (qualitative) where all three asset risks are shown with their respective appetite color bands (table 11), where R1-R3 are all above <10 range which is the maximum for risk allowed by a similar large organization. Figure 2 shows us the residual risk after implementing the controls where R1 and R2 assets are still above range i.e now 12, so further monitoring and hardening of security and assurance is required, while R3 is now within appetite after our controls are implemented. Finally, the risk register in table 12 ties all of this to a visual action where it records the asset to risk owners, the Risk= Likelihood x Impact scores, the scenario and finally treatment summary [18], [19].

4.3 Ratings (numeric) & Rationale

Scenario	Inherent (L×I)	Controls	Residual (L×I)
R-1 EMR/PHI	4×4 = **16** (High)	MFA admins; cloud guardrails; at-rest encryption; basic DLP; periodic access reviews	3×4 = **12** (Medium-High)
R-2 PACS/Modalities	3×5 = **15** (Medium-High)	VLAN segmentation; vendor patch cadence; limited FIM/EDR on gateways; on-call imaging admins	3×4 = **12** (Medium-High)
R-3 BMS	3×4 = **12** (Medium-High)	Jump hosts; vendor VPN approvals; weekly backups; change control	2×4 = **8** (Medium)

Table 13: Risk Scenario of Assets After Implementing Controls

Evidence & assumptions (after control implementation on day-to-day business):

- **R-1 Evidence:** cloud guardrail and EMR integrations exists; MFA coverage is present
  Assumptions: some legacy jobs use long-lived keys; DLP tuned for PHI but not all sources
- **R-2 Evidence:** PACS gateways are inventoried; VLANs are present; recent vendor patch dates; modality firmware ages known
  Assumptions: limited modality telemetry; code-sign verification not enforced everywhere
- **R-3 Evidence:** jump-host policy in place; vendor VPN approvals logged; weekly backups verified
  Assumptions: shared contractor accounts still exist; OT network map incomplete

4.3 Risk Evaluation

The **inherent heat map (figure 1)** concentrates all three risks in Medium-High/High territory (R1=16, R2=15, R3=12). The **residual heat map (figure 2)** shows control impact: **R1=12**, **R2=12** (both still above appetite), and **R3=8** (now within appetite). The **data from table 12-14** ties these positions to owners, treatments, targets, and KRIs. Appetite less than 10 is acceptable, so R1 and R2 must be treated even further. This is the case because as we have shown in table 13, implementation of strong controls still leaves higher probability of an incident to occur so implementation of controls does not decrease impact, but it does decrease likelihood score from inherent 4 to residual 3, which must be further reduced to a score of 2 (unlikely) after more steps in risk management which we will get into using KRIs, segmentation, drills, DLP and more.

Risk	Inherent L×I	Residual L×I	Appetite breach?	Triage	Why
R1 – EMR/PHI	16	12	Yes	Treat now	PHI exfil/integrity → PDPA notification + patient trust
R2 – PACS/Modalities	15	12	Yes	Treat now	Diagnostics delay/corruption → direct patient-care impact
R3 – BMS (Theatre/ICU)	12	8	No	Monitor	Within appetite after IT/OT segmentation + brokered access

Table 14: Risk Evaluation of Assets After Implementing Controls

Urgent treatment vs ongoing monitoring

- **Treat now (breach appetite):**

  R1 (12): Push least-privilege/SoD completion, KMS rotation, and DLP/UEBA tuning to drive residual to **≤10**.

  R2 (12): Enforce deny-by-default segmentation, allow-listing on imaging gateways, and code-signed updates; add FIM/EDR coverage to hit **≤10**.

- **Ongoing monitoring (within appetite):**

  R3 (8): Maintain brokered remote access and passive OT monitoring; keep quarterly restore drills. Escalate if KRIs drift.

Compliance checkpoints

- **R1 PDPA:** Evidence of "reasonable security" must be demonstrable (access reviews, DLP efficacy, key/secret hygiene). Any verified PHI exfil triggers breach-assessment workflows.
- **R2 Clinical safety:** Imaging availability/quality is a safety proxy; KRIs (ingest failure %, unsigned update attempts, FIM deviations) are compliance-relevant evidence of operating control.
- **R3 Safety & resilience:** Theatre/ICU environment integrity (setpoint change alerts, OT anomalies, successful restore tests) proves continued compliance with safety expectations.

What moves the residuals below appetite (next steps)

- **R1:** Close high-risk entitlements; enforce JIT access; complete KMS key rotations; raise DLP catch-rate and UEBA fidelity; verify **≥98%** cloud guardrail compliance.
- **R2:** Lock ACLs (deny-by-default), deploy allow-listing on gateways, mandate signed update chains with vendors, extend FIM/EDR coverage; target study-ingest failures ≤0.3%/week.
- **R3:** maintain **100%** brokered/recorded contractor sessions; quarterly setpoint-restore tests per site.

Monitor & escalate (from the register's KRIs):

- Spike in PHI DLP alerts or anomalous service-account use → escalate **R1**.
- Rising PACS ingest failures or unsigned update attempts → escalate **R2**.
- Unbrokered OT sessions or failed BMS restore tests → re-open treatment for **R3**.

Risk Treatment and Compliance Plan

5.1 Treatment decision & targets (ISO 31000)

Risk	Decision	Rationale	Target Residual	Due
R-1 EMR/PHI	**Treat**	PHI + clinical decision support; PDPA exposure	**≤ 10 (Medium)**	Q3
R-2 PACS	**Treat** (+ partial **transfer** via vendor SLAs)	Direct patient-flow impact	**≤ 10 (Medium)**	Q2
R-3 BMS	**Treat**	Safety-critical environments	**≤ 10 (Medium)**	Q2

Table 15: Risk Treatment Targets and Decision of Assets

In table 15, we show that our risk treatment plan prioritizes treating the two appetite-breaching risks—R1 (EMR/PHI) and R2 (PACS/Modalities)—with control bundles already defined (least-privilege/JIT + KMS + DLP/UEBA for R1; deny-by-default segmentation + gateway allow-listing + signed updates + FIM/EDR for R2) to drive residual risk from 12 → ≤10 and meet PDPA and clinical-safety thresholds by Q3 (R1) and Q2 (R2).

R3 (BMS) is now 8 (within appetite) after IT/OT segmentation and brokered access, so it moves to assurance monitoring (brokered sessions at 100%, passive OT analytics, quarterly restore drills) with escalation triggers tied to KRIs. Risk owners (CDO for R1, Director Imaging IT for R2, Facilities Director for R3) are accountable for hitting the target residuals and demonstrating effectiveness via the

KPI/KRI/KCI set; any drift going above risk appetite reopens treatment and all treatments aligned to NIST CSF PR.AC/PR.DS/DE.CM, CISv8, and ISO/IEC 27002 frameworks.

5.2 Control strategy (type-mapped & framework-aligned)

Scenario	Control focus	NIST CSF 2.0	CIS v8 (+IG)	ISO/IEC 27002 (theme)
R-1 EMR/PHI	Least privilege, SoD	PR.AC	5 Account Management (IG1/2), 6 Access Control (IG1/2/3)	Access control; identity management
	KMS & crypto hygiene	PR.DS	3 Data Protection (IG1/2/3)	Cryptography; key management
	DLP/UEBA, audit	DE.CM, DE.AE	8 Audit Logs (IG1/2), 13 Net Monitoring (IG1/2)	Ops security; monitoring
R-2 PACS	Segmentation, allow-listing	PR.PT, PR.AC	12 Network Infra (IG1/2/3), 10 Malware Defenses (IG1/2)	Hardening; network security
	FIM/EDR, logging	DE.CM	8 Audit Logs (IG1/2)	Logging & monitoring
R-3 BMS	IT/OT segmentation, brokered access	PR.AC, PR.PT	12 Network Infra (IG2/3), 15 Service Provider Management (IG1/2)	Supplier management; segregation
	OT monitoring & restore	DE.AE, RC.IM	11 Data Recovery (IG1/2), 13 Net Monitoring (IG2/3)	Continuity; monitoring

Table 16: Framework Crosswalk (IDs/IGs) [5], [6], [16]

R-1 EMR/PHI (Information Asset)

- **Preventive:** least-privilege & SoD for service accounts; just-in-time access; KMS with rotation; cloud guardrails; data classification & tagging.

- **Detective:** DLP tuned to PHI, UEBA for anomalous access; regular entitlement reviews.
- **Corrective/Resilience:** Immutable backups; tested breach response playbooks with PDPA notification workflows.
- **Deterrent/Compensating:** targeted awareness on phishing/MFA fatigue; role accountability.

R-2 PACS & Modalities (Non-Information IT Function Asset)

- **Preventive:** network segmentation (deny-by-default ACLs), application allow-listing on imaging gateways, code-signed updates; vendor hardening
- **Detective:** FIM on PACS servers/gateways; EDR telemetry where supported.
- **Corrective/Resilience:** golden image rebuilds, modality rollback plans, priority comms to ED/Theatres during outages.

R-3 BMS (Non-Information OT/ICS Business-Critical/Function Asset)

- **Preventive:** IT/OT segmentation by function; brokered remote access (MFA, session recording); controller hardening; secure backups of configs/setpoints; critical spares.
- **Detective:** passive OT monitoring; alerts for setpoint changes/parameter outliers; allow-list deviation alerts.
- **Corrective/Resilience:** theatre contingency SOPs; failover HVAC plans; periodic restoration drills.

5.3 Cost–Benefit (Qualitative)

Scenario	Treatment Bundle	Cost (Rel.)	Benefit (Risk↓ / Compliance↑)	Commentary
R-1	Privilege hardening + KMS + DLP/UEBA	**Medium**	**High**; strong PDPA readiness; reduced exfil risk	High ROI via breach-avoidance
R-2	Segmentation + allow-listing + FIM/EDR	**Medium**	**High**; protects diagnostics; faster detection	Direct clinical-ops benefit
R-3	IT/OT segmentation + brokered access + passive monitoring	**Medium-High**	**High**; constrains lateral movement; safeguards theatres/ICUs	Material safety uplift

Table 17: Cost-Benefit Analysis

How we're analyzing cost-efficient options:

- **Cost-effectiveness** = relative CapEx/OpEx + time-to-value vs the expected **risk** (drop in L×I) and operational load [20].
- **Compliance improvement** = how directly the bundle evidences "reasonable security" and sector obligations (PDPA; Cybersecurity Act CII where designated; ISO/IEC 27002 control themes; PCI DSS if in scope).

Evaluation (per scenario)

R1 – EMR/PHI (Privilege hardening + KMS + DLP/UEBA)

- **Cost-effectiveness:** Medium cost, high benefit. Privilege reductions and KMS rotations quickly remove high-consequence paths; DLP/UEBA increases early detection and reduces breach dwell time. Time-to-value is fast for guardrails/KMS (weeks), moderate for DLP tuning (1–2 quarters).
- **Compliance impact:** Strong PDPA uplift (protection + breach readiness), clear ISO 27002 alignment (access control, cryptography, ops monitoring). This bundle generates auditable artefacts: access review records, key-rotation logs, DLP incident workflows—useful for demonstrating "reasonable security."
- **Residual trajectory:** From 12 → **≤10** once coverage stabilizes (≥98% guardrail compliance; JIT/SoD closure; DLP detection efficacy).

R2 – PACS/Modalities (Segmentation + allow-listing + signed updates + FIM/EDR)

- **Cost-effectiveness:** Medium cost, high benefit. Deny-by-default ACLs and gateway allow-listing sharply reduce successful lateral movement. Signed update chains and FIM/EDR shrink tamper windows and improve evidence quality. Time-to-value depends on vendor footprint but typically 1–2 quarters across sites.
- **Compliance impact:** Uplifts clinical-safety posture and monitoring expectations (audit trails, integrity controls). ISO 27002 operations and system hardening themes are satisfied more fully; supplier-assurance clauses (update signing, SLA patch windows) improve contractual compliance.
- **Residual trajectory:** From 12 → **≤10** once ACLs are fully enforced, FIM/EDR coverage ≥95%, and vendors consistently deliver signed updates.

R3 – BMS (IT/OT segmentation + brokered access + passive OT monitoring + backups)

- **Cost-effectiveness:** Medium–high initial cost, but high benefit for patient-safety and outage avoidance. Brokered access (MFA + session recording) and passive monitoring decrease both event probability and blast radius; restore drills limit consequence.

- **Compliance impact:** Strengthens obligations linked to CII-style resilience if applicable and provides strong assurance for safety-critical environments; ISO 27002 continuity/monitoring themes clearly evidenced.
- **Residual trajectory:** Already at 8 (within appetite); maintain via assurance (100% brokered sessions, quarterly restore tests).

5.4 Implementation Roadmap

Phase	Timeframe	Key Activities
P1 Mobilize	Months 0–1	Confirm appetite; assign risk owners; baseline controls; approve policies
P2 Design	Months 1–3	Cloud guardrails & KMS patterns; PACS segmentation & gateway allow-listing; BMS remote-access design; metrics/dashboard design
P3 Build	Months 3–6	DLP/UEBA; EDR/FIM on PACS; enforce VLAN ACLs; brokered BMS access; secrets rotation
P4 Prove	Months 6–9	Table-tops: PHI exfil, PACS outage, BMS tamper; restore/rollback drills; red-team/segmentation tests
P5 Embed	Months 9–12	SOPs & training; supplier assurance cadence; KPI/KRI/KCI into daily governance

Table 18: Implementation Roadmap

Timeline and Cadence: The program runs over 12 months in 5 phases where **P1** mobilizes governance and baseline control coverage, **P2** completes patterns and design signoffs for cloud guardrails/KMS, PACS segmentation/allow-listing, and BMS brokered access, **P3** executes build—rolling out DLP/UEBA, enforcing deny-by-default ACLs, enabling signed-update chains and FIM/EDR on imaging gateways, and deploying brokered OT access. **P4** proves effectiveness with table-top exercises, golden-image rebuilds, restore drills, and independent validation. **P5** embeds SOPs, training, supplier assurance cadence, and KPI/KRI/KCI dashboards into day-to-day business.

Responsible parties: Accountability sits with the risk owners: Group CDO (R1 EMR/PHI), Director Imaging IT (R2 PACS), and Facilities Director (R3 BMS). Delivery is executed by cross-functional squads: Security Architecture (guardrails, KMS, access patterns), SOC Engineering (DLP/UEBA, SIEM use-cases), Network Security (segmentation, ACLs), Imaging IT (gateways, modality integration), OT Security + Facilities (brokered access, passive monitoring, backups), and GRC (policy, metrics, assurance). CISO is overall accountable for risk acceptance/treatment decisions and Procurement owns supplier obligations (signed updates, patch SLAs, remote-access terms).

Dependencies & critical path: Success is dependent on cloud guardrail coverage **≥98%** and KMS rotations so that R1 risk decreases; deny-by-default segmentation across all imaging VLANs and allow-listing on gateways so that R2 risk decreases; vendor commitment to signed-update chains and EDR/FIM coverage **≥95%** on supported gateways to also decrease likelihood of incident for R2; brokered/recorded contractor access 100% and validated offline BMS backups to decrease R3 risk. And finally, changing windows aligned to theatres and imaging rosters are the pacing item in P3–P4, and implement controls like tighter ACL on legacy modalities that lack EDR or signing.

Resource allocation. Budget splits **CapEx (enablement)** vs **OpEx (run)** by stream:

- **R1 (Medium CapEx/OpEx):** directory/SoD clean-up, KMS enablement, DLP/UEBA licenses and tuning hours.
- **R2 (Medium CapEx/OpEx):** network re-segmentation effort, gateway allow-listing, FIM/EDR licences where supported, vendor onboarding to sign updates.
- **R3 (Medium-High CapEx, Medium OpEx):** OT segmentation hardware/software where needed, brokered-access platform seats, passive OT monitoring, quarterly drill time. Staffing assumes 1–2 FTE per stream during P3 build (network/security engineers, imaging admins, OT engineers) plus shared SOC/GRC capacity for detection content and metrics. BAU absorbs ~**0.5–1.0 FTE** per stream post-P5 for tuning, reviews, and quarterly drills [20].

Assurance & hand-off. Each phase ends with an evidence gate: design artefacts in **P2**, deployment checklists and coverage report in **P3**, exercise/drill results and remediation closure in **P4**, and dashboard KPIs/KRIs/KCIs with owner sign-off in **P5**. Residual targets (R1/R2 ≤10; R3 maintained at 8) are only declared met when coverage and performance thresholds hold for one full reporting cycle; until then, items remain in “treat” rather than “monitor.”

5.5 Monitoring and Continuous Improvement

Metric Type	Example	Threshold/Target	Owner	Frequency

KPI	% EMR resources compliant with guardrails	≥ 98%	Platform Security	Weekly
KPI	% PACS gateways on latest signed image	≥ 97% within 14 days	Imaging IT	Monthly
KPI	% BMS remote sessions brokered & recorded	100%	Facilities/OT Sec	Weekly
KRI	PHI exfil alerts (true positives)	≤ 1/month; triage < 24h	SOC	Monthly
KRI	PACS study ingest failures (urgent)	≤ 0.3% / week	Imaging Ops	Weekly
KRI	OT abnormal protocol detections	Baseline ±10%	OT Sec	Weekly
KCI	Tested PDPA breach playbook	1/quarter	GRC	Quarterly
KCI	PACS rollback drill success	1/6 months	Imaging IT	Semi-annual
KCI	BMS setpoint restore test	1/quarter per site	Facilities	Quarterly

Table 19: KPI/KRI/KCI set (thresholds & ownership)

Monitoring data provenance & assurance

Data sources: cloud compliance feed, DLP/UEBA alerts, EDR/FIM events, PACS ingest logs, BMS trend logs. **GRC** performs quarterly metric quality checks; anomalies trigger corrective actions and report to senior governance.

How it actually reduces risk:

The KPI/KRI/KCI set turns our controls into a closed-loop system: **KPIs** (e.g., ≥98% cloud guardrail compliance, ≥97% signed PACS gateways, 100% brokered OT sessions) measure day-to-day control **performance** so drift is caught early; **KRIs** (e.g., PHI DLP spikes, PACS ingest-failure %, unbrokered OT sessions) provide **early warning** of emerging exposure before incidents land; and **KCIs** (e.g., quarterly PDPA breach playbook tests, PACS rollback drills, BMS setpoint restore drills) **prove effectiveness** under stress. Together, they lower **likelihood** (fewer open paths via segmentation/JIT/brokered access), shorten **dwell time** (UEBA/DLP/FIM/EDR signals + MTTR targets), and cap **consequence** (tested backups/rollback keep outages short). We use thresholds as gates: two consecutive periods **below** KPI targets or **above** KRI limits automatically re-open treatment actions; three clean periods allow re-rating (e.g., R1/R2 Likelihood from 3→2).

Review cycle (feedback > action > assurance):

- **Weekly ops huddle (Security + Imaging IT + Facilities/OT):** review KPI/KRI deltas; assign fixes for any breaches (owner + due date).
- **Monthly risk & compliance review (CISO + risk owners + GRC):** confirm remediation closure, inspect KCIs (exercise/drill outcomes), and adjust thresholds/use-cases; any repeat breaches escalate to change control.
- **Post-incident PIR (within 10 business days):** root-cause + control gaps feed new KPIs/KRIs (e.g., a new UEBA rule or tighter ACL) and update runbooks.
- **Quarterly assurance committee (Exec/CRO/Clinical Ops):** attest coverage and performance; if KPIs/KRIs/KCIs hold for the quarter, consider residual re-rating (aim: R1/R2 ≤10); if not, extend P4-style "prove" activities until green.

This cadence converts tables and graphs into repeatable governance: metrics surface drift fast, reviews drive concrete fixes, and exercises validate that fixes actually work—systematically pushing residual risk down and keeping it there.

Post-Assurance Residual Risk, Governance & RACI

Risk	Asset	Residual (before) L×I	Final Residual (post-assurance) L×I	Rating	Appetite (≤10)	Owner	Decision
R1	EMR & PHI Data Warehouse	12 (3×4)	**8 (2×4)**	Within	**Met**	Group CDO	Monitor
R2	Radiology PACS & Modalities	12 (3×4)	**8 (2×4)**	Within	**Met**	Director, Imaging IT	Monitor
R3	BMS (Theatres/ICUs)	8 (2×4)	**8 (2×4)**	Within	**Met**	Facilities Director	Monitor

Table 20: Final Residual Risk (Post Assurance)

Body	Purpose	Members	Frequency	Key artefacts/decisions

Weekly Ops Huddle	Triage KPI/KRI breaches; assign fixes	Sec Arch, SOC Eng, Network Sec, Imaging IT, OT Sec, Facilities	Weekly	Drift list; hotfix owners/dates
Monthly Risk & Compliance Review	Confirm remediation; review KCIs; adjust thresholds	CISO (chair), Risk Owners, GRC, Privacy	Monthly	Residual status; reopen “treat” if needed
Change Advisory Board (Clinical Windows)	Approve network/OT changes aligned to theatres/rosters	CAB chair, Clinical Ops, Imaging IT, Facilities, Sec	Bi-weekly	Approved change sets; rollback plans
Quarterly Assurance Committee	Attest coverage & performance; approve re-ratings	Exec, CRO, CISO, Clinical Ops, Internal Audit	Quarterly	Re-rate to final residuals; audit actions
Post-Incident Review (PIR)	Root cause; feed metrics & runbooks	IR Lead, SOC, Owners, Privacy, Clinical	As needed (≤10 days)	New use-cases; metric updates

Table 21: Governance Cadence [21]

Activity	R	A	C	I
Cloud guardrails & KMS patterns (R1)	Security Architecture	CISO	Platform, Data, Privacy	Exec
JIT/SoD rollout & access reviews (R1)	IAM Team	Group CDO	App Owners, GRC	Clinical Leads
DLP/UEBA tuning & MTTR tracking (R1)	SOC Engineering	CISO	Privacy Officer, Data	Exec
PACS segmentation/ACLs & gateway allow-listing (R2)	Network Security & Imaging IT	CIO (Cluster IT)	Vendors, Sec Arch	ED/Theatres
Signed-update enforcement with vendors (R2)	Procurement	CIO	Imaging IT, Legal, Sec	Exec

FIM/EDR on imaging gateways (R2)	SOC Eng & Imaging IT	CISO	Network Sec, Vendors	Clinical Ops
Brokered OT access (MFA, recording) (R3)	OT Security & Facilities	COO (Hospitals)	Vendors, Sec Arch	Site GMs
Passive OT monitoring & anomaly triage (R3)	OT Security	CISO	Facilities, SOC	Exec
Offline backups & restore drills (R2/R3)	Imaging IT / Facilities	CIO / COO	SOC, GRC	Audit & Risk Cttee
KPI/KRI/KCI dashboards & assurance packs	GRC	CRO	SOC, Imaging, Facilities	Exec/Board
Table-tops/PIRs & runbook updates	IR Lead	CISO	Clinical Ops, Privacy	Board/Audit

Table 22: RACI of Organization [7]

Table 20 shows all three risks **within appetite (≤10)** post-assurance, with **R1** and **R2** re-rated to **8 (2×4)** after two clean quarters and **R3** sustained at **8** after sustained continuous improvement using our KRIs (table 17). Table 20 defines how drift becomes action—weekly ops huddles, monthly risk & compliance reviews, CAB for clinical windows, quarterly assurance committee, and PIRs—with thresholds that automatically re-open treatment when breached.

The **RACI** table 22 fixes accountability: **Group CDO** (R1), **Director Imaging IT** (R2), **Facilities Director** (R3), supported by Security Architecture, SOC, Network/Imaging IT, OT Security/Facilities, GRC, and Procurement. Together, these tables turn controls into a measurable operating system: responsibilities are unambiguous, evidence is routine, and KPIs/KRIs/KCIs drive timely remediation. The outcome is sustained **likelihood reduction** (R1/R2 from 3→2), bounded consequence through practiced recovery, and a defensible, audit-ready posture. In short, ownership + evidence + cadence = risks kept **within appetite** with clear escalation paths.

Conclusion

This framework report applied ISO 31000 to SingHealth's cyber risk profile and identified three material risks—R1: EMR/PHI privacy & integrity, R2: PACS/Modalities diagnostic integrity & availability, and R3: BMS theatre/ICU environment safety. These risks were treated with least-privilege/JIT + KMS + DLP/UEBA (R1), deny-by-default segmentation + gateway allow-listing + signed updates + FIM/EDR (R2), and IT/OT segmentation + brokered access + passive OT monitoring + restore drills (R3). These controls were aligned to PDPA and (where designated) Cybersecurity Act expectations and organized via NIST CSF 2.0 and ISO/IEC 27002 regulatory expectations. These measures reduced residual risk to within appetite post-assurance (each at 2×4=8), as shown in the final section. Key learnings were that removing whole attack paths delivers the largest reduction, two clean quarters of evidence are needed to justify re-rating likelihood from 3 to 2, vendor capability (e.g., signed updates, EDR support) materially shapes outcomes, and KPI/KRI/KCI thresholds turn controls into a closed loop that prevents drift. Application of recognized risk management standards and frameworks across a 12-month roadmap with clear governance/RACI embed these improvements into day-to-day business that sustain resilience, strengthens compliance, and supports safe, reliable clinical operations for large organizations like SingHealth and more.

References

1. SingHealth. (2019). *Singapore Health Services - Singapore Hospitals and Doctors - www.singhealth.com.sg*. Singhealth.com.sg. https://www.singhealth.com.sg/
2. Luo, N., Koh, W. P., Ng, W. Y., Yau, J. W., Lim, L. K., Sim, S. S., & Tay, E. G. (2009). Acceptance of information and communication technologies for healthcare delivery: a SingHealth Polyclinics study. *Annals Academy of Medicine Singapore*, *38*(6), 529.
3. Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and CIA triangle. *Journal of medical systems*, *40*(4), 100.
4. Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk management*, *14*(4), 272-300.
5. Edwards, J. (2024). *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons.
6. Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Ltd.
7. Hartono, Y., Cahyo, W. N., & Immawan, T. (2024). The Assignment of Risk Mitigation Tasks Based on The RACI Matrix and Key Risk Indicator. *Jurnal Ilmiah Teknik Industri*, 235-244.
8. Teoh, A. A., Ghani, N. B. A., Ahmad, M., Jhanjhi, N., Alzain, M. A., & Masud, M. (2022). Organizational data breach: Building conscious care behavior in incident. *Organizational data*

breach: Building conscious care behavior in incident response. *Computer Systems Science and Engineering*, *40*(2), 505-515.

9. Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, *29*(5), 554-575.
10. Gorian, E. (2018, October). Singapore's cybersecurity act 2018: A new generation standard for critical information infrastructure protection. In *The International Science and Technology Conference" FarEastCon"* (pp. 1-9). Cham: Springer International Publishing.
11. O'Hara, K. (2008). Identity, Privacy and Technology in Singapore.
12. Vu, C., & Rajaratnam, S. (2022). *Cyber security in Singapore*. S. Rajaratnam School of International Studies.
13. HEALTH INFORMATION BILL: CYBER & DATA SECURITY GUIDEBOOK FOR HEALTHCARE PROVIDERS VERSION 1.4 APRIL 2025 DEVELOPED BY AIC AND MOH 2. (n.d.). https://www.healthinfo.gov.sg/files/Guidebook_for_Cyber_and_Data_Security_for_Healthcare_Providers_1_4.pdf
14. Trim, P., & Lee, Y. I. (2016). *Cyber security management: a governance, risk and compliance framework*. Routledge.
15. Asfoor, A. H., Kasim, H., Latif, A. B. A., Razali, R. A., Ibrahim, Z. A., & Shanneb, A. (2022). Identifying factors of non-compliance, compliance with information security policy, and behavior change to compliance: literature review. *Journal of Hunan University Natural Sciences*, *49*(12).
16. Bashofi, I., & Salman, M. (2022, June). Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)* (pp. 58-62). IEEE.
17. Piper, J. (2018). Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis. *NATO Science and Technology Organization. MP-IST-166-07*.
18. Liu, D., Xu, Z., Fan, C., & Zhou, Y. (2021). Development of fire risk visualization tool based on heat map. *Journal of Loss Prevention in the Process Industries*, *71*, 104505.
19. Bensahraoui, M., Al Nahdi, J. A., King, D. E., & Macwan, N. (2012, November). Risk Management Register in Projects & Operations. In *Abu Dhabi International Petroleum Exhibition and Conference* (pp. SPE-162500). SPE.
20. Mayeke, N. R. (2025). Evaluating the Cost-Benefit Dynamics of Cybersecurity Compliance Investments: A Multi-Sectoral Analysis Across Financial, Educational, and Ecommerce Industries.
21. Pyone, T., Smith, H., & Van Den Broek, N. (2017). Frameworks to assess health systems governance: a systematic review. *Health Policy and Planning*, *32*(5), 710-722.