10.48047/jocaaa.2023.31.04.109

Cyber Risk Modeling and Security Governance for Networked Medical Devices in Critical Healthcare Infrastructure

Prasanth Alluri
Principle IT Security Architect,California, USA

Abstract

The increasing integration of networked medical devices within critical healthcare infrastructure has significantly expanded the cyber risk surface of modern hospitals. Devices such as infusion pumps, patient monitors, imaging systems, and implantable technologies are now tightly coupled with hospital information systems, cloud services, and remote vendor platforms, creating complex interdependencies between clinical operations and digital networks. Cyber incidents affecting these devices pose not only data security and privacy risks, but also direct threats to patient safety, service continuity, and regulatory compliance. This study examines the limitations of conventional information technology risk assessment methods when applied to safety critical medical device environments and argues for a healthcare specific approach to cyber risk modeling and security governance. The paper proposes an integrated framework that combines structured cyber risk modeling with standards aligned governance mechanisms to support informed decision making in hospitals. By incorporating device criticality, network exposure, threat likelihood, and clinical impact into a unified risk assessment process, the framework enables prioritization of security controls that are both technically feasible and clinically acceptable. The study further maps risk modeling outputs to established regulatory and industry guidance, demonstrating how analytical results can be operationalized within hospital governance structures. The findings provide practical guidance for healthcare providers, regulators, and device manufacturers seeking to strengthen cyber resilience while maintaining safe and effective clinical care.

Keywords: *Cyber risk modeling; networked medical devices; Internet of Medical Things; healthcare cybersecurity; security governance; patient safety; critical infrastructure resilience*

10.48047/jocaaa.2023.31.04.109

1. Introduction

1.1 Background: IoMT growth, IT and OT convergence, and patient safety exposure

Healthcare systems worldwide are undergoing rapid digital transformation driven by the adoption of networked medical devices and the broader Internet of Medical Things (IoMT). These devices include implantable devices such as pacemakers and insulin pumps, bedside devices such as infusion pumps and patient monitors, diagnostic and imaging systems, and wearable or remote monitoring technologies. Increasingly, these devices are no longer isolated clinical tools but are integrated into hospital information systems, electronic health records, middleware platforms, cloud services, and vendor managed remote access infrastructures.

This transformation has led to a convergence of traditional information technology (IT) systems with operational technology (OT) environments in hospitals. Clinical networks now combine enterprise IT assets such as servers, databases, and workstations with safety critical OT assets such as medical devices that directly influence diagnosis, therapy, and patient outcomes. While this convergence enables interoperability, real time data exchange, and efficiency gains, it also significantly expands the cyber attack surface of healthcare infrastructure.

Unlike many other sectors, cybersecurity incidents in healthcare can have direct and immediate implications for patient safety. Disruptions to the availability, integrity, or performance of networked medical devices may delay treatment, alter therapy delivery, or compromise clinical decision making. High profile ransomware attacks and device vulnerabilities have demonstrated that cyber risk in healthcare is no longer limited to data breaches or financial losses, but extends to risks of physical harm, service disruption, and systemic loss of trust in critical healthcare services. As a result, cybersecurity for networked medical devices has become a core component of patient safety, clinical resilience, and healthcare governance.

1.2 Problem statement: limitations of conventional IT risk models in clinical environments

Despite the growing recognition of cybersecurity as a patient safety issue, many healthcare organizations continue to rely on conventional IT focused risk assessment models to manage cyber risks associated with networked medical devices. These models are typically designed for enterprise information systems and emphasize confidentiality, integrity, and availability of data assets, often expressed through qualitative risk matrices or generic compliance checklists.

10.48047/jocaaa.2023.31.04.109

However, clinical environments impose constraints and priorities that differ fundamentally from traditional IT contexts. Medical devices often operate on legacy operating systems, have limited patching and configuration options, and are subject to strict regulatory and safety requirements that restrict rapid changes. Device downtime that might be acceptable in an office IT system can be unacceptable in a clinical setting where continuity of care is essential. In addition, risk impact in healthcare cannot be adequately captured by financial or reputational metrics alone, as patient harm, clinical workflow disruption, and regulatory noncompliance play a central role.

Conventional IT risk models also struggle to represent the interconnected nature of hospital systems, where compromise of a single device or subnet can propagate across clinical networks and affect multiple services. They frequently lack mechanisms to incorporate device criticality, clinical context, and risk propagation pathways into decision making. As a result, healthcare organizations face difficulties prioritizing cybersecurity investments, aligning technical controls with governance decisions, and demonstrating risk based justification to clinical leadership and regulators.

1.3 Aim and research questions

The primary aim of this study is to develop a structured and healthcare specific approach to cyber risk modeling and security governance for networked medical devices operating within critical healthcare infrastructure. The study seeks to bridge the gap between technical risk assessment and organizational governance by providing a framework that is both analytically rigorous and operationally practical.

To achieve this aim, the study is guided by the following research questions:

- How can cyber risks associated with networked medical devices be modeled in a way that reflects clinical criticality, patient safety, and interdependencies within hospital networks?
- What limitations do existing risk assessment approaches present when applied to IoMT environments in healthcare?
- How can cyber risk modeling outputs be systematically integrated into security governance, compliance, and decision making processes in hospitals?
- What practical artifacts and metrics can support healthcare organizations in prioritizing controls, investments, and postmarket security activities for medical devices?

1.4 Contributions of the study

This research makes several key contributions to the field of healthcare cybersecurity and medical device risk management.

10.48047/jocaaa.2023.31.04.109

First, it proposes a cyber risk modeling framework tailored to networked medical devices that explicitly incorporates device criticality, clinical impact, threat likelihood, and network exposure. Unlike generic IT risk assessments, the proposed approach emphasizes patient safety and operational resilience as core dimensions of cyber risk.

Second, the study integrates cyber risk modeling with security governance by mapping analytical outputs to governance mechanisms such as policy enforcement, control selection, compliance reporting, and executive decision making. This integration addresses a critical gap in current practice, where technical risk assessments are often disconnected from organizational accountability and resource allocation.

Third, the paper provides operationalizable artifacts, including structured risk inputs, scoring logic, prioritization matrices, and governance workflows, that can be adopted or adapted by healthcare organizations. These artifacts are designed to support real world implementation, regulatory alignment, and audit readiness rather than remaining purely conceptual.

Finally, the study contributes to the academic literature by synthesizing insights from medical device security, healthcare informatics, risk management, and governance frameworks into a unified model applicable to modern IoMT enabled healthcare systems.



Figure 1. Study focus and scope

10.48047/jocaaa.2023.31.04.109

2. Networked Medical Devices in Critical Healthcare Infrastructure

2.1 Definitions and device classes

Networked medical devices refer to medical equipment that relies on digital connectivity to exchange data with other devices, hospital information systems, or external services for clinical operation, monitoring, or maintenance. Within modern healthcare environments, these devices form the core of the Internet of Medical Things and are embedded in safety critical clinical workflows. Regulatory and standards bodies define medical devices broadly as instruments intended for diagnosis, monitoring, treatment, or mitigation of disease, whose safety and effectiveness must be preserved throughout their lifecycle (ISO, 2019; IEC, 2021a).

Implantable medical devices include pacemakers, implantable cardioverter defibrillators, neurostimulators, and insulin pumps. These devices are characterized by long service lifecycles, strict safety certification requirements, and highly constrained update mechanisms. Although many implantables communicate wirelessly with external programmers or home monitoring units, security modifications are often limited due to patient safety considerations and regulatory constraints (Halperin et al., 2008; Cámara et al., 2015).

Bedside clinical devices encompass patient monitors, infusion pumps, ventilators, and anesthesia machines. These devices are typically connected to clinical networks for centralized monitoring, alarm management, and integration with electronic health record systems. Bedside devices frequently run embedded or customized operating systems and are deployed in large numbers across hospitals, which increases the scale and complexity of their cyber risk exposure (Sametinger et al., 2015; Williams C Woodward, 2015).

Imaging and diagnostic systems, such as MRI, CT, ultrasound, and laboratory analyzers, represent another critical device class. These systems are highly network dependent and often integrate directly with Picture Archiving and Communication Systems and radiology information systems. Imaging devices commonly rely on commercial operating systems and third party software components, which can introduce vulnerabilities inherited from general purpose IT platforms (Maisel et al., 2006; Rasool et al., 2022).

Infusion devices and therapeutic delivery systems, including smart infusion pumps and dialysis machines, occupy a particularly sensitive position because cyber incidents affecting these devices may directly alter therapy delivery. Security weaknesses in these systems can therefore have immediate patient safety implications, reinforcing

10.48047/jocaaa.2023.31.04.109

the need for risk modeling approaches that extend beyond data protection considerations (Park, 2014; Farlow et al., 2023).

2.2 Connectivity and data flows

The clinical value of networked medical devices is closely tied to their integration with hospital information systems and external services. Data generated by devices are commonly transmitted to Electronic Health Record platforms to support documentation, clinical decision making, and continuity of care. For example, bedside monitors continuously stream vital sign data into EHR systems, enabling clinicians to review patient status remotely and over time (Weininger et al., 2017).

Diagnostic imaging devices exchange large volumes of data with Picture Archiving and Communication Systems, which store, index, and distribute medical images across departments. These data flows are essential for clinical workflows but also create high value targets for cyber attackers due to the sensitivity and operational importance of imaging data (Li et al., 2025).

Middleware platforms play a central role in aggregating, normalizing, and routing data between heterogeneous medical devices and hospital systems. While middleware improves interoperability, it also introduces additional software layers and interfaces that may expand the attack surface and complicate responsibility for security controls (Richter C Ammenwerth, 2023).

Remote monitoring and vendor managed services further extend data flows beyond hospital boundaries. Many devices transmit telemetry to cloud platforms for performance monitoring, predictive maintenance, or patient follow up. Remote access pathways, while operationally beneficial, represent a significant source of cyber risk if not governed through strong authentication, segmentation, and contractual security requirements (AAMI, 2019; FDA, 2016).

2.3 Hospital network zones and trust boundaries

To manage complexity and reduce risk, healthcare organizations typically segment their networks into distinct zones based on function and trust level. Clinical device networks often operate as dedicated virtual local area networks that isolate medical devices from general purpose enterprise IT systems. This segmentation is intended to limit lateral movement and protect device availability during cyber incidents (Stouffer et al., 2023). Enterprise IT networks host systems such as EHR servers, administrative applications, and user workstations. Although these systems may not directly control medical devices, they frequently serve as gateways for data exchange and user authentication, making them critical dependencies in the overall risk landscape (NIST, 2024).

10.48047/jocaaa.2023.31.04.109

Operational technology segments may be present in facilities where medical devices interact with building management systems, power infrastructure, or specialized clinical automation. These OT segments often follow different security and lifecycle management practices than IT systems, complicating unified governance and risk assessment (IEC, 2013; IEC, 2018).

Vendor access zones and external connections represent another key trust boundary. Medical device manufacturers and service providers commonly require remote access for software updates, diagnostics, and support. If these connections are insufficiently controlled, they may bypass internal safeguards and introduce supply chain related risks into clinical environments (IMDRF, 2020; Ostermann et al., 2025).

Understanding these zones and boundaries is essential for accurate cyber risk modeling. Risk does not reside solely within individual devices, but emerges from the interaction between device classes, data flows, and network trust relationships within critical healthcare infrastructure.

Table 1. Device categories, connectivity, and typical security constraints

Device class	Interfaces	Typical OS or firmware	Update feasibility	Clinical criticality	Common exposure points
Implantable devices	Wireless telemetry, external programmer	Proprietary embedded firmware	Very limited, tightly regulated	Very high	Wireless interfaces, external programmers
Bedside clinical devices	Ethernet, Wi-Fi, serial interfaces	Embedded Linux or customized OS	Limited, scheduled maintenance	High	Clinical networks, middleware connections
Imaging and diagnostic systems	Ethernet, PACS interfaces	Commercial OS with vendor software	Moderate, vendor controlled	High	PACS integration, third party software
Infusion and therapy devices	Ethernet, Wi-Fi, device controllers	Embedded real-time OS	Limited due to safety constraints	Very high	Network connectivity, configuration interfaces
Remote monitoring devices	Cellular, Wi-Fi, cloud APIs	Embedded OS with cloud agents	Moderate, over- the-air updates	Medium to high	Cloud platforms, vendor managed services

3. Threat Landscape and Attack Surface for Medical Devices

3.1 Threat actors

The threat landscape affecting networked medical devices is shaped by a diverse set of actors with varying motivations, capabilities, and targets. Cybercriminal groups represent the most visible and prevalent threat to healthcare infrastructure. Their

10.48047/jocaaa.2023.31.04.109

primary motivations are financial, often pursued through ransomware attacks, data exfiltration, and extortion schemes. Hospitals are attractive targets due to their operational urgency, limited tolerance for downtime, and historically uneven cybersecurity maturity, which increases the likelihood of ransom payment during disruptions (Jiang et al., 2025; Shahzadi et al., 2025).

Nation state and state sponsored actors pose a more covert but potentially severe risk. These actors may target healthcare infrastructure for espionage, strategic intelligence gathering, or as part of broader geopolitical campaigns. Medical research data, population health information, and critical healthcare services can be of strategic value, particularly during public health crises. While such actors may not directly aim to disrupt patient care, their presence within networks can create latent risks if tools or access are repurposed or leaked (ENISA, 2021; Lee et al., 2023).

Insider threats include both malicious insiders and unintentional actors such as clinicians or technicians who inadvertently introduce vulnerabilities. In clinical environments, high workload, emergency operations, and usability constraints can lead to insecure practices such as password sharing, unmanaged device connections, or bypassing security controls. Given their legitimate access to systems and devices, insiders can significantly expand the attack surface, whether intentionally or accidentally (Williams C Woodward, 2015).

Supply chain actors, including medical device manufacturers, software vendors, and service providers, represent an increasingly critical threat vector. Vulnerabilities introduced during device development, insecure update mechanisms, or compromised vendor credentials can provide attackers with privileged access to hospital networks. The reliance on remote maintenance and third party software components makes supply chain risk a central concern for medical device security governance (AAMI, 2019; IMDRF, 2020).

3.2 Common attack vectors

Ransomware entry paths remain one of the most common initial access mechanisms in healthcare cyber incidents. Attackers frequently exploit phishing emails, compromised credentials, or exposed remote access services to gain a foothold in hospital IT environments. Once inside, they may pivot toward clinical networks that host medical devices, leveraging weak segmentation or shared services to expand their reach (Li et al., 2025; Stouffer et al., 2023).

Lateral movement is a key phase in many attacks involving networked medical devices. After initial compromise, attackers seek to traverse network segments to reach high

10.48047/jocaaa.2023.31.04.109

value targets such as device management systems, middleware platforms, or imaging servers. Flat network architectures, legacy protocols, and insufficient monitoring can facilitate this movement, allowing attackers to impact multiple devices or departments simultaneously (Rasool et al., 2022).

Remote services and vendor access pathways are another prominent attack vector. Many medical devices depend on remote connectivity for diagnostics, updates, and support. If remote access is enabled without strong authentication, network isolation, and continuous oversight, it can serve as a direct conduit into clinical environments. Misconfigured virtual private networks, shared vendor accounts, and insufficient logging have all been associated with healthcare security incidents (FDA, 2016; Ostermann et al., 2025).

In addition, vulnerabilities in middleware and integration engines can be exploited to manipulate data flows between devices and hospital systems. Because middleware often aggregates data from many devices, compromise at this layer can amplify the impact of an attack and obscure detection efforts (Richter C Ammenwerth, 2023).

3.3 Medical device specific weaknesses

Medical devices exhibit a range of structural weaknesses that distinguish them from conventional IT assets. One of the most significant challenges is the prevalence of legacy operating systems and proprietary firmware. Many devices remain in service for ten to twenty years and may rely on outdated software that no longer receives security updates, creating persistent exposure to known vulnerabilities (Halperin et al., 2008; Sametinger et al., 2015).

Patch constraints further complicate risk mitigation. Unlike enterprise systems, medical devices cannot always be patched promptly due to regulatory approval requirements, validation testing, and the need to avoid disrupting clinical operations. In some cases, patches must be coordinated with manufacturers and scheduled during maintenance windows that may be infrequent or clinically constrained (ISO, 2019; AAMI, 2016).

Vendor tools and service software can also introduce risk. Device configuration utilities, remote diagnostic tools, and update mechanisms often require elevated privileges and persistent connectivity. If these tools are not securely designed or adequately governed, they may bypass local security controls and expose devices to unauthorized access (AAMI, 2019; IEC, 2021b).

Additionally, many devices lack native security features such as strong authentication, encryption, or detailed logging. This limits visibility into device behavior and hampers

10.48047/jocaaa.2023.31.04.109

incident detection and response, increasing the likelihood that attacks will go unnoticed until clinical impact occurs (Williams C Woodward, 2015).

3.4 Safety impacts of cyber threats

The consequences of cyber threats to medical devices extend beyond traditional information security concerns and directly affect patient safety and clinical operations. Loss of availability is often the most immediate and visible impact. Ransomware or denial of service attacks can render devices or entire clinical networks unavailable, forcing care delays, patient diversion, or manual workarounds that increase the risk of error (Jiang et al., 2025).

Integrity compromise poses a more insidious threat. Unauthorized modification of device settings, calibration data, or transmitted measurements can lead to incorrect diagnoses or inappropriate therapy delivery. Such impacts may be difficult to detect, particularly if clinicians continue to trust compromised systems (Halperin et al., 2008; Cámara et al., 2015).

Clinical workflow disruption is another critical outcome. Even when patient harm is avoided, cyber incidents can degrade situational awareness, overwhelm staff, and strain coordination between departments. Prolonged disruptions erode trust in digital systems and can have cascading effects across critical healthcare services (Weininger et al., 2017).

These safety impacts underscore the need for threat modeling approaches that explicitly account for clinical context and patient outcomes, rather than treating medical devices as conventional IT endpoints.

10.48047/jocaaa.2023.31.04.109

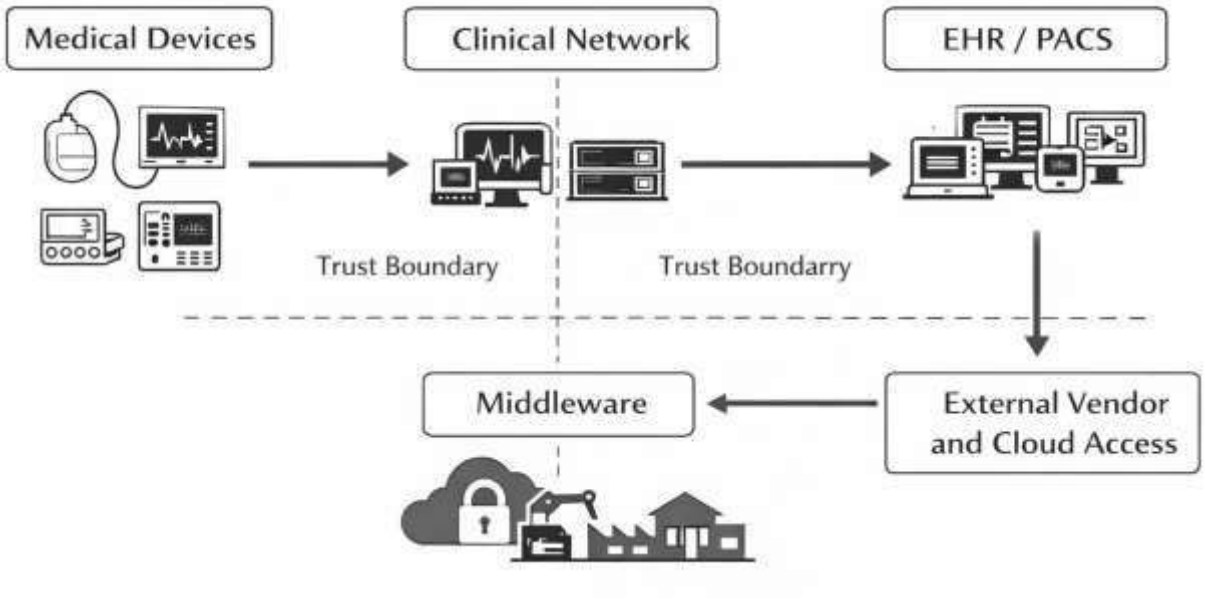


Figure 2. Attack surface map for networked medical devices

Table 2. Threat taxonomy mapped to clinical impact

Threat type	Vector	Affected asset	Likely outcome	Patient safety implication	Example control
Ransomware	Phishing, exposed remote services	EHR, device networks	Loss of availability	Treatment delays, patient diversion	Network segmentation, offline backups
Lateral movement attack	Compromised credentials	Multiple device subnets	Widespread device disruption	Reduced monitoring and therapy capability	Zero trust access controls
Supply chain compromise	Vendor software update	Medical devices, middleware	Persistent unauthorized access	Undetected manipulation of device behavior	Secure update validation, vendor risk management
Insider misuse	Legitimate access abuse	Device configurations	Integrity compromise	Incorrect therapy delivery	Role based access control
Data manipulation	Middleware exploitation	Clinical data streams	Altered measurements	Misdiagnosis or delayed intervention	Data integrity checks, monitoring

4. Cyber Risk Modeling Foundations for Healthcare IoMT

4.1 Core risk concepts in medical device environments

Cyber risk modeling provides a structured means of estimating the likelihood and consequences of adverse cyber events. In healthcare IoMT contexts, several foundational concepts must be interpreted through a clinical and operational lens.

10.48047/jocaaa.2023.31.04.109

- **Likelihood** refers to the probability that a specific threat event will occur within a defined time horizon. In medical device environments, likelihood is influenced by factors such as device exposure to networks, prevalence of known vulnerabilities, threat actor activity, and the presence or absence of effective controls. Unlike general IT systems, likelihood estimation for medical devices must account for constrained patch cycles and long device lifetimes, which can elevate exposure over time (NIST, 2012; AAMI, 2016).
- **Impact** represents the magnitude of harm resulting from a successful cyber event. In healthcare, impact extends beyond financial loss or data confidentiality breaches to include patient safety, interruption of clinical services, regulatory consequences, and reputational damage. Impact assessment must therefore incorporate clinical severity, potential for patient harm, and duration of service disruption, rather than relying solely on traditional business impact metrics (ISO, 2019; FDA, 2016).
- **Exposure** captures the degree to which an asset is reachable by a threat actor. For networked medical devices, exposure is shaped by network architecture, remote access pathways, middleware dependencies, and trust relationships across hospital systems. Devices connected to multiple networks or external services typically exhibit higher exposure than isolated or segmented assets (Rasool et al., 2022).
- **Vulnerability** refers to weaknesses that can be exploited by threat actors. In IoMT environments, vulnerabilities often arise from legacy operating systems, insecure communication protocols, weak authentication mechanisms, and third party software components. The inability to rapidly remediate vulnerabilities due to safety and regulatory constraints amplifies their significance in risk calculations (Sametinger et al., 2015; Williams C Woodward, 2015).
- **Criticality** is a distinguishing concept in healthcare risk modeling. It reflects the importance of a device or system to patient care and clinical operations. Devices that directly deliver therapy or support life sustaining functions possess higher criticality than devices used for ancillary or administrative purposes. Incorporating criticality into risk models ensures that prioritization aligns with patient safety and care continuity, rather than purely technical considerations (IEC, 2021a; AAMI, 2019).

4.2 Why healthcare is different: safety critical constraints and downtime limits

Healthcare IoMT environments differ fundamentally from conventional enterprise IT settings due to their safety critical nature. Medical devices are often integral to diagnosis and therapy, meaning that cyber incidents can translate into physical harm if

10.48047/jocaaa.2023.31.04.109

not properly managed. As a result, healthcare organizations operate under stringent regulatory frameworks that emphasize safety, effectiveness, and risk management throughout the device lifecycle (ISO, 2019; IEC, 2021b).

Operational downtime tolerance in healthcare is extremely limited. While planned outages may be acceptable in many IT environments, unplanned downtime in clinical settings can delay treatment, force patient diversion, or necessitate manual workarounds that increase error risk. These constraints limit the feasibility of aggressive security interventions such as frequent reboots, rapid patch deployment, or intrusive monitoring agents on devices (FDA, 2016; Jiang et al., 2025).

Furthermore, responsibility for medical device security is distributed across multiple stakeholders, including hospitals, manufacturers, vendors, and regulators. This shared responsibility complicates risk ownership and control implementation, reinforcing the need for governance aware risk models that can support coordinated decision making rather than isolated technical assessments (IMDRF, 2020; Ostermann et al., 2025).

4.3 Risk model options for healthcare IoMT

Several categories of cyber risk models are commonly applied in practice, each with implications for suitability in medical device environments.

- **Qualitative risk models** rely on expert judgment and descriptive scales to assess likelihood and impact. These models are widely used in healthcare due to their simplicity and alignment with compliance driven processes. However, they often lack precision, suffer from subjective bias, and provide limited support for prioritizing investments across complex device ecosystems (NIST, 2012).
- **Semi quantitative models** introduce numerical scoring or weighted matrices to improve comparability between risks. By assigning scores to factors such as exposure, vulnerability, and criticality, semi quantitative approaches offer greater structure while remaining relatively accessible. Nevertheless, their outputs may still obscure uncertainty and can give a false sense of precision if underlying assumptions are not transparent (AAMI, 2016).
- **Quantitative risk models**, such as those based on the FAIR methodology, seek to estimate risk in probabilistic and monetary terms. These models can support more rigorous decision making by explicitly modeling threat frequency, loss magnitude, and uncertainty. In healthcare contexts, quantitative approaches can be challenging due to limited historical data, difficulty monetizing patient harm, and the complexity of modeling interconnected clinical systems (The Open Group, 2013).

10.48047/jocaaa.2023.31.04.109

- **Attack graph based models** focus on mapping potential attack paths through networks and systems. By representing how vulnerabilities and trust relationships can be chained together, attack graphs are particularly useful for understanding lateral movement and cascading risk in hospital environments. However, they require detailed network and configuration data and may be computationally intensive to maintain at scale (Koo et al., 2022; Palma C Bonomi, 2025).

4.4 Model selection rationale for this study

Given the characteristics of healthcare IoMT environments, this study adopts a hybrid risk modeling approach that combines elements of semi quantitative scoring with attack graph inspired dependency analysis. This selection balances analytical rigor with practical feasibility, acknowledging the data limitations and safety constraints inherent in medical device ecosystems.

Semi quantitative scoring enables the incorporation of clinical criticality, exposure, and vulnerability in a structured manner that is accessible to both technical and nontechnical stakeholders. Attack graph concepts are used to model propagation pathways and interdependencies without requiring full scale probabilistic computation. This hybrid approach supports prioritization, transparency, and governance alignment while avoiding overreliance on uncertain quantitative estimates.

By design, the selected model produces outputs that can be readily mapped to governance processes, including control selection, investment prioritization, and compliance reporting. This alignment ensures that cyber risk modeling serves as an enabler of security governance rather than a standalone analytical exercise.

Table 3. Comparison of risk modeling approaches for medical device environments

Method	Data needs	Outputs	Strengths	Limitations	Best use case
Qualitative	Expert judgment, high level asset lists	Descriptive risk ratings	Simple, low data burden	Subjective, limited prioritization	Initial assessments, compliance reviews
Semi quantitative	Asset inventory, vulnerability data, criticality scores	Ranked risk scores	Structured, interpretable	Limited uncertainty representation	Operational prioritization in hospitals
Quantitative (FAIR)	Threat frequency, loss data, control effectiveness	Probabilistic loss estimates	Rigorous, decision focused	Data intensive, complex	Strategic investment analysis
Attack graph based	Network topology, vulnerabilities, trust relationships	Attack paths and propagation insights	Reveals cascading risk	High modeling effort	Network segmentation and resilience planning

10.48047/jocaaa.2023.31.04.109

5. Proposed Cyber Risk Modeling Framework for Networked Medical Devices

5.1 Model inputs

Effective cyber risk modeling for networked medical devices depends on the quality, completeness, and clinical relevance of its inputs. Unlike generic IT environments, healthcare IoMT ecosystems require inputs that reflect device lifecycle constraints, clinical usage, and network dependencies.

- **Device inventory** forms the foundation of the model. This inventory must include not only device type and manufacturer, but also clinical function, deployment location, connectivity characteristics, and lifecycle status. Incomplete or outdated inventories are a well documented challenge in hospitals and are a primary source of risk blind spots (Richter C Ammenwerth, 2023). For this framework, devices are uniquely identified and mapped to clinical services to support criticality assessment.
- **Vulnerability data** is drawn from multiple sources, including manufacturer advisories, coordinated vulnerability disclosure programs, and publicly available databases. Given that many medical devices cannot be patched immediately, vulnerabilities are treated as persistent risk factors rather than transient issues. The model therefore emphasizes vulnerability severity, exploitability, and compensating controls rather than patch status alone (AAMI, 2016; ISO, 2019).
- **Threat intelligence** provides contextual information on active threat actors, prevalent attack techniques, and sector specific campaigns targeting healthcare. Rather than attempting real time prediction, threat intelligence is used to adjust likelihood estimates and identify relevant attack vectors for specific device classes and network zones (ENISA, 2021; Jiang et al., 2025).
- **Network topology** captures how devices, middleware, and core hospital systems are interconnected. This includes segmentation boundaries, shared services, authentication dependencies, and external connections. Topological data enables the model to assess exposure and understand how compromise may propagate across trust boundaries (Stouffer et al., 2023).
- **Existing controls** represent the final input category. These include technical safeguards such as network segmentation, access control, and monitoring, as well as procedural and governance controls such as patch approval processes and vendor access policies. Control effectiveness is considered when estimating residual risk, ensuring that the model reflects actual operational conditions rather than theoretical exposure (NIST, 2024).

10.48047/jocaaa.2023.31.04.109

5.2 Risk scoring design

The proposed framework employs a structured risk scoring approach that integrates clinical criticality, threat likelihood, and exposure into a single interpretable metric. This design supports prioritization while remaining transparent to both technical and clinical stakeholders.

- **Clinical criticality weighting** is applied to reflect the potential patient safety impact of device compromise. Devices directly involved in life sustaining or therapy delivery functions are assigned higher criticality weights than devices used for ancillary or administrative purposes. This weighting ensures that patient safety considerations dominate prioritization decisions, consistent with healthcare risk management principles (IEC, 2021a; AAMI, 2019).
- **Threat likelihood** is estimated by combining threat intelligence relevance, historical incident patterns, and vulnerability exploitability. Rather than relying on precise probabilities, likelihood is expressed using calibrated ordinal scales that balance realism with data availability. This approach reduces false precision while maintaining comparability across risks (NIST, 2012).
- **Exposure assessment** captures how reachable a device or system is from potential threat entry points. Exposure factors include network segmentation strength, presence of remote access, reliance on shared services, and middleware dependencies. Devices located in highly connected zones or accessible through external pathways receive higher exposure scores (Rasool et al., 2022).

The overall risk score is derived by combining these components in a weighted formulation that can be tuned to organizational priorities. Importantly, the scoring logic is explicitly documented, allowing governance bodies to understand how scores are generated and to adjust assumptions as conditions change.

5.3 Propagation logic and dependency modeling

A defining feature of the proposed framework is its ability to represent how cyber risk propagates across interconnected hospital systems. Medical devices rarely operate in isolation, and compromise of one component can cascade through dependencies to affect multiple clinical services.

Propagation logic is informed by attack graph principles, mapping how attackers can move from initial entry points to higher value targets through network paths, shared credentials, or middleware platforms (Koo et al., 2022; Palma C Bonomi, 2025). Rather than constructing exhaustive graphs, the framework focuses on clinically meaningful dependency chains, such as device to middleware to EHR or PACS.

10.48047/jocaaa.2023.31.04.109

Trust boundaries are explicitly represented to highlight where controls should prevent or detect lateral movement. For example, segmentation between clinical device networks and enterprise IT systems is modeled as a boundary that reduces, but does not eliminate, propagation risk. If a boundary is weak or bypassed through vendor access, the model reflects increased propagation likelihood.

This dependency aware approach enables identification of systemic risks that may not be apparent when assessing devices individually. It also supports evaluation of control effectiveness at architectural choke points, where targeted improvements can reduce risk across many assets simultaneously.

5.4 Model outputs and governance alignment

The outputs of the framework are designed to support both technical remediation and executive level governance.

- **Prioritized risk lists** rank device and system risks based on residual risk scores, enabling focused allocation of limited security resources. Because scores incorporate clinical criticality, these lists naturally align with patient safety priorities rather than purely technical severity.
- **Control gap maps** identify where existing safeguards are insufficient relative to risk exposure. By mapping risks to specific control domains, such as segmentation, access control, or monitoring, the framework supports actionable remediation planning (ISO/IEC, 2022).
- **Governance ready metrics** translate technical findings into indicators suitable for oversight and decision making. Examples include counts of high criticality devices with unresolved vulnerabilities, proportion of clinical networks with strong segmentation, and trends in residual risk over time. These metrics support accountability, compliance reporting, and continuous improvement (NIST, 2024).

By producing outputs that are interpretable, auditable, and aligned with governance processes, the framework ensures that cyber risk modeling functions as a practical decision support tool rather than a standalone analytical exercise.

10.48047/jocaaa.2023.31.04.109

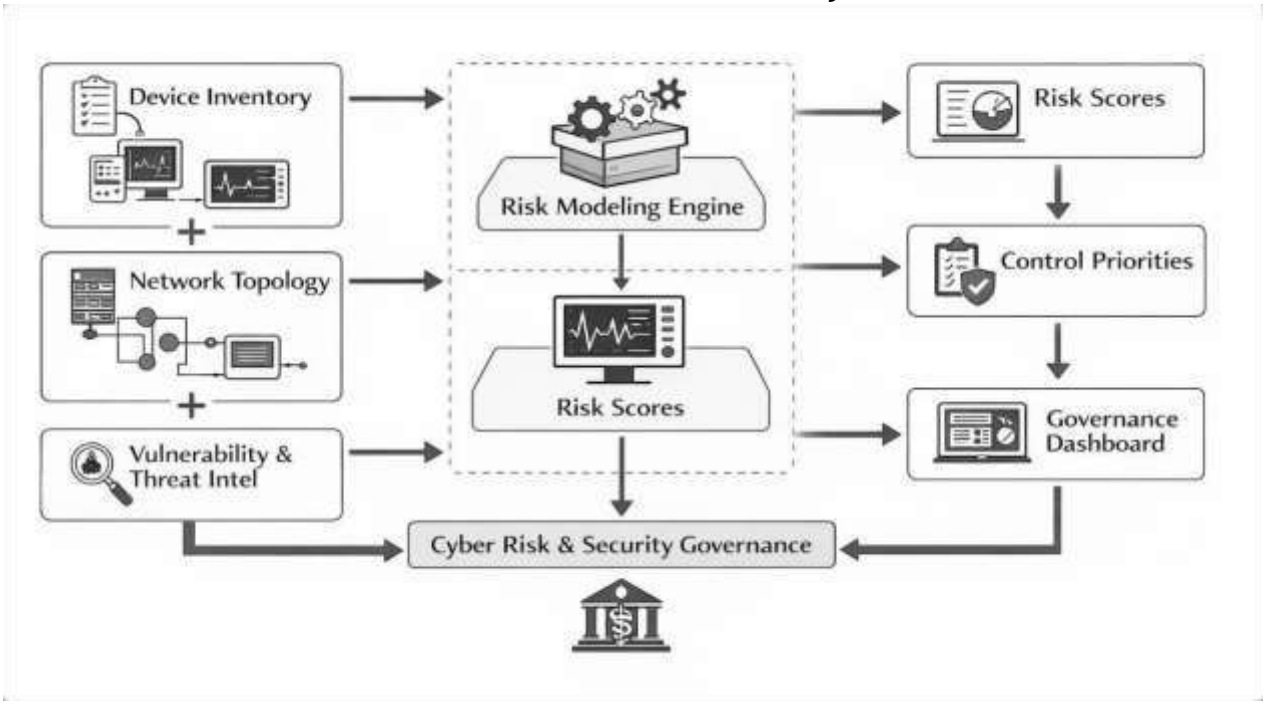


Figure 3. Cyber risk modeling workflow for IoMT

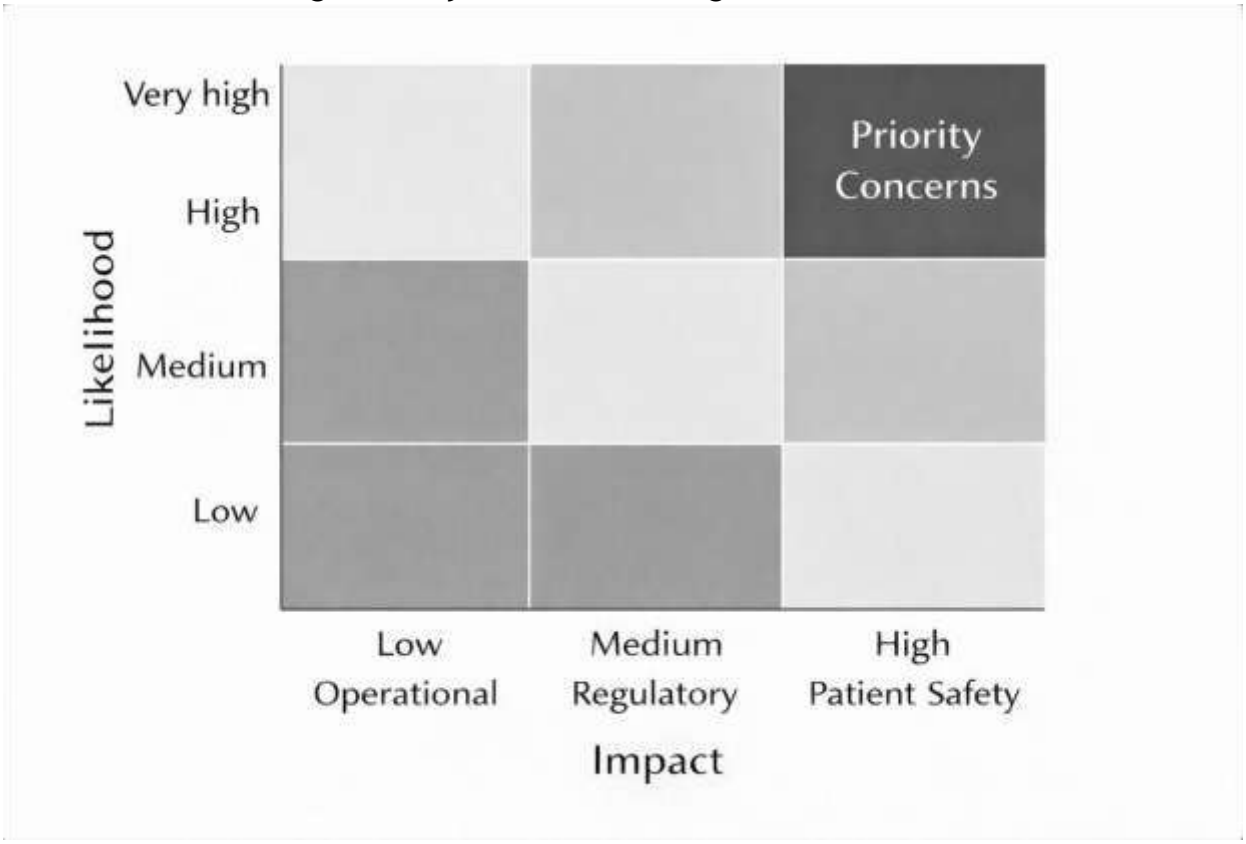


Figure 4. Likelihood-Impact Risk Matrix for Healthcare IoMT

10.48047/jocaaa.2023.31.04.109

This risk matrix illustrates the prioritization of cyber risks affecting networked medical devices by mapping estimated threat likelihood against clinically defined impact severity. Impact is assessed based on patient safety consequences, operational downtime, and regulatory exposure. Risks positioned in the high or very high likelihood and high impact region represent priority concerns that require immediate governance attention and mitigation.

6. Security Governance and Compliance for Medical Devices

6.1 Governance goals

Security governance for networked medical devices establishes the structures, processes, and accountability mechanisms through which cyber risk is directed and controlled. In safety critical healthcare environments, governance goals extend beyond technical protection to encompass patient safety, regulatory compliance, and organizational resilience.

- **Accountability** is the foundation of effective governance. Healthcare organizations must define clear ownership for medical device cybersecurity risks, ensuring that decisions related to risk acceptance, mitigation, and escalation are formally assigned and auditable. Without explicit accountability, cyber risk decisions may be deferred, fragmented, or implicitly transferred across departments, increasing systemic exposure (AAMI, 2016; IMDRF, 2020).
- **Policy alignment** ensures that cybersecurity practices for medical devices are consistent with organizational policies, clinical safety objectives, and external regulatory expectations. Governance frameworks translate high level policies into enforceable requirements for device procurement, deployment, operation, and maintenance. Alignment is particularly important in healthcare, where clinical priorities and security controls must be balanced to avoid unintended disruption of care (IEC, 2021a; ISO, 2019).
- **Assurance** refers to the ability to demonstrate that controls are implemented and functioning as intended. Assurance activities include audits, monitoring, risk reviews, and evidence collection to support regulatory inspections and internal oversight. In medical device environments, assurance must address both cybersecurity and safety requirements, reflecting their interdependence (ISO/IEC, 2022; NIST, 2024).
- **Resilience** emphasizes the capacity of healthcare systems to anticipate, withstand, recover from, and adapt to cyber incidents. Given the inevitability of cyber threats, governance must support preparedness, incident response, and recovery planning to maintain continuity of care. Resilience oriented governance

10.48047/jocaaa.2023.31.04.109

recognizes that risk cannot be eliminated entirely, but must be managed dynamically over time (NIST, 2024; Jiang et al., 2025).

6.2 Alignment with standards and guidance

Medical device cybersecurity governance is shaped by a complex ecosystem of standards, technical reports, and regulatory guidance. Effective governance requires harmonizing these sources into a coherent and actionable framework.

AAMI TIR57 and TIRG7 provide practical guidance on risk management and postmarket cybersecurity activities for medical devices. TIR57 focuses on integrating cybersecurity into risk management processes, emphasizing threat modeling, vulnerability assessment, and control selection. TIR97 extends this approach into the postmarket phase, addressing monitoring, vulnerability disclosure, and coordinated response activities (AAMI, 2016; AAMI, 2019).

- **IEC 80001-1** addresses risk management for IT networks incorporating medical devices, with a focus on shared responsibility between healthcare delivery organizations and manufacturers. It emphasizes the identification of roles, responsibilities, and risk acceptance criteria when devices are connected to clinical networks (IEC, 2021a).
- **IEC 81001-5-1** provides lifecycle oriented security requirements for health software and health IT systems, including activities related to secure development, deployment, maintenance, and decommissioning. This standard reinforces the need for security considerations throughout the device lifecycle, aligning closely with postmarket governance objectives (IEC, 2021b).
- **ISO 14G71** establishes the overarching framework for medical device risk management, traditionally focused on safety risks. Increasingly, cybersecurity risks are recognized as contributors to safety hazards, making ISO 14971 a critical anchor for integrating cyber risk into clinical risk management processes (ISO, 2019).
- **ISO/IEC 27001 and ISO/IEC 27002** provide a comprehensive information security management system framework and control catalogue. While not specific to medical devices, these standards support governance by defining policies, risk assessment processes, and control domains applicable to healthcare environments when tailored appropriately (ISO/IEC, 2022).
- **NIST Cybersecurity Framework 2.0** offers a flexible, outcome based structure for managing cybersecurity risk across organizations. Its functions and categories support alignment between technical controls, governance objectives, and performance measurement, making it particularly suitable for executive oversight and continuous improvement in healthcare settings (NIST, 2024).

10.48047/jocaaa.2023.31.04.109

6.3 Roles and responsibilities

Cybersecurity governance for medical devices depends on clearly defined roles across multiple stakeholders, each contributing to risk management within their sphere of control.

Hospitals and healthcare delivery organizations are responsible for the secure deployment, configuration, and operation of medical devices within their networks. This includes asset inventory management, network segmentation, access control, monitoring, and incident response. Hospitals also play a central role in risk acceptance decisions, balancing clinical needs with security considerations (IEC, 2021a; Richter C Ammenwerth, 2023).

Medical device manufacturers are responsible for designing devices with appropriate security controls, managing vulnerabilities throughout the product lifecycle, and providing timely security updates and documentation. Manufacturers are also expected to support coordinated vulnerability disclosure and collaborate with healthcare organizations during incident response (AAMI, 2019; IMDRF, 2020).

Vendors and service providers often manage remote access, maintenance, and cloud based services associated with medical devices. Their responsibilities include securing remote connections, protecting credentials, and adhering to contractual security requirements. Weak governance of vendor activities has been repeatedly identified as a source of elevated risk in healthcare environments (FDA, 2016; Ostermann et al., 2025).

Regulators and oversight bodies establish expectations for safety, effectiveness, and cybersecurity through guidance, standards, and enforcement mechanisms. While regulators do not manage individual devices, their frameworks shape governance practices by defining acceptable risk management processes and evidence requirements (FDA, 2023; ISO, 2019).

6.4 Postmarket managementand continuous governance

Postmarket cybersecurity management is a critical component of medical device governance, reflecting the reality that risks evolve after deployment. Continuous monitoring enables early detection of anomalous behavior, emerging threats, and changes in exposure. Monitoring activities must be proportionate to clinical risk and compatible with device safety constraints (AAMI, 2019; NIST, 2024).

- **Coordinated vulnerability disclosure** processes facilitate responsible reporting and remediation of security weaknesses. Governance frameworks should define how vulnerabilities are received, assessed, prioritized, and communicated across

10.48047/jocaaa.2023.31.04.109

stakeholders. Clear timelines and escalation paths support transparency and trust while reducing the likelihood of unmanaged exposure (ISO/IEC, 2018).

- **Patch governance** addresses the unique challenges of updating medical devices. Governance processes must ensure that patches are evaluated for safety impact, scheduled appropriately, and supported by compensating controls when immediate remediation is not feasible. Documented patch governance supports both assurance and regulatory compliance (FDA, 2016; IEC, 2021b).

By embedding these postmarket activities within formal governance structures, healthcare organizations can move from reactive responses to proactive, lifecycle based cybersecurity management.

Table 4. Governance controls mapping across standards and guidance

Control domain	AAMI	IEC 80001-1	IEC 81001-5-1	ISO/IEC 27001/27002	NIST CSF 2.0	Evidence artifact
Risk management	TIR57	Required	Lifecycle activity	Risk assessment	Govern	Risk register
Asset inventory	TIR57	Required	Required	Asset management	Identify	Device inventory
Network segmentation	Guidance	Required	Required	Network security	Protect	Network diagrams
Vulnerability management	TIR97	Required	Required	Vulnerability mgmt	Protect	Vulnerability reports
Incident response	TIR97	Required	Required	Incident mgmt	Respond	Incident playbooks
Assurance and audit	Guidance	Required	Required	ISMS audit	Measure	Audit reports

7. Integrated Framework: Linking Risk Modeling to Security Governance

7.1 From risk score to action: decision thresholds for clinical environments

An integrated framework must translate analytical risk scores into concrete, timely actions that are appropriate for safety critical clinical settings. In healthcare IoMT environments, risk scores are not ends in themselves but decision signals that trigger governance responses based on predefined thresholds.

Decision thresholds are established by combining residual risk scores with clinical criticality. High risk scores associated with life sustaining or therapy delivering devices trigger immediate governance attention, even when likelihood estimates are moderate. Conversely, lower criticality devices may tolerate higher technical risk scores if compensating controls are in place and patient safety is not directly affected (AAMI, 2016; IEC, 2021a).

10.48047/jocaaa.2023.31.04.109

Thresholds typically fall into three categories. **Immediate action thresholds** require rapid mitigation or containment measures, such as network isolation, access restriction, or enhanced monitoring. **Managed risk thresholds** allow for planned remediation through patch scheduling, compensating controls, or architectural changes. **Accepted risk thresholds** represent residual risks that are formally documented and approved by governance bodies due to clinical necessity, technical constraints, or proportionality considerations (ISO, 2019; NIST, 2024).

By defining these thresholds in advance, healthcare organizations reduce ambiguity during incidents and ensure that risk responses are consistent, auditable, and aligned with patient safety priorities.

7.2 Governance workflow: approval gates, clinical sign off, vendor coordination

The governance workflow operationalizes risk based decisions through structured approval and oversight mechanisms. Once risks are prioritized, they enter a workflow that involves multiple stakeholders and decision gates.

Approval gates ensure that proposed security actions are reviewed for feasibility, safety impact, and regulatory implications. Technical teams may recommend controls such as segmentation changes or access restrictions, but final approval often requires governance oversight to balance cybersecurity benefits against potential clinical disruption (IEC, 2021a; Richter C Ammenwerth, 2023).

Clinical sign off is a distinguishing feature of healthcare governance. Changes affecting device availability, configuration, or connectivity require validation by clinical leadership or biomedical engineering to confirm that patient care will not be compromised. This step embeds patient safety considerations directly into cybersecurity decision making rather than treating them as secondary concerns (ISO, 2019).

Vendor coordination is essential for many remediation actions. Manufacturers and service providers may need to approve configuration changes, provide patches, or support temporary compensating controls. Governance frameworks define escalation paths, communication protocols, and contractual obligations to ensure timely and secure collaboration during both routine risk management and incident response (AAMI, 2019; FDA, 2016).

This structured workflow transforms risk modeling outputs into coordinated action while maintaining traceability and accountability.

10.48047/jocaaa.2023.31.04.109

7.3 Metrics and reporting: KRIs, KPIs, and audit ready evidence

Metrics form the bridge between technical risk assessment and executive oversight. An integrated framework employs both **Key Risk Indicators** and **Key Performance Indicators** to monitor exposure and control effectiveness over time.

KRIs focus on the level and trajectory of cyber risk. Examples include the number of high criticality devices with unresolved vulnerabilities, proportion of clinical networks lacking segmentation, and trends in residual risk scores following control implementation. These indicators support forward looking governance by highlighting emerging risks before incidents occur (NIST, 2024).

KPIs measure the performance of governance and security processes. Examples include patch approval cycle times, percentage of vendors compliant with remote access policies, and completion rates for risk reviews. KPIs enable governance bodies to assess whether processes are functioning as intended and where improvement is needed (ISO/IEC, 2022).

Audit ready evidence underpins assurance and compliance. The integrated framework ensures that decisions, actions, and outcomes are documented through artifacts such as risk registers, approval records, monitoring logs, and incident reports. These artifacts support regulatory inspections and internal audits while reinforcing accountability across stakeholders (IMDRF, 2020).

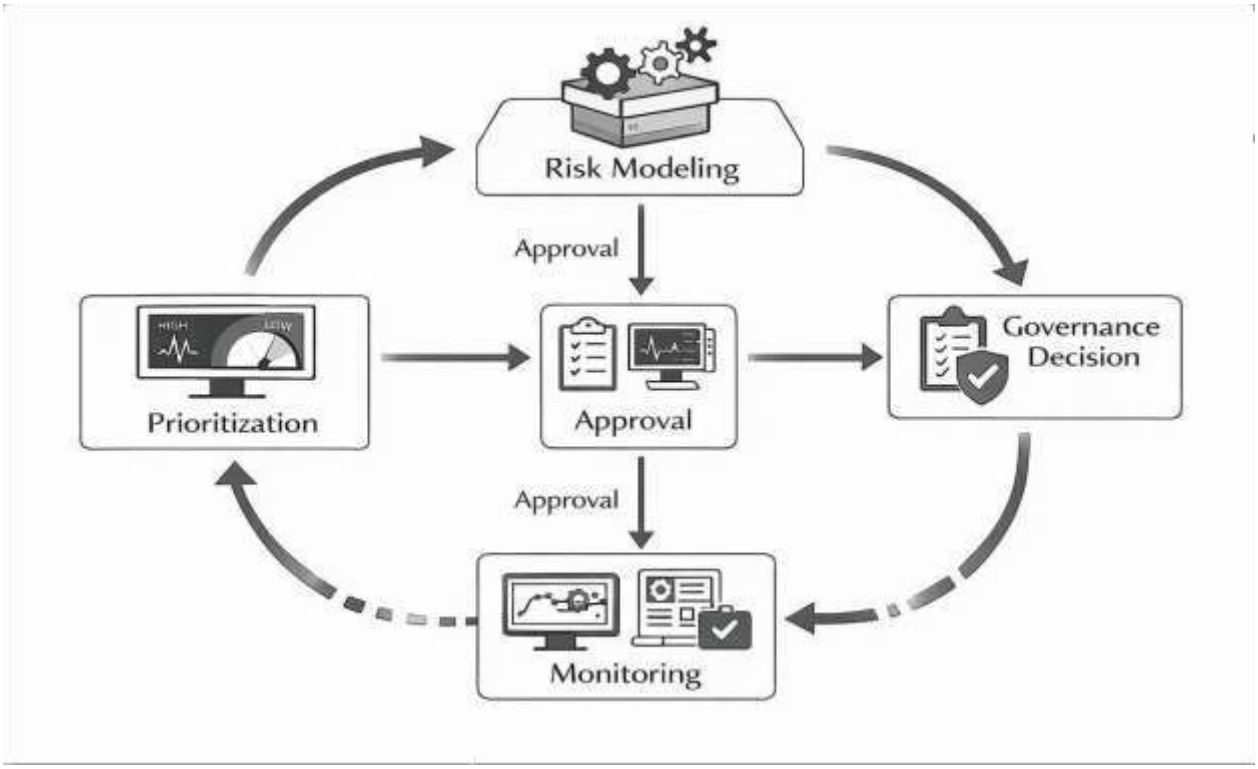
7.4 Incident response integration and resilience planning

Incident response and resilience planning are core components of integrated governance, particularly in the context of ransomware and widespread disruption scenarios. Risk modeling informs preparedness by identifying critical assets, dependencies, and likely attack paths that require protection during incidents.

In ransomware scenarios, governance decisions must be made rapidly under uncertainty. Predefined thresholds and workflows enable swift containment actions such as isolating affected network segments, suspending nonessential vendor access, and activating continuity of care plans. Risk modeling outputs guide prioritization, ensuring that resources are focused on preserving patient safety and essential services (Jiang et al., 2025; Shahzadi et al., 2025).

Resilience planning extends beyond immediate response to include recovery and adaptation. Post incident reviews feed lessons learned back into the risk model, updating assumptions about threat likelihood, exposure, and control effectiveness. This feedback loop supports continuous improvement and strengthens organizational resilience over time (NIST, 2024).

10.48047/jocaaa.2023.31.04.109



10.48047/jocaaa.2023.31.04.109

Figure 4. Integrated cyber risk and governance decision loop

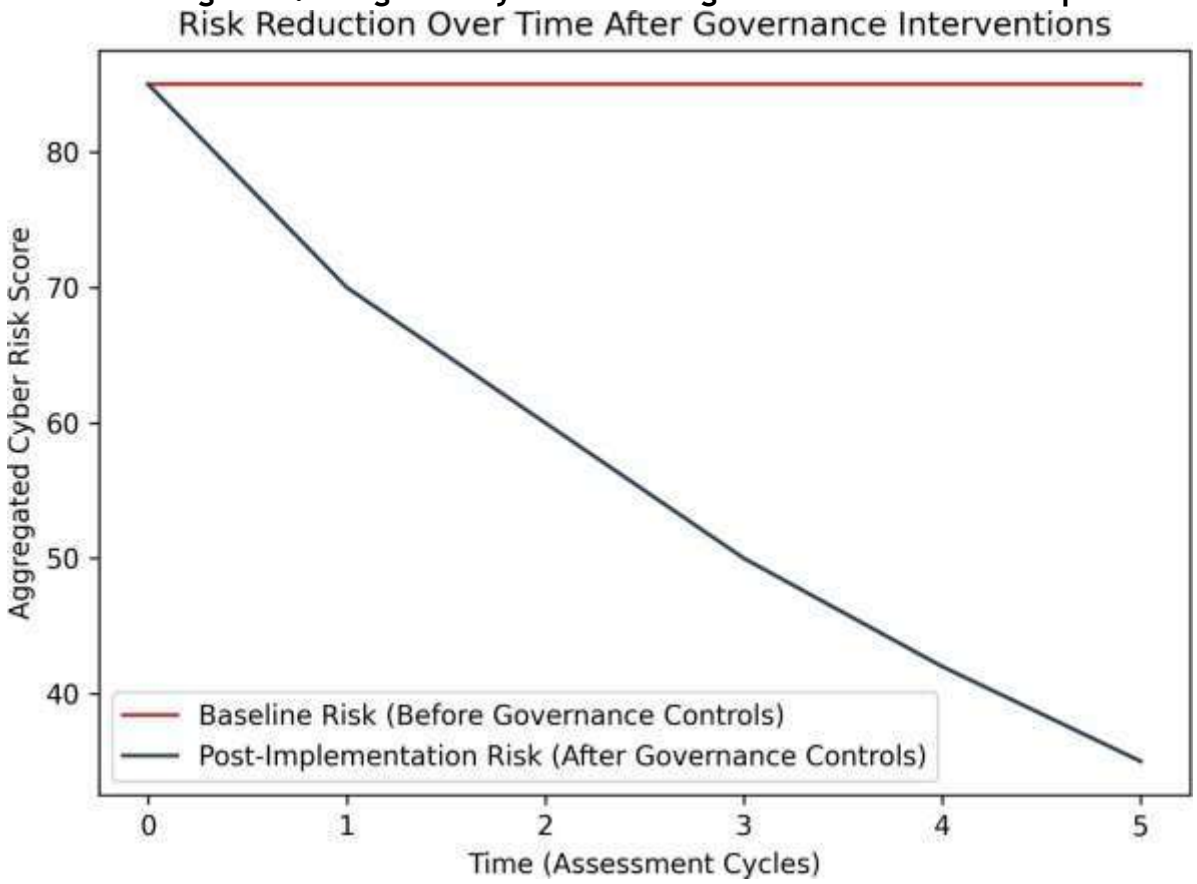


Figure 5. Risk reduction over time after governance interventions

8. Implementation Blueprint for Hospitals

8.1 Data collection plan

Effective implementation of the proposed framework begins with a structured and repeatable data collection plan. Accurate data is essential for risk modeling, governance decisions, and assurance activities.

- **Device inventory** is the primary dataset. Hospitals should maintain a centralized inventory that captures device identity, manufacturer, model, software or firmware version, clinical function, physical location, network interfaces, and ownership. Linking devices to clinical services enables criticality assessment and supports patient safety oriented prioritization (IEC 80001-1; AAMI TIR57).
- **Network segmentation maps** document how devices connect to clinical VLANs, enterprise IT networks, middleware platforms, and external services. These maps identify trust boundaries and shared dependencies that influence exposure

10.48047/jocaaa.2023.31.04.109

and propagation risk. Maintaining current segmentation documentation is a prerequisite for both risk analysis and incident response (NIST CSF 2.0).

- **Vulnerability sources** include manufacturer advisories, coordinated vulnerability disclosure feeds, national vulnerability databases, and sector specific threat intelligence. Hospitals should define processes for consolidating and validating vulnerability information to ensure relevance to deployed devices (AAMI TIR97; ISO/IEC 29147).
- **Device lifecycle information** captures procurement date, expected service life, support status, and end of life timelines. Lifecycle data informs compensating control decisions for legacy devices that cannot be patched or upgraded and supports long term risk planning (ISO 14971; IEC 81001-5-1).

8.2 Practical controls for medical device environments

Implementation emphasizes practical controls that reduce risk while respecting clinical and safety constraints.

- **Network segmentation** remains the most effective control for limiting lateral movement. Clinical device networks should be isolated from enterprise IT systems with controlled gateways and strict traffic rules. Where full isolation is not feasible, micro segmentation and application level controls provide incremental protection (IEC 62443; NIST CSF 2.0).
- **Access control** focuses on enforcing least privilege for users, service accounts, and vendor connections. Strong authentication, role based access, and time limited access approvals reduce the likelihood of credential misuse and insider related incidents (ISO/IEC 27002).
- **Logging and monitoring** provide visibility into device and network activity. While endpoint agents may not be feasible on many devices, network based monitoring, anomaly detection, and centralized log aggregation support early detection without interfering with device operation (AAMI TIR97; NIST CSF 2.0).
- **Vendor remote access hardening** addresses a common source of exposure. Controls include dedicated access zones, multi factor authentication, session recording, and contractual enforcement of security requirements. These measures reduce supply chain related risk while preserving operational support capabilities (FDA postmarket guidance; IMDRF).

10.48047/jocaaa.2023.31.04.109

8.3 Procurement and lifecycle governance

Procurement represents a critical leverage point for improving medical device security. Security requirements should be embedded into purchasing contracts and vendor evaluations rather than treated as post deployment add ons.

Contracts should require manufacturers to document secure development practices, vulnerability disclosure processes, update mechanisms, and support timelines. Hospitals should also specify expectations for remote access security, logging capabilities, and incident response cooperation (AAMI TIR57; IEC 81001-5-1).

Lifecycle governance extends these requirements into operation and decommissioning. Devices approaching end of support should be flagged for replacement or enhanced compensating controls. Documented lifecycle decisions support governance accountability and regulatory assurance (ISO 14971).

8.4 Deployment roadmap

Implementation is most effective when phased to balance urgency, resource constraints, and organizational change.

- **Short term actions (0 to G0 days)** focus on visibility and risk reduction foundations, including inventory completion, segmentation review, and vendor access controls.
- **Medium term actions (3 to 12 months)** emphasize governance formalization, integration of risk modeling into decision making, and expansion of monitoring and assurance capabilities.
- **Long term actions (12 months and beyond)** address structural improvements such as procurement reform, device modernization, and continuous improvement of risk and governance processes.

Table 5. Phased implementation roadmap with deliverables

Phase	Activities	Owners	Tools or data	Outputs	Success indicators
Short term	Complete device inventory, review segmentation, restrict vendor access	IT, clinical engineering	Asset tools, network maps	Updated inventory, access controls	Inventory completeness, reduced exposure
Medium term	Integrate risk modeling, formalize governance workflows, expand monitoring	Security, governance committees	Risk model, SIEM	Risk dashboards, policies	Timely risk decisions, audit readiness
Long term	Procurement reform, legacy device	Executive leadership	Contracts, lifecycle plans	Secure procurement, resilience	Sustained risk reduction

10.48047/jocaaa.2023.31.04.109

	replacement, continuous improvement				

G. Evaluation Approach and Case Illustration

G.1 Evaluation criteria

The proposed framework is evaluated against four criteria to ensure practical and scientific value.

- **Feasibility** assesses whether required data, tools, and skills are realistically available in hospital environments. The framework favors commonly available datasets and incremental implementation to reduce barriers to adoption (Richter and Ammenwerth).
- **Interpretability** examines whether outputs are understandable to technical, clinical, and executive stakeholders. Transparent scoring and clear visualizations support shared understanding and informed decision making (NIST CSF 2.0).
- **Reproducibility** evaluates whether the framework can be applied consistently across departments or institutions using the same inputs and assumptions. Documented methods and standardized artifacts support repeatability.
- **Audit readiness** considers the ability to produce evidence for regulatory and internal review. Traceable decisions, documented approvals, and preserved metrics enable assurance and compliance activities (ISO/IEC 27001).

G.2 Example scenario: ransomware propagation

A representative scenario involves a ransomware campaign entering a hospital through a compromised user account on the enterprise IT network. The attacker exploits weak segmentation to pivot into a clinical subnet hosting infusion pumps and patient monitors. Middleware services shared across departments facilitate further spread, disrupting device availability and clinical workflows.

Applying the proposed framework, risk modeling highlights the high criticality of affected devices and the weak trust boundary between networks. Governance thresholds trigger immediate containment actions, including subnet isolation and suspension of nonessential vendor access, while clinical leadership approves temporary workflow adaptations.

G.3 Model output interpretation

Model outputs guide prioritization under constrained budgets and operational pressure. Controls that reduce risk across multiple high criticality devices, such as segmentation

10.48047/jocaaa.2023.31.04.109

and vendor access hardening, are addressed first. Investments requiring longer timelines or affecting lower criticality assets may be deferred with documented risk acceptance.

Funding decisions prioritize actions with measurable impact on residual risk and patient safety. Transparent interpretation of outputs supports defensible governance decisions and aligns cybersecurity investment with clinical value.

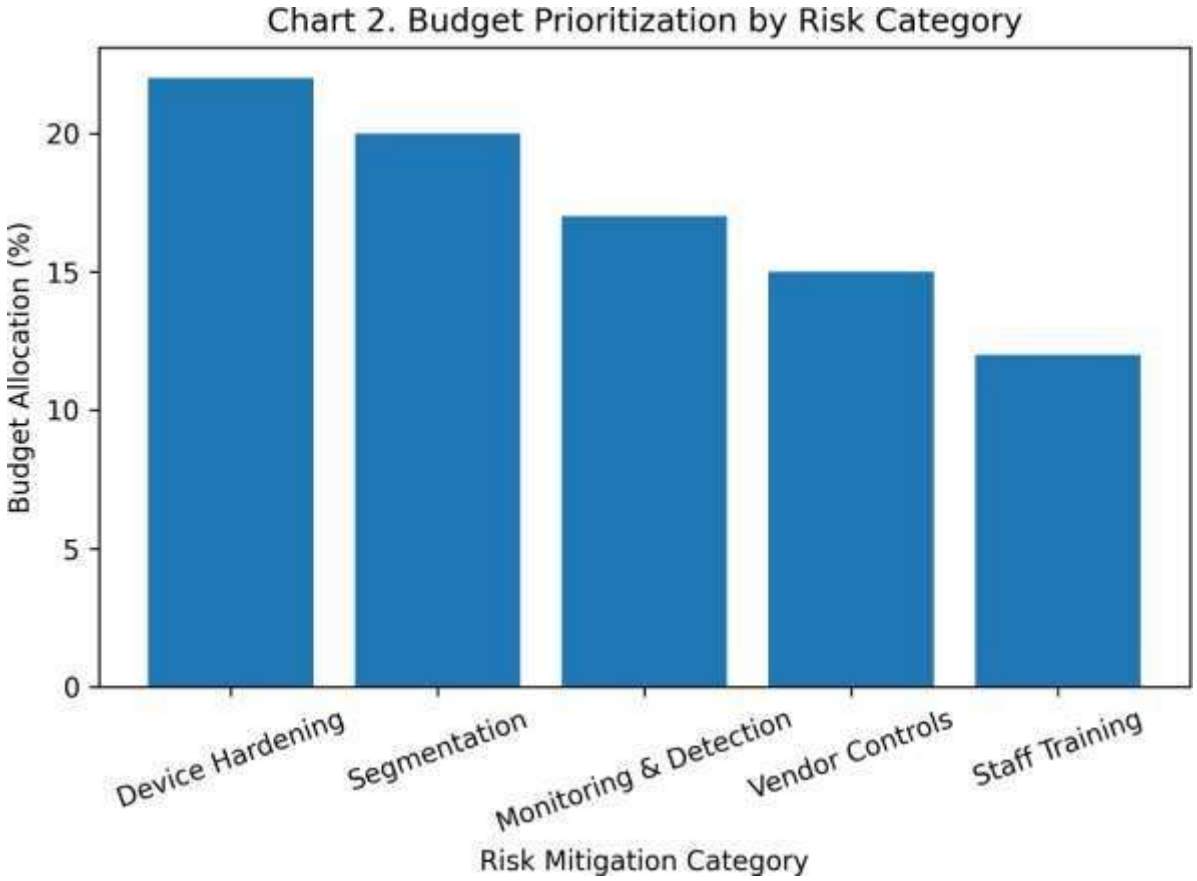


Figure 6. Budget prioritization by risk category

10. Discussion

Advancing prior IoMT security approaches

The framework proposed in this study advances prior approaches to IoMT security by moving beyond device centric or compliance driven assessments toward an integrated, governance aware risk modeling paradigm. Earlier work in medical device cybersecurity has often focused on identifying vulnerabilities, cataloging threats, or recommending technical safeguards in isolation. While these efforts have improved awareness, they have provided limited support for prioritization and executive decision making in complex clinical environments (Williams C Woodward, 2015; Rasool et al., 2022).

10.48047/jocaaa.2023.31.04.109

In contrast, the proposed framework explicitly incorporates clinical criticality, network dependencies, and propagation pathways into cyber risk modeling. By integrating these dimensions, the framework enables healthcare organizations to distinguish between technically severe vulnerabilities and those that pose the greatest patient safety and operational risk. This shift aligns cybersecurity investment with clinical value, addressing a key limitation of prior IoMT security approaches that treated medical devices as conventional IT endpoints.

Furthermore, the integration of risk modeling with formal governance workflows represents a substantive contribution. Rather than producing static risk reports, the framework embeds analytical outputs into approval processes, policy enforcement, and continuous monitoring. This linkage transforms risk assessment into a living decision support function that evolves alongside clinical operations and threat conditions (NIST CSF 2.0; AAMI TIR57).

Policy implications and regulatory alignment

The findings of this study have important implications for healthcare policy and regulation. Regulators increasingly emphasize cybersecurity as a component of medical device safety and effectiveness, yet healthcare organizations often struggle to operationalize regulatory guidance across heterogeneous device ecosystems. The proposed framework offers a practical mechanism for translating regulatory expectations into measurable, auditable practices.

By aligning risk modeling outputs with established standards such as ISO 14971, IEC 80001- 1, IEC 81001-5-1, ISO/IEC 27001 and 27002, and the NIST Cybersecurity Framework, the framework supports harmonization across regulatory regimes. This alignment enables healthcare organizations to demonstrate due diligence and risk based decision making without duplicating effort across compliance silos.

At a policy level, the framework highlights the need for clearer guidance on shared responsibility between hospitals, manufacturers, and service providers. Risk propagation across trust boundaries underscores that effective medical device cybersecurity cannot be achieved through isolated organizational action. Policymakers may therefore consider encouraging greater transparency, standardized security disclosures, and collaborative governance mechanisms across the medical device supply chain.

Adoption barriers and practical challenges

Despite its benefits, adoption of the proposed framework faces several practical barriers. Legacy medical devices represent a persistent challenge, as many operate on

10.48047/jocaaa.2023.31.04.109

unsupported platforms and lack modern security capabilities. Replacing or upgrading such devices may require significant capital investment and clinical disruption, limiting the pace of improvement.

Vendor constraints also affect implementation. Hospitals often depend on manufacturers and service providers for updates, configuration changes, and remote access. Inconsistent vendor security practices and limited contractual leverage can impede timely risk mitigation, particularly in postmarket contexts.

Cost and staffing constraints further shape adoption. Implementing segmentation, monitoring, and governance processes requires financial resources and skilled personnel that may be scarce, especially in smaller or resource constrained healthcare organizations. Without executive support and clear prioritization, cybersecurity initiatives may compete unsuccessfully with other operational demands.

Addressing these barriers requires phased implementation, risk based prioritization, and sustained leadership engagement, as reflected in the implementation blueprint presented in this study.

Ethical and safety considerations

Cybersecurity governance for medical devices raises ethical considerations that extend beyond technical risk management. Decisions to isolate devices, delay updates, or accept residual risk may have direct implications for patient care. Ethical governance therefore requires transparency, clinical involvement, and documentation of trade offs between security and safety.

The framework emphasizes ethical responsibility by embedding clinical sign off and patient safety considerations into decision making processes. By making risk assumptions explicit and auditable, the framework supports accountable governance and helps avoid implicit risk shifting to patients or frontline clinicians.

11. Limitations and Future Research

Study limitations

This study is subject to several limitations. The effectiveness of the proposed framework depends on the availability and quality of input data, particularly device inventories and network topology information. Incomplete or inaccurate data may lead to underestimation or misprioritization of risk, a challenge that remains prevalent in many healthcare organizations.

10.48047/jocaaa.2023.31.04.109

Generalizability is another limitation. While the framework is designed to be adaptable, healthcare institutions vary widely in size, technical maturity, regulatory context, and resource availability. Implementation outcomes may therefore differ across regions and organizational types, warranting caution in extrapolating results without contextual adaptation.

Future research directions

Future research may extend this work in several directions. One promising avenue is the use of **digital twins** to simulate hospital cyber risk, enabling dynamic analysis of attack scenarios and control effectiveness without disrupting live systems. Digital twin models could enhance propagation analysis and resilience planning.

Machine learning assisted risk prediction represents another area for exploration. By analyzing historical incidents, vulnerability trends, and network data, ML models could support more adaptive likelihood estimation and early warning capabilities, complementing the structured approach presented here.

Finally, automated evidence generation for governance and compliance remains an open research area. Integrating risk modeling outputs with audit and reporting systems could reduce administrative burden and improve the timeliness of assurance activities, strengthening the link between cybersecurity practice and regulatory oversight.

12. Conclusion

This study presents an integrated framework for cyber risk modeling and security governance tailored to networked medical devices in critical healthcare infrastructure. By combining clinical criticality aware risk modeling with structured governance processes, the framework addresses longstanding gaps between technical assessment and organizational decision making.

For hospital executives, the framework provides a defensible basis for prioritizing cybersecurity investment in alignment with patient safety and regulatory expectations. For clinical engineering teams, it offers a structured method for managing device risk across complex lifecycles. For security and governance stakeholders, it delivers measurable, auditable insights that support continuous improvement.

Healthcare organizations should adopt risk modeling approaches that explicitly incorporate clinical context, device dependencies, and governance integration. Implementation should be phased, measurable, and aligned with established standards and guidance. By doing so, hospitals can move beyond reactive cybersecurity measures toward resilient, patient centered security governance that evolves alongside emerging threats and technologies.

10.48047/jocaaa.2023.31.04.109

References

1. Association for the Advancement of Medical Instrumentation. (2016, reaffirmed 2023). AAMI TIR57: Principles for medical device security: Risk management.
2. Association for the Advancement of Medical Instrumentation. (2019). AAMI TIR97: Principles for medical device security: Postmarket risk management for device manufacturers.
3. Camara, C., Peris-Lopez, P., C Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of biomedical informatics, 55, 272-289.
4. Center for Internet Security. (2021). CIS Critical Security Controls v8. https://www.cisecurity.org/insights/white-papers/cis-controls-v8
5. Clark, S. S., C Fu, K. (2011, October). Recent results in computer security for medical devices. In International Conference on Wireless Mobile Communication and Healthcare (pp. 111-118). Berlin, Heidelberg: Springer Berlin Heidelberg.
6. Cybersecurity in medical devices: quality system considerations and content of premarket submissions : guidance for industry and Food and Drug Administration staff - Digital Collections - National Library of Medicine. (2023). Nih.gov. https://collections.nlm.nih.gov/catalog/nlm:nlmuid-9918716786306676-pdf
7. Denning, T., Fu, K., C Kohno, T. (2008, July). Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In HotSec.
8. Fagan, M., Megas, K., Scarfone, K., C Smith, M.(2020). Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (No. NIST Internal or Interagency Report (NISTIR) 8259 (Withdrawn)). National Institute of Standards and Technology.
9. Prasanth Alluri. (2022, December). Data-Driven and Artificial IntelligenceEnabled Frameworks for Sustainable Energy, Rural Transportation Networks, and Water Resource Management in Developing Economies. (IJCNIS) : https://www.ijcnis.org/index.php/ijcnis/article/view/8807
10. Farlow, C. S., Jump, M. L., Seeberger, M. S., C Fitzgerald, B. J. (2023). Ansi/aami sw96: Raising the bar for medical device security risk management. Biomedical Instrumentation C Technology, 57(2), 40-43.
11. Force, J. T. (2017). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (discussion draft) (No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft)). National Institute of Standards and Technology.

10.48047/jocaaa.2023.31.04.109

12. Force, J. T. (2020). Security and privacy controls for information systems and organizations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Withdrawn)). National Institute of Standards and Technology.
13. Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., C Maisel, W. H. (2008). Security and privacy for implantable medical devices. IEEE pervasive computing, 7(1), 30-39.
14. Health Sector Coordinating Council. (2018). Health Industry Cybersecurity Practices (HICP): Managing threats and protecting patients. https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf
15. International Electrotechnical Commission. (2013). IEC 62443-3-3:2013: Security for industrial automation and control systems: System security requirements and security levels. https://webstore.iec.ch/en/publication/7033
16. International Electrotechnical Commission. (2018). IEC 62443-4-1:2018: Security for industrial automation and control systems: Secure product development lifecycle requirements. https://webstore.iec.ch/en/publication/33615
17. International Electrotechnical Commission. (2021). IEC 80001-1:2021: Application of risk management for IT networks incorporating medical devices: Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software. https://www.iso.org/obp/ui/en/#iso:std:iec:80001:-1:ed-2:v1:en,fr
18. International Electrotechnical Commission. (2021). IEC 81001-5-1:2021: Health software and health IT systems safety, effectiveness and security: Part 5-1: Security: Activities in the product life cycle. https://webstore.iec.ch/en/publication/63293
19. International Organization for Standardization. (2018). ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:29147:ed-2:v1:en
20. International Organization for Standardization. (2019). ISO 14971:2019: Medical devices: Application of risk management to medical devices. https://www.iso.org/obp/ui/#iso:std:iso:14971:ed-3:v1:en
21. International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection: Information security management systems: Requirements. https://www.iso.org/obp/ui/en/#iso:std:iso- iec:27001:ed-3:v1:en
22. International Organization for Standardization. (2022). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection: Information security controls. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en

10.48047/jocaaa.2023.31.04.109

23. International Organization for Standardization. (2025). ISO 27799:2025: Health informatics: Information security management in health using ISO/IEC 27002. https://www.iso.org/obp/ui/en/#iso:std:iso:27799:ed-3:v1:en
24. Jiang, J. X., Ross, J. S., C Bai, G. (2025). Ransomware Attacks and Data Breaches in US Health Care Systems. JAMA Network Open, 8(5), e2510180-e2510180.
25. Prasanth Alluri. (2022). Behavior-Based Cyber Defense Architectures for Enhancing the Resilience of Defense and National Critical Infrastructure. Journal of Electrical Systems (JES) : https://journal.esrgroups.org/jes/article/view/9428
26. Jump, M. (2019). Setting Standards: AAMI TIR97: A Vital Resource in the Postmarket Management of Medical Device Security. Biomedical Instrumentation C Technology, 53(6), 462-464.
27. Koo, K., Moon, D., Huh, J. H., Jung, S. H., C Lee, H. (2022). Attack graph generation with machine learning for network security. Electronics, 11(9), 1332.
28. Landscape, E. T. (2021). European Union Agency for Cybersecurity. URL: https://www. enisa. europa. eu/topics/cyber-threats/threats-and-trends.
29. Lee, A., Gourisetti, S. N. G., Sebastian-Cardenas, D. J., Lambert, K., Navarro, V., Pasetti, M., ... C Saha, S. S. (2023). Assessment of the distributed ledger technology for energy sector industrial and operational applications using the mitre attCck® ics matrix. IEEE Access, 11, 69854-69883.
30. Li, S., Surineni, K., C Prabhakaran, N. (2025). Cyber-Attacks on Hospital Systems: A Narrative Review. The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice.
31. Maisel, W. H., Moynahan, M., Zuckerman, B. D., Gross, T. P., Tovar, O. H., Tillman, D.
B., C Schultz, D. B. (2006). Pacemaker and ICDgenerator malfunctions: analysis of Food and Drug Administration annual reports. Jama, 295(16), 1901-1906.
32. Martínez Montoya, M. (2022). Improvement of HL7 FHIR security and privacy with the use of other existing standards (Master's thesis, Universitat Politècnica de Catalunya).
33. National Institute of Standards and Technology (US), C National Institute of Standards and Technology (US). (2024). NIST Cybersecurity Framework 2.0: Quick- start Guide for Creating and Using Organizational Profiles. US Department of Commerce, National Institute of Standards and Technology.
34. Prasanth Alluri. (2022). Integrating Artificial Intelligence for Climate- Resilient Energy Planning, Rural Infrastructure Development, and Water Conservation in

10.48047/jocaaa.2023.31.04.109

Underdeveloped Regions. Computer Fraud and Security : https://computerfraudsecurity.com/index.php/journal/article/view/954

35. Nithyavani, G., C Raja, G. N. (2025). A comprehensive survey on security and privacy challenges in internet of medical things applications: Deep learning and machine learning solutions, obstacles, and future directions. IEEE Access.
36. Ostermann, M., Mathias, R., Jahed, F., Parker, M. B., Hudson, F. D., Harding, W. C., ...
C Freyer, O. (2025). Cybersecurity requirements for medical devices in the EU and US-A comparison and gap analysis of the MDCG 2019-16 and FDA premarket cybersecurity guidance. Computational and Structural Biotechnology Journal.
37. Ozcelik, M. M., Kok, I., C Ozdemir, S. (2025). A Survey on Internet of Medical Things
(IoMT): Enabling Technologies, Security and Explainability Issues, Challenges, and Future Directions. Expert Systems, 42(5), e70010.
38. Palma, A., C Bonomi, S. (2025). Behind the scenes of attack graphs: Vulnerable network generator for in-depth experimental evaluation of attack graph scalability. Computers C Security, 104576.
39. Park, C. S. (2014). Security mechanism based on hospital authentication server for secure application of implantable medical devices. BioMed research international, 2014(1), 543051.

40. Principles and Practices for Medical Device Cybersecurity. (2020). International Medical Device Regulators Forum. https://www.imdrf.org/documents/principles- and-practices-medical-device-cybersecurity
41. Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., C Qadir, J. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. Journal of Network and Computer Applications, 201, 103332.
42. Richter, S., C Ammenwerth, E. (2023). IT risk management for medical devices in hospital IT networks: a catalogue of measures and indicators. BMJ Health C Care Informatics, 30(1), e100639.
43. Ross, R. S. (2012). Guide for conducting risk assessments.
44. Sametinger, J., Rozenblit, J., Lysecky, R., C Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74-82.
45. Shahzadi, A., Ishaq, K., Dogar, A. B., Khan, J. A., Mylonas, A., Nawaz, N. A., ... C Khan, F. A. (2025). Safeguarding the healthcare sector from ransomware attacks:

10.48047/jocaaa.2023.31.04.109

insights from a literature review. PeerJ Computer Science, 11, e3073.

46. Stouffer, K., Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., ... C Thompson, M. (2023). Guide to operational technology (ot) security.
47. The Open Group. (2013). Risk analysis (O-RA) standard (Open FAIR), Version 2.0.
48. The Open Group. (2013). Risk taxonomy (O-RT) standard (Open FAIR), Version 2.0.
49. U.S. Food and Drug Administration. (2016). Postmarket management of cybersecurity in medical devices (Guidance for Industry and Food and Drug Administration Staff). https://www.fda.gov/files/medical%20devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf
50. van Vroonhoven, J. (2020). Risk management for medical devices and the new BS EN ISO 14971. ASM International.
51. Weininger, S., Jaffe, M. B., C Goldman, J. M. (2017). The need to apply medical device informatics in developing standards for safe interoperable medical systems. Anesthesia C Analgesia, 124(1), 127-135.
52. Williams, P. A., C Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices:

Evidence and Research, 305-316.