Bachelor's thesis

Information and Communications Technology | Data Networks and Cybersecurity

2025 | 90

Fatema Sahiwala

An Integrated Risk Management Approach Using the NIST CSF-2.0, NIST 800-82, and IEC 62443 Frameworks

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology | Data Networks and Cybersecurity

2025 | 67 Pages

Fatema Sahiwala

An Integrated Risk Management Approach Using the NIST CSF-2.0, NIST 800-82, and IEC 62443 Frameworks

Genomic diagnostic laboratories increasingly depend on IoT and OT systems, creating cybersecurity challenges that traditional approaches cannot adequately address. This study introduces and validates an integrated risk assessment methodology combining NIST Cybersecurity Framework 2.0, NIST SP 800-82, and IEC 62443 to establish a comprehensive security posture for specialized healthcare environments.

A case study at ACME Inc.’s genomic diagnostic laboratory uncovered significant vulnerabilities in vulnerability management, access control, and business continuity. The methodology involved documentation review, interviews, and control assessments. The assessment revealed inconsistent patching, incomplete asset inventories, and insufficient continuous monitoring, exposing the lab to considerable cyber risks. Applying this integrated methodology and mapping over 300 security controls established a quantitative measure of the laboratory’s cybersecurity maturity. This data-driven approach identified critical vulnerabilities and informed a structured, multi-phase remediation plan. This thesis provides a roadmap for a proactive cybersecurity strategy, prioritizing actions for immediate and long-term risk mitigation.

Keywords: Cybersecurity, risk assessment, NIST, CSF, IEC, qualitative.

Contents

Appendices

Appendix 1. Interview Questions and Answers

Figures

Tables

List of abbreviations (or) symbols

ABA	Applied Behavioral Analysis
BC/DR	Business Continuity/Disaster Recovery
CMS	Centers for Medicare & Medicaid Services
CSF	Cybersecurity Framework
DMZ	Demilitarized Zone
EDR	Endpoint Detection and Response
ELK	Elasticsearch, Logstash, and Kibana
EPSDT	Early and Periodic Screening, Diagnostic, and Treatment
GRC	Governance, Risk, and Compliance
HCBS	Home- and Community-Based Services
HIPAA	Health Insurance Portability and Accountability Act
HRSA	Health Resources and Services Administration
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IR	Incident Response
IT	Information Technology
KPI	Key Performance Indicator
MCO	Managed Care Organization
NIST	National Institute of Standards and Technology
OT	Operational Technology
PAR	Prior Authorization Review
PDN	Private Duty Nurse

PE	Physical and Environmental (NIST control family)
PIRL	Preliminary Information Request List
PLC	Programmable Logic Controller
RBAC	Role-Based Access Control
RFID	Radio-Frequency Identification
RN	Registered Nurse
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SC	System and Communications (NIST control family)
SIEM	Security Information and Event Management
SL	Security Level (IEC 62443)
SLA	Service-Level Agreement
SOC	Security Operations Center
SoD	Separation of Duties
SOP	Standard Operating Procedure
SP	Special Publication
SR	Security Requirement (IEC 62443)
UM	Utilization Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XLS	Excel Spreadsheet

1 Introduction

According to Ansari, et al. (2024), the Internet of Things (IoT) is a network that performs multiple tasks including; monitoring, sensing and connecting with smart devices to exchange collected data using local networks and internet enabled networks. It offers remote control, real-time telemetry, and automation to the users. However, Kortemaa, (2025) stated that operational technology (OT) consists of systems that join directly with the hardware and software to monitor or control the physical processes. A study conducted by Weitoish (2025) examined that programmable logic controllers are employed in the laboratories to ensure appropriate medical diagnostics. In addition, it examined robotics analyzers and environmental control systems to meet the needs of medical diagnostics. Sustainability is achieved in healthcare diagnostic labs through integration of IoT and OT devices. This study explores how integrating NIST CSF 2.0, NIST SP 800-82, and IEC 62443 enables comprehensive cybersecurity risk assessment in hybrid IoT/OT laboratory environments.

1.1 Background of the Problem

In the medical industry, rapid adoption of healthcare technologies has brought about a convergence of Information Technology (IT), OT, and IoT devices in critical healthcare environments. Although this integration enhances diagnostic capabilities and operational efficiency, it also introduces cybersecurity vulnerabilities that many existing frameworks alone are unable to fully address (Carello, 2025). Diagnostic laboratories, especially those specializing in genomic testing and precision medicine, depend heavily on interconnected systems that range from cloud-connected environmental sensors to robotic analyzers and specialized diagnostic equipment. Such hybrid infrastructures significantly increase the attack surface. A single vulnerability may compromise multiple interconnected systems, putting patient data at risk, disrupting diagnostic services, and threatening both patient privacy and safety (Riurean, et al., 2025).

According to Bucelli et al. (2021), healthcare institutions are prime cyber targets because they store sensitive patient health records, and any service interruption can directly affect patient survival. Paul (2025) stated that nearly 89% of healthcare organizations said they suffer almost one cyberattack per week, and over the past year the average number of attacks was 43. Large numbers of healthcare IoT or Internet of Medical Things (IoMT) devices are frequently exposed due to insecure configurations such as default credentials, insufficient update mechanisms, and unnecessary or improperly secured network connectivity. Historically, IT and OT systems in healthcare have been managed in separate silos: each domain developed its own risk tolerance, operational priorities, and security posture. As these domains converge to support automated diagnostics, continuous monitoring, or cloud-enabled services, the complexity of harmonizing security controls becomes much more difficult (Rahman et al., 2024).

In healthcare settings, these governance expectations are especially relevant because labs and medical facilities often rely heavily on third-party vendors, have legacy devices with limited security support, and must deal with strict regulatory or safety constraints. Devices may run continuously for patient safety; downtime for patching or reconfiguration can directly impact diagnostics or treatment (Bucelli et al 2021). W Such hybrid infrastructures significantly increase the attack surface: a single vulnerability may compromise multiple interconnected systems, putting patient data at risk, disrupting diagnostic services, and threatening both patient privacy and safety (Riurean et al., 2025). Hile the Govern function pushes for stronger governance, vendor oversight, and policy alignment. Healthcare organizations often struggle to implement multiple, overlapping frameworks while keeping core diagnostic and operational services available. Balancing security improvements with the need for constant availability and safety adds complexity (Rahman et al., 2024).

Another major issue is that implementing these governance changes demands certain capacities: staff expertise, resources to monitor supply chains, risk management skills, clarity over roles and responsibility (Progoulakis, et al.,

2024). In many hospitals or labs, people specialize in either IT, OT, or medical devices/IoT but rarely have deep expertise spanning all three domains. This creates gaps in implementation of governance, in enforcing vendor contracts, in maintaining consistent policies, and in understanding how frameworks and regulatory obligations overlap or conflict (Dohin, et al., 2025). Many healthcare organizations lag in implementing CSF 2.0's Govern function, with policies existing formally but lacking consistent oversight and resource allocation (Hossain et al., 2024).

1.2 Problem Statement

In many healthcare diagnostic laboratories that use hybrid IoT/OT systems, there is a serious gap: there is no fully integrated, usable methodology for applying cybersecurity frameworks such as NIST CSF 2.0, NIST SP 800-82, and IEC 62443. Although each framework offers strong guidance CSF 2.0 for enterprise-level risk governance and IT/IoT behavior, SP 800-82 for operational technology (OT) with industrial control systems, and IEC 62443 for industrial automation and control systems security, these are commonly implemented in isolation or only partially. As a result, lab infrastructures with a mixture of traditional IT, OT, medical devices, and IoT sensors often end up with overlapping controls, neglected vulnerabilities, unclear roles, and redundant or conflicting procedures (Dohin, et al., 2025).

When these frameworks are applied for piecemeal, certain assets—especially legacy OT/IoT devices are frequently excluded or improperly protected because they do not easily satisfy standard control requirements. For example, many IoT/OT devices lack robust authentication, patching is delayed or impossible, and continuous monitoring is weak or non-existent (Hossain, et al., 2024). In addition, organizational responsibility is often ambiguous: clinical engineering, IT security, OT operations, and lab management may believe that certain controls lie outside their domain. This leads to gaps not solely in technical coverage, but in accountability, incident response, regulatory compliance, and ultimately in risk management (Metin, Özhan, and Wynn, 2024).

These shortcomings pose serious risks: diagnostic operations may be interrupted by ransomware or OT failures; patient data may be compromised; regulatory violations may trigger legal consequences; and institutional reputation may suffer irreparably. Moreover, the increasingly pressing threat landscape driven by IoT expansion, IT/OT convergence, supply-chain risks, and stricter regulatory expectations means that nominal or fragmented compliance is no longer sufficient to assure security or resilience (Malatji, 2023).

What is lacking, therefore, is a unified framework or methodology that integrates all three standards (CSF 2.0, SP 800-82, IEC 62443) specifically for the healthcare diagnostic lab environment. This includes mapping overlapping controls; defining coverage for all device types including legacy and IoT/OT systems; clarifying team responsibilities; ensuring regulatory alignment; and balancing safety with security. Without such an integrated methodology, healthcare labs remain vulnerable to disruptions, breaches, and non-compliance, and may incur severe operational, legal, and reputational costs (Halawi Ghoson, et al., 2025).

1.3 Purpose of the Study

The purpose of this qualitative case study is to develop and validate an integrated cybersecurity risk assessment methodology that combines NIST CSF 2.0, NIST SP 800-82, and IEC 62443 to secure hybrid IoT/OT healthcare diagnostic laboratory environments. This study aims to produce a unified and operationally realistic approach that overcomes the fragmentation currently observed in security framework implementation. The goal is to offer comprehensive protection for interconnected diagnostic infrastructure while respecting diagnostic throughput, device safety, and regulatory compliance.

The study will proceed through multiple phases including documentation review, semi-structured interviews, field observations, and control assessments. Key constructs to be investigated include vulnerability management, access control, business continuity, monitoring systems, governance structures, network

architecture, and operational practices tied to device maintenance and vendor support. The study population comprises technical, operational, and management personnel within the diagnostic laboratory, and the facility will be referred to pseudonymously as “ACME Inc.” to preserve confidentiality.

1.4 Significance of the Study

This research is significant for several reasons. First, it is relatively novel in seeking to harmonize three major cybersecurity frameworks NIST CSF 2.0, NIST SP 800-82, and IEC 62443 in a single healthcare diagnostic laboratory setting. Doing so promises to yield methods and tools that are more coherent and interoperable than implementing frameworks in isolation. For practitioners, the study may deliver tools such as a remediation roadmap, metrics for maturity, and control-mapping matrices, which should improve efficiency in resource allocation across IT, OT, and IoT components (Halawi Ghoson, et al., 2025). Laboratory managers stand to gain substantially from recommendations that strengthen security posture without disrupting critical diagnostic operations. By implementing integrated guidance, they can safeguard lab workflows against cyber threats while ensuring minimal interference with testing, calibration, and data collection. From an academic perspective, this study has the potential to uncover multiple frameworks NIST CSF 2.0, NIST SP 800-82, and IEC 62443 reinforce each other, and where they conflict when applied in real-world healthcare/IoT/OT contexts. Such empirical insights will help determine which specific controls deliver the greatest effectiveness, under what conditions, and with what trade-offs (Abergos, and Medjek, 2024). More broadly, this research may shift organizational culture from one reaction responding to breaches after they occur to one anchored in foresight and resilience, with emphasis on prevention, governance, and continuous risk management.

1.5 Aims and Objectives

The study aims to develop and validate an integrated cybersecurity methodology that harmonizes the requirements of NIST CSF 2.0, NIST SP 800-82, and IEC 62443 for hybrid IoT/OT healthcare diagnostic laboratories. It systematically maps framework requirements to lab operations, assesses current controls in IT/OT/IoT environments, evaluates risk mitigation effectiveness, and proposes a prioritized remediation roadmap aligned with regulatory obligations.

The objectives of the study are as follows;

- To systematically map and compare the requirements of NIST CSF 2.0, NIST SP 800-82, and IEC 62443 in the context of genomic diagnostic laboratories, in order to identify overlaps, inconsistencies, and gaps in coverage across IoT, OT, and IT domains.
- To evaluate the laboratory's current cybersecurity controls technical, procedural, and governance especially as it is related to IoT/OT convergence and assess how effectively these controls mitigate key risks under real-world operational constraints and regulatory obligations.
- To develop and validate an integrated, prioritized remediation roadmap and methodology that aligns security improvements with business continuity, regulatory compliance, and stakeholder needs through pilot-testing or stakeholder feedback.

1.6 Scope and Research Question

This research investigates cybersecurity risk management in hybrid IoT/OT environments through a detailed case study of ACME Inc.'s healthcare diagnostic laboratory. The facility employs extensive smart automation, IoT-based diagnostic tools, and specialized OT infrastructure tailored to diagnostic workflows.

The study systematically identifies vulnerabilities and control gaps by aligning with three established frameworks: NIST CSF 2.0, NIST SP 800-82, and IEC 62443 (Abergos and Medjek, 2024). The assessment spans sixteen operational units across facilities, cybersecurity operations, engineering, and administrative functions, evaluating technical, procedural, and governance controls. Over 175 policy documents are audited, and control gaps are mapped against more than 300 framework requirements, enabling detailed compliance analysis and informing a prioritized remediation roadmap (Kaliappan, Sudha, and Shankar, 2024).

The guiding research question is: **How can an integrated framework approach using NIST CSF 2.0, NIST SP 800-82, and IEC 62443 enhance the effectiveness of cybersecurity risk assessment in hybrid IoT/OT test environments?** In pursuing this question, the research combines deep technical investigation with business and regulatory strategy, evaluating not only discrete security flaws but also ACME's overall maturity and readiness to adapt to evolving threats and regulatory expectations.

1.7 Thesis Organization

- Chapter 2 presents the methodology, detailing the five-phase assessment strategy, framework overviews, integration rationale, tools used, and methodological value.
- Chapter 3 reports findings, including risk assessments, gap analysis, and maturity evaluation.
- Chapter 4 offers discussion, recommendations, remediation roadmaps, quick-win and strategic work streams, and reflections on lessons learned.

2 Literature Review

This chapter details the cybersecurity assessment of ACME Inc.'s genomic laboratory, where evaluation of 309 controls against NIST and IEC frameworks revealed critical gaps in vulnerability management, access control, and business continuity. The assessment identified 29 high-risk deficiencies and established the organization's maturity at Tier 2.24, with particular weaknesses in monitoring and incident response. A structured remediation roadmap was developed, prioritizing immediate quick-win actions and long-term strategic investments to transition the organization from reactive to proactive cybersecurity management.

2.1 Cybersecurity Risk Assessment

According to Abergos, and Medjek, (2024), comprehensive cybersecurity risk assessment of ACME Inc.'s hybrid IoT/OT healthcare diagnostic laboratory environment revealed critical vulnerabilities and control deficiencies across multiple operational domains. Through systematic evaluation against the integrated framework of NIST CSF 2.0, NIST SP 800-82, and IEC 62443, the assessment identified 309 total controls, of which 29 were classified as high risk requiring immediate remediation, 101 as medium risk with partial effectiveness, and 179 as adequately implemented. The findings presented in this section represent the culmination of extensive fieldwork, including walkthroughs across pre-analytical and analytical laboratory zones, interviews with 16 operational groups, and review of over 175 evidence items ranging from configuration files to incident response reports. Each identified vulnerability has been mapped to specific framework controls, enabling precise benchmarking against industry standards and regulatory requirements (Choi, 2025). The risk domains examined span from technical vulnerabilities in asset management and network architecture to organizational gaps in governance, training, and business continuity planning. These findings not only expose the current security posture weaknesses but also demonstrate how the convergence of IoT devices, OT

systems, and traditional IT infrastructure creates unique attack vectors that require specialized remediation approaches. The following subsections detail each risk category: vulnerabilities, impacts, framework alignment, and mitigation recommendations for ACME's laboratory (Sishuba et al., 2024).

2.1.1 Vulnerability Management Deficiencies

The assessment revealed systemic gaps in ACME Inc.’s vulnerability management lifecycle. These weaknesses spanned asset discovery, patch deployment, system monitoring, and endpoint visibility. This section outlines key issues identified, their potential impacts, and their alignment with established control frameworks (Metin, Özhan, and Wynn, 2024).

2.1.2 Incomplete Asset Discovery and Inventory

The assessment identified critical IoT and OT devices that were not included in any active asset inventory. Many systems, particularly legacy OT controllers and vendor-managed devices, operate without documented IP addresses or endpoint tags. This discovery gap creates substantial operational risks, as organizations cannot protect assets; they are unaware of (Dohin, et al., 2025). The absence of comprehensive asset visibility directly undermines vulnerability detection capabilities, prevents effective device health monitoring, and severely compromises threat modeling efforts. These findings align with established security standards, specifically NIST SP 800-82 Section 5.3.1 on Asset Identification, IEC 62443-2-1 SR 7.6 requirements for asset inventory, and NIST CSF 2.0's ID.AM-1 control requires physical devices and systems to be properly inventoried (Metin, Özhan, and Wynn, 2024).

2.1.3 Patch Management Deficiencies

The patch management evaluation revealed particularly troubling findings, with multiple IoT sensors and OT applications discovered running firmware versions

that were more than 18 months out of date. The assessment team found that patch cycles occurred sporadically and without any documented rationale or schedule (Malatji, 2023). Perhaps most concerning was the complete absence of automated systems for verifying current patch status or for prioritizing which vulnerabilities required immediate attention based on criticality and exposure. This inadequate approach to system updates directly contradicts established security requirements, including NIST SP 800-82's Section 5.5.1 patch management specifications, IEC 62443-3-3's SR 2.6 mandate for timely application of security patches, and NIST CSF 2.0's PR. IP-12 control requires organizations to implement comprehensive vulnerability management plans (Halawi Ghoson, et al., 2025).

2.1.4 Endpoint Monitoring Coverage Gaps

Although ACME had invested in CrowdStrike's endpoint detection and response platform, the deployment across IoT and OT systems remained spotty and inconsistent. The assessment team identified several OT controllers operating entirely without EDR agents, while compatibility issues prevented installation on multiple IoT platforms (Choi, 2025). This patchwork deployment created dangerous blind spots where unauthorized modifications or malware infections could occur undetected. These coverage gaps failed to meet various framework requirements: NIST SP 800-82's Section 5.6.2 specifications for comprehensive system monitoring, IEC 62443-3-3's SR 3.1 requirements for security event logging across all systems, and NIST CSF 2.0's DE.CM-7 control mandating continuous monitoring for unauthorized personnel, connections, and devices (Sishuba, Edoun, and Pradhan, 2024).

2.1.5 Absence of Real-Time Vulnerability Scanning

A particularly concerning finding involved the deliberate exclusion of IoT/OT devices from all real-time vulnerability scanning activities. Operations staff justified this decision by citing fears of device instability and potential scan-

induced outages. However, this risk-averse stance actually created far greater vulnerabilities by allowing newly disclosed security flaws to remain undetected for extended periods (Halawi Ghoson, et al., 2025). Without regular scanning protocols, ACME had no systematic way to identify when their devices became vulnerable to newly discovered exploits. This practice violated NIST SP 800-82's Section 6.4 vulnerability analysis requirements, contradicted IEC 62443-3-3's SR 2.8 mandate for security function testing and failed to implement NIST CSF 2.0's DE.CM-8 vulnerability monitoring control (Sishuba, Edoun, and Pradhan, 2024).

2.1.6 Risk Implications and Strategic Recommendations

The combined impact of these deficiencies created multiple, overlapping vulnerabilities. Unauthorized actors could gain remote access to unmanaged endpoints without detection. The organization faced delayed identification of both known exploits and emerging zero-day threats. Compliance teams could not confirm device patch status or overall security compliance, creating significant regulatory exposure under HIPAA, GDPR, and FDA 21 CFR Part 11 (Chairopoulou, 2024). The team recommended automated asset discovery platforms, baseline patch policies, comprehensive OT endpoint monitoring, and bi-weekly vulnerability scans with real-time alerting (Mexis et al., 2025).

2.2 Access Control and Change Management Deficiencies

Access control and change management formed the backbone of any mature security program, yet the assessment revealed these foundational elements were poorly implemented across ACME's environment. Laboratory users possessed largely unrestricted abilities to alter system configurations without oversight or approval processes. This uncontrolled access destroyed any possibility of maintaining reliable audit trails and made it nearly impossible to trace the source of system problems or security incidents (Kaliappan, Sudha, and Shankar, 2024).

End users throughout the laboratory maintained full administrative rights to install any software they chose on critical diagnostic workstations. During interviews, multiple technicians confirmed they routinely downloaded and installed utility programs, browser extensions, and productivity tools without any approval process or security review (Lill, Doleh, and Katzenbeisser[1], 2025). The continued use of shared accounts across departments represented another critical failure. These generic logins eliminated individual accountability and would make forensic investigation nearly impossible following any security incident. Most troubling was the complete absence of a defined separation of duties, with single individuals holding both operational and administrative privileges that should never coexist. These combined weaknesses earned a high-risk classification due to their potential for enabling both accidental mishaps and deliberate insider attacks (Reuben-Owoh, and Haig, 2025).

2.3 Control Mapping, Gap Analysis & Maturity Evaluation

ACME's cybersecurity posture was assessed by mapping over 300 operational and technical controls against three key frameworks: the NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-82 Revision 2, and IEC 62443. This comprehensive mapping allowed for a systematic evaluation of control implementation, alignment with leading practices, and identification of areas requiring improvement (Kaliappan, Sudha, and Shankar, 2024).

“The NIST CSF 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization regardless of its size, sector, or maturity to better understand, assess, prioritize, and communicate its cybersecurity efforts” (*Agenda Center*, 2026) (Lill, Doleh, and Katzenbeisser[1], 2025). The CSF does not prescribe how outcomes should be achieved; rather, it links to online resources that provide additional guidance on practices and controls that could be wholly incorporated into this publication. "NIST SP 800-82 Revision 2 offers guidance on securing Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA)

systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements“ (Search | CSRC, 2026), (Sishuba, Edoun, and Pradhan, 2024).

“IEC 62443 is a series of standards that address security for operational technology in automation and control systems. The series is divided into different sections and describes both technical and process-related aspects of automation and control system of security” (Welcome to Zscaler Directory Authentication, 2026). Each framework's controls were categorized into domains and subdomains, facilitating alignment with ACME’s organizational functions. The mapped data was analyzed both qualitatively and quantitatively, factoring in maturity levels, framework overlap, and operational applicability (Choi, 2025).

Control effectiveness was assessed using a three-tier rating system: "Effective" for fully implemented and enforced controls, "Partially Effective" for those with inconsistencies or coverage gaps, and "Not Effective" for controls that were either not implemented or non-functional in practice. These effectiveness scores were directly used to assign risk levels and guide remediation planning. The gap analysis revealed that ACME's average maturity across all domains was Tier 2.24, placing it between Tier 2 and early Tier 3. The highest maturity was observed in training and policy enforcement, while the lowest was in monitoring, detection, and recovery functions (Lill, Doleh, and Katzenbeisser[1], 2025).

The integration of the three frameworks revealed overlapping controls, especially in areas such as Access Control, Incident Response, and Configuration Management. This mapping helped eliminate duplicative efforts and informed ACME’s decision to centralize several functions such as logging, identity management, and security documentation. Strategic implications include the need to maintain a centralized risk register linked to control effectiveness, invest in weak domains such as Detect (SIEM, IDS), Respond (playbooks, escalation), and Recover (BC/DR testing), and leverage cross-framework implementation to adapt to healthcare regulations like HIPAA and GDPR while ensuring ICS-specific coverage (Reuben-Owoh, and Haig, 2025).

2.4 Recommendations and Prioritized Remediation Roadmap

Healthcare organizations often face challenges in implementing cohesive cybersecurity frameworks, leading to fragmented security measures that may leave critical vulnerabilities unaddressed. To address this, a comprehensive risk assessment and control evaluation were conducted, resulting in actionable recommendations categorized into prioritized workstreams. Each remediation activity was assessed for urgency, implementation complexity, and anticipated return on investment (Edwards, 2024). The roadmap aligns with the strategic goal of elevating cybersecurity maturity toward Tier 3+ within the NIST Cybersecurity Framework (CSF). A cost-benefit analysis matrix was employed to evaluate and categorize the security and privacy gap remediation workstreams identified during the assessment. This systematic approach enables organizations to optimize resource allocation while maximizing security improvements aligned with business objectives (Reuben-Owoh, and Haig, 2025).

2.5 Quick Win Workstreams

Quick win workstreams deliver immediate, high-impact improvements to ACME Inc.'s cybersecurity controls, targeting the 29 high-risk gaps identified in vulnerability management and access control. These targeted interventions, spanning incident response enhancements, OT monitoring expansion, network segmentation, and physical security reinforcement, enable rapid risk reduction while building momentum for strategic initiatives

2.5.1 Incident Response and Management

Developing and testing playbooks for common attack scenarios, such as ransomware and privilege escalation, is crucial for enhancing incident response capabilities. Integrating alerts from security tools like CrowdStrike into Security Information and Event Management (SIEM) systems with real-time escalation

procedures ensures timely detection and response to security incidents. Conducting quarterly tabletop exercises helps in assessing the effectiveness of the incident response plan and identifying areas for improvement (Edwards, 2024).

2.5.2 OT System Monitoring and Audit

Expanding Endpoint Detection and Response (EDR) and Antivirus (AV) tools to cover all Internet of Things (IoT) and Operational Technology (OT) endpoints enhance visibility into potential threats. Enabling logging, time synchronization, and log integrity validation ensures accurate and reliable audit trails. Defining audit log retention and access policies is essential for compliance and forensic analysis (Salihu, and Dervishi, 2024).

2.5.3 IoT/OT Network Segmentaation

Implementing logical segmentation using Virtual Local Area Networks (VLANs) and applying firewall rules based on least privilege and system criticality reduces the attack surface. Disabling unnecessary protocols on shared subnets minimizes potential entry points for attackers (Edwards, 2024).

2.5.4 Physical Security and Controls

Reinforcing access control to laboratories and server rooms, updating badge and visitor tracking systems, and installing tamper alarms on critical OT cabinets to enhance the physical security posture. These measures prevent unauthorized access and protect sensitive equipment from physical threats (Kortemaa, 2025).

2.6 Strategic Remediation Workstreams

Strategic remediation workstreams address foundational, long-term enhancements to elevate ACME Inc.'s cybersecurity maturity from Tier 2.24 toward repeatable Tier 3 practices under NIST CSF 2.0.

2.6.1 Business Continuity and Disaster Recovery

Developing laboratory-specific Business Continuity and Disaster Recovery (BC/DR) plans ensures preparedness for unforeseen events. Performing scenario-based testing and updating Recovery Time Objective (RTO) and Recovery Point Objective (RPO) documentation helps assess the effectiveness of the plans. Introducing alternate storage sites with geo-redundancy enhances data availability and resilience (Kortemaa, 2025).

2.6.2 Configuration and Patch Management

Maintaining hardened baseline configurations for all systems and automating patching for supported platforms reduces vulnerabilities. Performing monthly vulnerability validation scans ensures that systems remain secure and compliant with security standards (Rahman, et al., 2024).

2.6.3 Policy and SOP Documentation

Version controlling all policies and ensuring annual review cycles maintain the relevance and effectiveness of security measures. Training teams on updated Standard Operating Procedures (SOPs) during onboarding and role changes ensure consistent implementation. Ensuring consistency between written policies and observed behavior fosters a culture of security compliance (Menzel, Hurink, and Remke, 2025).

3 Methodology

This study adopts a qualitative case study design focused on ACME Inc., a genomic healthcare diagnostic laboratory. The aim is to understand in depth how IoT/OT device security is managed, how established frameworks namely NIST CSF 2.0, NIST SP 800-82, and IEC 62443 are applied or fall short, and how regulatory obligations (such as those from medical device regulation, data privacy laws, device safety / post-market obligations) are perceived and fulfilled in real operational settings. Given the complex interdependencies of devices, regulations, safety, and operational continuity, the qualitative case study method allows the collection of rich, contextual, detailed data from multiple sources (Ahmed, and Tonoy, 2025). The methodology is structured in phases: stakeholder alignment and scope definition; document and policy review; field observations, interviews, and close-ended questionnaire; control and regulatory mapping; and reporting with remediation planning.

3.1 Phases of the Assessment

The first phase of the assessment comprises project kick-off and stakeholder alignment. During this phase, stakeholders from laboratory services, IT/OT engineering, cybersecurity/governance, facilities/environmental control, compliance or regulatory offices, senior management, and where possible vendor representatives are engaged to define the scope. The scope includes the lab zones (pre-analytical, analytical, possibly post-analytical), all classes of connected devices (environmental sensors, analyzers, robotics, etc.), data flows, and vendor relationships. Additionally, regulatory obligations applicable to ACME Inc. are identified, including medical device safety, data protection/privacy laws (e.g., GDPR/equivalent local laws), post-market surveillance, device certification, and vendor obligations. The frameworks being used (NIST CSF 2.0, SP 800-82, IEC 62443) are introduced among stakeholders, and initial alignments are made about what control/maturity levels are expected or targeted. The interview guide and the closed-ended

questionnaire instruments are designed in this phase, drawing upon framework domains and regulatory clauses to capture both policies/practices and regulatory or framework awareness/perceptions. Ethical approvals, confidentiality, recording consent, and data handling plans are also established here.

The second phase focuses on documentation and policy review. The research team collects existing documentation from ACME Inc., including asset inventories of IoT/OT/IT devices, network architecture and segmentation diagrams, standard operating procedures or SOPs for device configuration, firmware update and patching, change management, incident response, vendor contracts and service level agreements, and policies for data privacy, safety, and compliance. Regulatory documentation such as device technical files, conformity or certification records, previous audit or regulatory review reports, privacy impact assessments, incident reports, or near misses is also gathered. This documentation sets the baseline for understanding what is formally required or claimed, which enables comparison between documented expectations and actual practice.

Phase three comprises field observations, semi-structured interviews, and responses to a closed-ended questionnaire. Field observations occur in the physical laboratory zones, observing how devices are installed, how environmental and physical access controls are implemented, how network cables and connections are organized, how devices are powered, cooled, maintained, how staff interact with devices during diagnostic operations, whether firmware updates are applied, whether logging and monitoring tools are active and what is observable of their configuration or behavior. The interviews were conducted with staff members who played different roles in the operational industry and sectors; however, attention was given to the pre-analytical and analytical. The staff was responsible for different device management and networking, environmental control personnel, cybersecurity personnel, and senior management. It took around 20 to 30 minutes to interview a participant to gain more appropriate and detailed information about the regulatory and

technical details. Similarly, the questionnaire was designed to collect responses from the participants to understand their experiences and reviews about the framework and regulatory awareness used. It was essential to collect responses to ensure suggestions are offered for improving the safety vs security trade-offs and device or vendor challenges.

The fourth phase is control and regulatory mapping, and evidence review. After collecting interviews, questionnaire responses, field observation notes, policy documents, and vendor contract data, the data is systematically analyzed. The research team maps each finding practices, gaps, perceptions to control criteria drawn from NIST SP 800-82 (particularly the OT/ICS technical, operational controls), IEC 62443 (component and system security levels, zone/conduit architecture, component hardening), and NIST CSF 2.0 (governance, supply chain/vendor obligations, the six core functions including the newer “Govern” function, maturity tiers). Regulatory obligations identified earlier (medical device regulation, device safety, post-market obligations, data protection/privacy, vendor or manufacturer responsibility) are also mapped in parallel so that findings are evaluated not only against framework best practices but also legal and regulatory duties. Gaps and areas where practices partly meet or fail to meet expectations are identified, and root causes are sought via interview or observation, or questionnaire narrative.

Phase five reporting, remediation planning, and target settings. The phase is very important for presenting the findings in the form of detailed reports for the policymakers and technical staff. In addition, the evaluated cases highlight the regulatory exposures and key risks associated with the subject matter. The remediation road map is designed for improvements in terms of short-term, mid-term, and long-term. However, it was essential to set targets for evaluating the security or maturity levels for being relative to NIST CSF 2.0 tiers or IEC 62443 security levels that ensure alignment of change to the regulatory obligations. The recommendations offered in the study promote changes in the configuration or device, firmware update practices or vendor contracts, procedural or policy updates, training or staff awareness, and regulatory

compliance documentation. Operational constraints are also considered in the roadmap for availability, safety, vendor support, diagnostic throughput, and budget.

3.2 Qualitative Case Study Design: Interviews, Questionnaire, Participant Numbers, Saturation

The research used semi-structured interviews and a closed-ended questionnaire as qualitative data collection methods. The interview method affords in-depth accounts of practice, trade-offs, regulatory understanding, and technical constraints, and aligns with observations and documents. Interviewees are selected via purposive sampling to ensure a range of functional roles: lab technicians from pre-analytical and analytical zones, IT/OT engineers, cybersecurity/compliance officers, facilities/environmental staff, senior management, and vendor representatives. Each interview is approximately forty-five to seventy-five minutes, conducted in private settings (onsite or virtual), audio recorded (with consent), and transcribed in full. Where translation is required, checks ensure accuracy. The interview guide is semi-structured: beginning with role and operational context, then device/vendor/framework/regulatory topics, and concluding with ideas for improvement or perceived trade-offs. However, to avoid disruptions during the schedule of interviews in the diagnostic operations, it requires improving operational load and staff availability.

A broader group of staff was selected to answer or respond to the closed-ended questionnaire; these were the participants who were not included or available for the interviews. The respondents shared the challenges, perceptions, framework, or regulatory awareness, and experiences through the options of the questionnaire. Challenges like vendor issues, device lifestyle, and near misses were identified that were used for suggesting changes. It can be distributed electronically or via paper, where necessary, to all staff in roles that touch on device operation, maintenance, security, compliance, safety, vendor relations, and management. Vendor contacts are included where possible. The

questionnaire is administered after the initial policy/documentation review, so respondents may reference known policies or devices in their responses.

Regarding participant numbers, the study targets 10 interviews in total. This figure is chosen so that a diverse set of roles is represented and that thematic saturation can be reached; qualitative research literature indicates that ten to twenty interviews are often sufficient in case studies with multiple stakeholder types, though saturation is the guiding principle. Empirical studies suggest that saturation of themes in health and technical contexts often occurs around fifteen interviews, but because of differing perspectives (roles, device types, operational zones), the plan allows for up to twenty or slightly more if new themes continue to emerge. For the closed-ended questionnaire, the aim is to receive between 40 narrative responses with sufficient depth and detail. Vendor or supplier participants are expected to number about 2 to 4, subject to availability. In addition, senior management/compliance/regulatory roles are expected to contribute through at least 2-3 interviews to ensure oversight and governance perspectives are included.

3.3 Data Analysis and Framework/Regulatory Mapping

The qualitative data collected from all the sources, including field observations, questionnaire narratives, interview transcripts, and literature review, were processed using thematic analysis. The approach contained multiple stages that were aligned to the objectives of the study. The transcripts were read and re-read by the researcher several times to ensure the correct meaning of the observation and participant experience was included in the study.

Second, coding is applied: inductively to capture new or unexpected themes emerging from staff narratives (for example vendor constraints, safety vs diagnostics trade-off, regulatory awareness gaps), and deductively with codes based on framework control domains (e.g. device hardening, access control, network segmentation, monitoring & detection, incident response) from NIST SP 800-82, IEC 62443, and CSF 2.0 (including its governance, supply chain,

and maturity tier aspects). Regulatory duties identified earlier (device safety, model certification, data privacy/breach notification, regulatory reporting) are coded as separate but linked categories.

Next, the codes are grouped into theme clusters of related ideas that together reflect patterns across participants (for example, “firmware lifecycle gaps,” “vendor non-responsiveness,” “policy vs real practice,” “lack of regulatory clarity,” “safety or availability overriding security,” etc.). During this thematic construction, the researcher checks consistency across roles, zones, and device types, and examines whether participants’ perceptions align or diverge. Thematic saturation is assessed: after a certain number of interviews (e.g. after ~15), the researcher notes whether new interviews are yielding new themes; if not, extra interviews may be curtailed; if yes, additional participants are recruited until saturation seems achieved or resources are exhausted.

After theme development, a mapping matrix is developed in which each identified theme or gap is linked to the relevant control criteria in the three frameworks (NIST CSF 2.0, NIST SP 800-82, IEC 62443) and relevant regulatory obligations. For each theme, the researcher determines whether current states fully meet, partially meet, or fail to meet those criteria or obligations. These reveals overlap among frameworks and regulatory requirements, where certain framework controls may cover regulatory duties, where there are regulatory obligations outside of framework coverage, and where framework expectations are not met in practice.

Finally, findings are synthesized into recommendations and target settings. Zones or device categories are assessed for their current maturity or security level (using CSF 2.0 maturity tiers and IEC 62443 security levels) relative to what is required by best practice and regulatory law. Recommendations are prioritized considering the severity of gaps (both risk to operations/data/patient safety and regulatory exposure), feasibility given current resources and device/vendor lifecycle, and operational constraints such as device availability, safety, lab throughput. Reports compiled include direct quotations (anonymized by role), context descriptions (device type, zone, vendor dependency), and

show where policy or documentation misaligns with practice. Member checking is used: summaries are shared with some participants to verify interpretations.

3.4 Justification Tools, and Value

Qualitative research design was employed in the study to understand the complex phenomenon related to the management of cybersecurity and handling risks in the field through evaluating the natural environment. It allowed us to examine the interaction of staff to maintain and perceive the working of IoT/OT devices in various constraints. In addition, it allowed to examine the relationships of vendor, safety concerns, regulatory obligations, framework expectations, and diagnostic throughput. However, the questionnaire and semi-structured interviews allowed us to capture deep and broad perspectives. The chosen participant numbers (10 interviews, 40 narrative responses) are supported by qualitative methods of literature regarding saturation: around ten to twenty interviews often suffice in case study settings with multiple stakeholder roles. For example, some studies show saturation often occurs around 9-17 interviews in health settings.

Tools used include document management systems and manual qualitative data analysis to organize, code, and map data. Observation forms are used during field walkthroughs to document physical, environmental, network layout, and device configuration. Vendor contracts, policy documents, and vendor device lifecycle documentation are reviewed. Regulatory documents are examined.

The value of this methodology lies in its ability to produce richly detailed findings that not only identify what gaps exist at the technical or procedural level but also reveal why those gaps exist (vendor support, device constraints, regulatory ambiguity, safety vs availability trade-offs). The mapping frameworks and regulatory obligations ensure that recommendations are both feasible and compliant, not simply ideal but out of reach. Because this is a case study, generalizability is limited, but transferability is supported via thick description of

context (device types, vendor relationships, safety constraints, regulatory environment) so other labs or similar settings can judge applicability.

3.5 Data immersion

This CSF 2.0's **ID.AM-1** control requires a foundational step in qualitative analysis for several reasons; therefore, it was addressed under the following elements;

Depth and Richness

Immersion ensures the researcher doesn't miss small but meaningful details, like how something is said, hesitation, emphasis, etc., that could be lost if one only skimmed transcript or jumped quickly into coding.

Reducing Bias

By reading and revisiting the data, the researcher becomes aware of their own preconceptions. Getting familiar with multiple accounts helps prevent premature assumptions or imposing frameworks before the data is well understood.

Identifying Themes and Gaps

Repeated readings allow themes to emerge naturally. Also, contradictions become visible, and the researcher can notice where certain topics are underrepresented, which may affect whether more interviews are needed.

Grounding Interpretation

Later, when assigning codes (labels for pieces of data), building themes, or mapping to theory/framework/regulation, the researcher referred to the data with confidence, knowing the context, possible alternative interpretations, and where individual narratives reinforce or diverge from trends.

Credibility & Trustworthiness

Immersion supports rigor: it helped to ensure findings are credible (reflecting participants' experiences), dependable (others could see the same themes), and possibilities of transferability (others can understand context). It also supports transparency to trace findings back to specific quotations or contradictions you noticed during immersion.

4 Findings, Results and Discussion

Through interviews with cybersecurity professionals, questionnaire responses, and literature analysis, this chapter reveals a complex picture of cybersecurity readiness in healthcare diagnostic laboratories. While most organizations recognize cybersecurity as a strategic priority and have implemented frameworks like NIST CSF, significant challenges remain in harmonizing controls across IT and OT systems, with nearly 70% of participants reporting moderate to extreme difficulty. The assessment of ACME Inc. identified concerning gaps across 309 evaluated controls, achieving only Tier 2.24 maturity, with critical weaknesses in asset management, network segmentation, and incident response preparedness. Resource constraints emerged as a persistent barrier, with organizations lacking adequate budget and skilled personnel despite the importance of cybersecurity. The findings demonstrate that while integrated frameworks provide valuable strategic clarity, success depends on continuous education, clear role definition, proactive monitoring, and sustained organizational commitment to bridging the gap between policy and practice.

4.1 Findings of Interview Responses

The interviews revealed that while patient safety is the primary motivation for cybersecurity efforts, significant challenges exist in harmonizing various frameworks. Key weaknesses were identified in network segmentation, asset management, and staff training, highlighting a clear need for a standardized and integrated approach to cybersecurity. Participants consistently expressed that a unified methodology would not only address these gaps but also significantly reduce the likelihood of security incidents.

4.1.1 Participant Background and Methodology

Interviews were conducted with 10 participants from diverse departments, including IT, OT, lab management, and clinical engineering. This cross-functional representation provided valuable insights into risk management mechanisms and the current state of cybersecurity in hybrid IoT/OT diagnostic laboratories. While participants brought varied perspectives based on their roles and experience levels, several key themes and concerning areas emerged consistently.

4.1.2 Patient Safety and Regulatory Alignment

Participants identified patient safety as the primary driver for implementing cybersecurity strategies in healthcare settings. A significant majority (72.5%) emphasized the critical importance of aligning cybersecurity initiatives with regulatory compliance requirements, particularly MHRA and GDPR standards. Framework adoption varied across organizations, with NIST CSF implemented by 62.5%, ISO/IEC 27001 by 50%, and IEC 62443 by 45%. However, 55% of participants reported challenges in harmonizing these frameworks, citing difficulties in integrating diverse standards within complex diagnostic laboratory environments.

4.1.3 Control Effectiveness and Identified Gaps

While 42.5% of participants rated their cybersecurity controls as moderately to highly effective in mitigating diagnostic lab risks, significant gaps emerged. The most frequently identified weaknesses included insufficient network segmentation, incomplete asset inventories, and limited staff training. These deficiencies create vulnerabilities that require robust, tailored controls to address. Additionally, participants noted only partial clarity in defining cybersecurity responsibilities across clinical engineering, IT, OT, and lab management teams, leading to coordination challenges.

4.1.4 Incident Preparedness and Framework Integration

Organizations reported moderate preparedness for cybersecurity incidents affecting IoT/OT systems, with the same gaps as network segmentation, asset inventory, and training, identified as critical bottlenecks. Notably, 75% of participants supported adopting standardized methodologies for integrating cybersecurity frameworks, believing this approach would significantly reduce incident likelihood. Participants emphasized the need for scalable guidelines and structured approaches to meet evolving cybersecurity needs while balancing operational efficiency with security measures.

Objective 1: Assess the alignment of cybersecurity strategies with patient safety objectives

General alignment of patient safety objectives and cybersecurity strategies is identified in the responses of interviews. It is indicated by the participants that the main reason for implementing cybersecurity measures is patient safety for the organizations, while challenges are a part of implementing the strategies and safety goals. Therefore, improvements in the areas are suggested for ensuring the safety of the patient.

Objective 2: Evaluate the implementation and harmonization of cybersecurity frameworks

The findings indicate that the need for standardized methodologies is mandatory in different departments for integrating cybersecurity frameworks. There are many challenges harmonizing in the view of the participants that are required to be addressed effectively. In this regard, it can be said that the present cybersecurity frameworks are absolutely not supporting seamless integration.

Objective 3: Examine the effectiveness of cybersecurity controls in mitigating risks specific to diagnostic lab environments

Levels of effectiveness are reported by the participants for cybersecurity controls that have the capacity to mitigate the diagnostic lab environment risks. The interview responses reveal that some controls are inadequate, and some are deemed effective for addressing unique risks. It reflects the need to measure tailored needs of cybersecurity risks to manage the working ideologies of diagnostic lab settings.

4.2 Summary of Qualitative Interview Themes:

The semi-structured interviews provided critical context, revealing that while patient safety is a recognized driver for cybersecurity, significant challenges persist. Key themes that emerged include the difficulty of harmonizing multiple frameworks, the existence of gaps in critical controls like network segmentation and asset management, and a need for clearer role definition among departments to improve incident preparedness.

4.3 Introduction to Quantitative Questionnaire Data:

To build upon qualitative insights, a closed-ended questionnaire was administered to a broader group of staff. The following sections present the quantitative findings from this questionnaire, which were designed to measure the specific attitudes and the perceived state of cybersecurity readiness across the organization. These results provide a statistical overview of the key areas discussed in the interviews.

4.4 Findings of Questionnaire Responses:

To build upon the qualitative insights, a closed-ended questionnaire was administered to a broader group of staff. The following sections present the quantitative findings from this questionnaire, which were designed to measure

the specific attitudes and the perceived state of cybersecurity readiness across the organization. The first question assessed the alignment between the organization's cybersecurity strategy and its patient safety objectives, with the results shown in Figure 1.

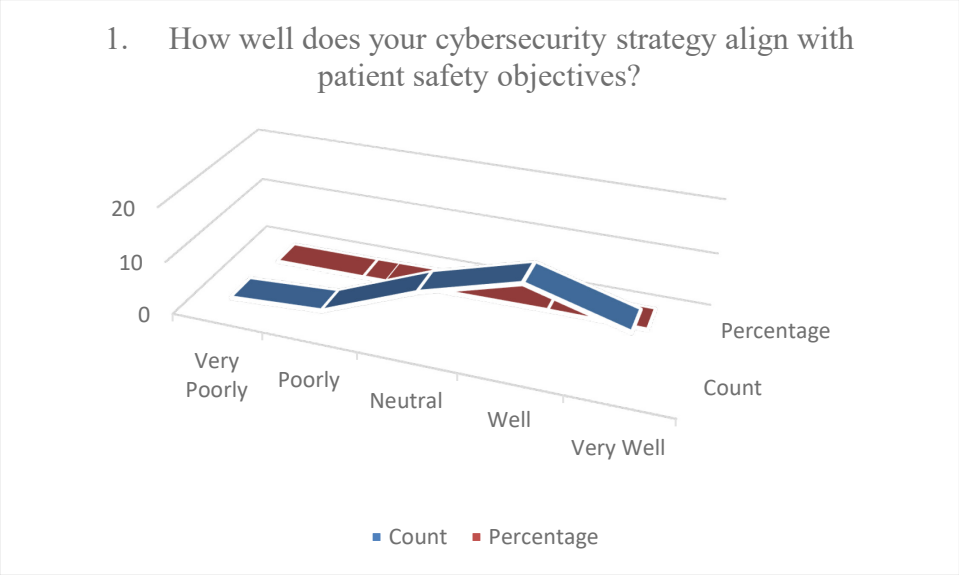

Figure 1. Question 1: Cybersecurity strategy for patient safety.

A mix alignment in the patient safety objectives and cybersecurity strategies is identified in response to the question. The percentages were concluded according to the strategies as follows: effectively aligned was 37.5%, very well aligned was 25%, while the percentage for neutral and poorly aligned was 32.5%. This reflects that the alignment of the patient's safety objectives is not effectively aligned with cybersecurity measures. The recent reports of cybersecurity attacks present that at least once a year cyberattack occurs to the 92% of the healthcare organizations. Therefore, improvement in the institutions is required for safeguarding data and patient care using efficient and reliable cybersecurity frameworks.

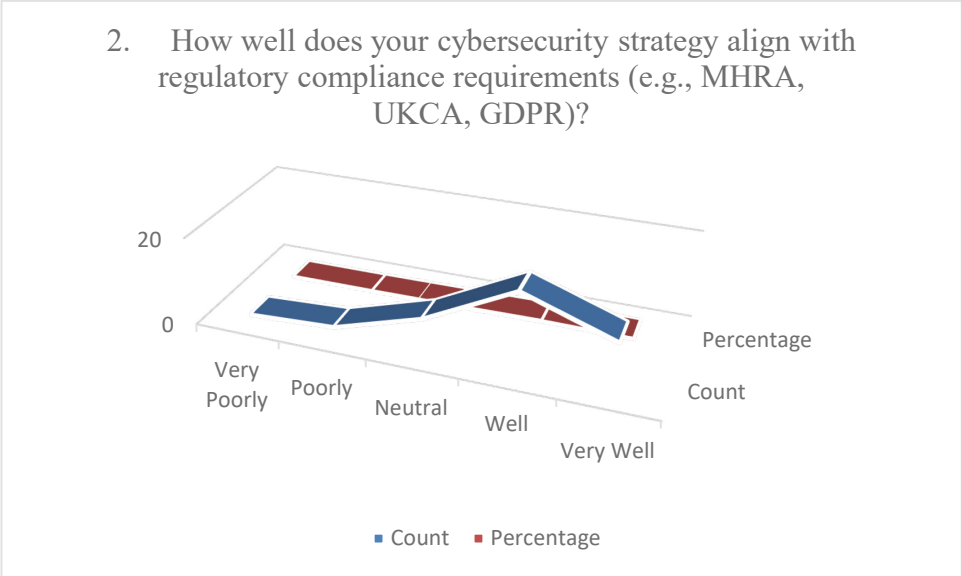

Figure 2. Question 2: Cybersecurity strategy and regulatory compliance requirements.

A strong alignment between regulatory compliance requirements and cybersecurity strategies was observed. As detailed in Figure 2, 45% of participants indicated a "Well" alignment and 27.5% indicated a "Very Well" alignment, while only 8% of participants referred to it as poorly aligned. The results reflect that effective integration of the compliance framework is ensured for cybersecurity by means of the organizations. The value of aligning the cybersecurity strategies is optimized with the regulatory advancements for ensuring data protection and patient safety.

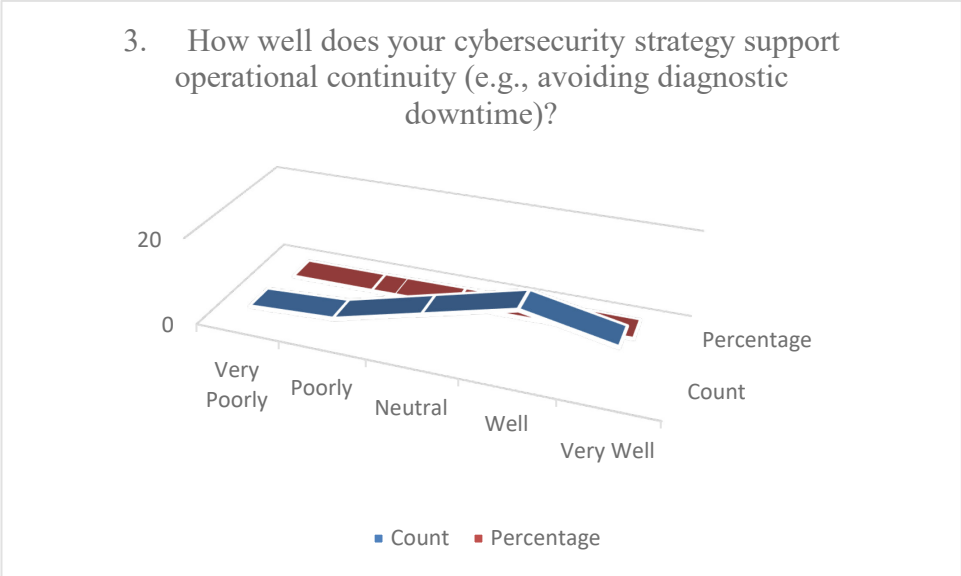

Figure 3. Question 3: Cybersecurity strategy and operational continuity.

The survey also questioned how well the current cybersecurity strategy supports the critical goal of operational continuity by avoiding diagnostic downtime. As shown in Figure 3, while 60% of participants believe the strategy provides effective support, a significant 40% were either neutral or felt the alignment was poor, indicating a clear need for improvement. Therefore, it is essential to foster the cybersecurity culture to attain effective recovery and incident response plans with cross-departmental collaboration.

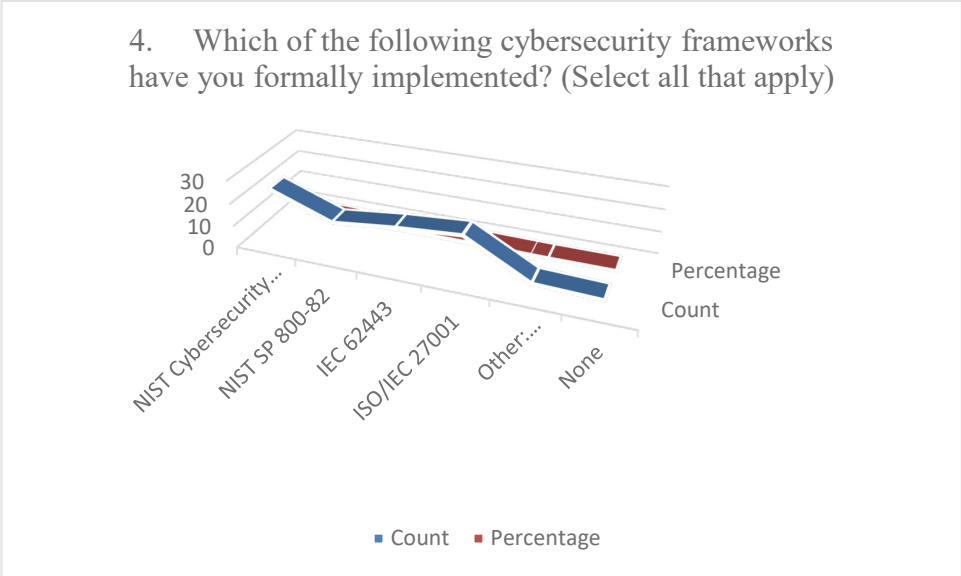

Figure 4. Question 4: Implementation of cybersecurity frameworks.

To understand the foundational standards in use, participants were asked which cybersecurity frameworks their organization has formally implemented. The responses, detailed in Figure 4, show that the NIST Cybersecurity Framework (CSF) is the most widely adopted at 62.5%, though other key frameworks like IEC 62443 are also utilized, reflecting a multi-framework approach in many laboratories.

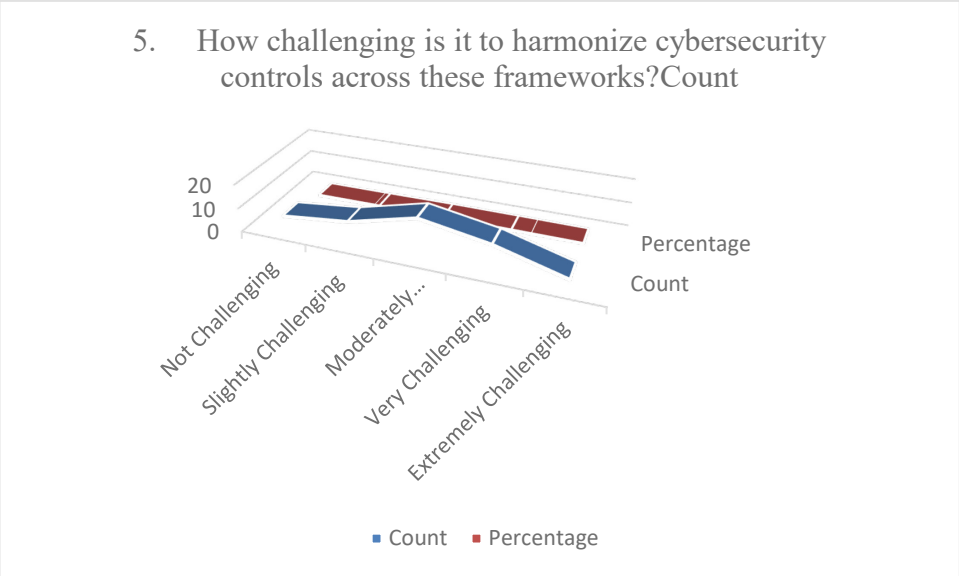

Figure 5. Question 5: Challenges in harmonizing cybersecurity controls across frameworks.

Given that multiple frameworks are often in use, the next question assessed the difficulty of harmonizing controls across them. The feedback, illustrated in Figure 5, reveals this is a significant issue, with a combined 68.75% of participants finding the process to be moderately, very, or even extremely challenging.

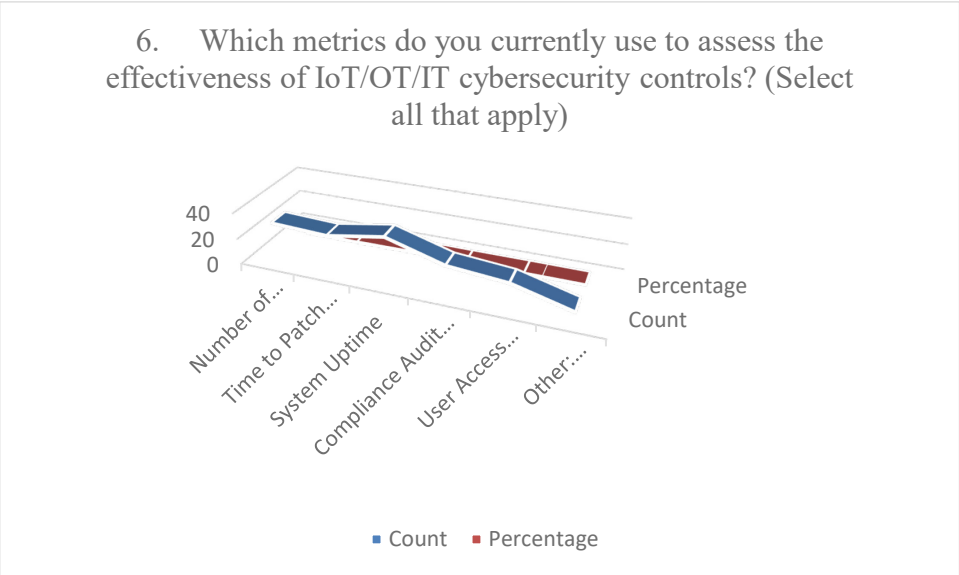

Figure 6. Question 6: Metrics to access cybersecurity controls.

Participants were asked to identify the metrics they currently use to measure the effectiveness of their IoT, OT, and IT cybersecurity controls. As summarized in Figure 6, the most common metrics are system uptime (87.5%), the number of security incidents (75%), and the time required to patch vulnerabilities (70%).

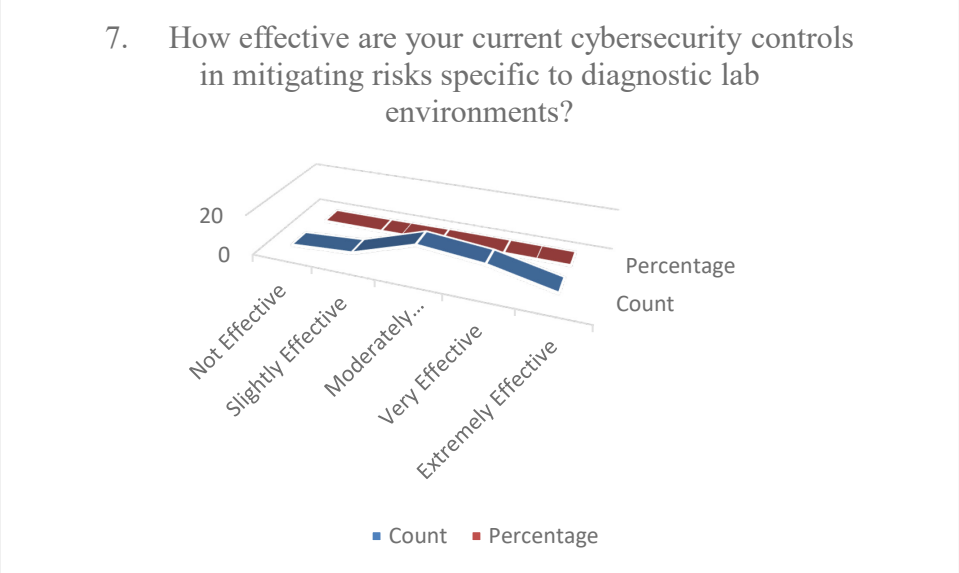

Figure 7. Question 7: Cybersecurity control for mitigating risks in diagnostic lab environments.

The perceived effectiveness of current cybersecurity controls in mitigating risks specific to the diagnostic lab environment was a key area of inquiry. Figure 7 shows a mixed level of confidence, as 42.5% of participants rated their controls as moderately to extremely effective, while 20% reported very low effectiveness, highlighting a clear gap between implemented controls and perceived security.

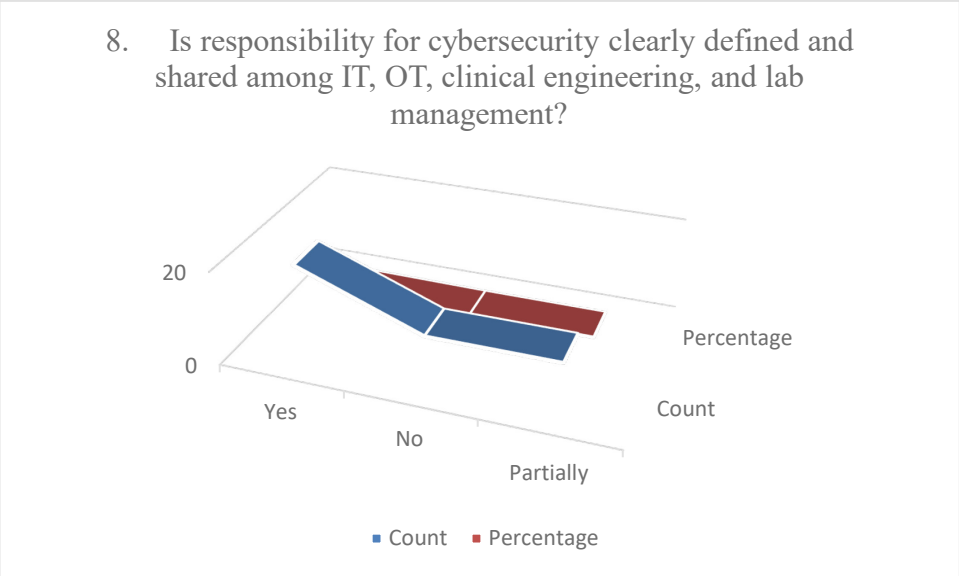

Figure 8. Question 8: Shared responsibility among IT, OT, clinical engineering, and lab management.

To gauge the clarity of governance, the survey asked whether responsibility for cybersecurity is clearly defined and shared among IT, OT, clinical engineering, and lab management. The responses presented in Figure 8, were split, with exactly 50% of participants confirming that roles are clearly defined, while the other 50% reported that this is only partially true or not true at all.

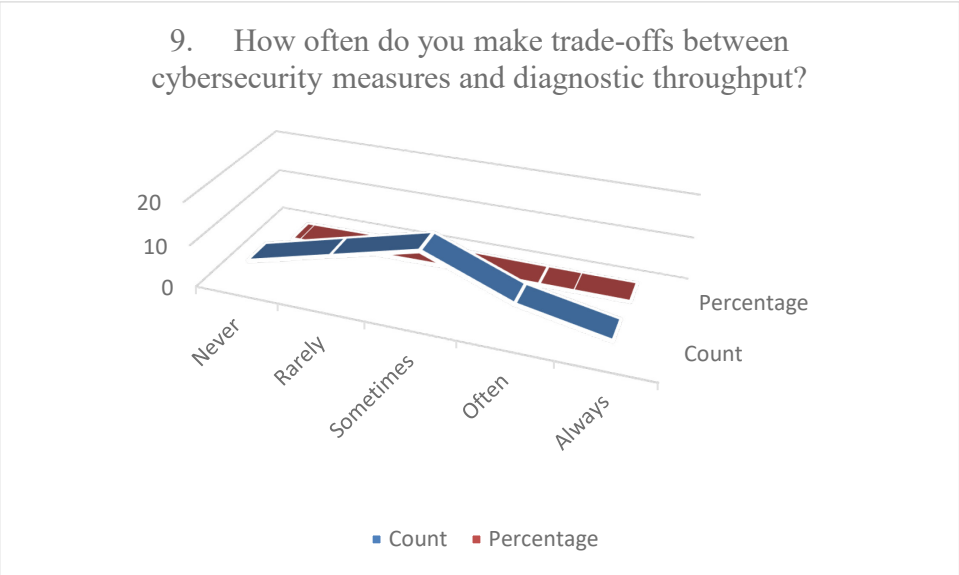

Figure 9. Question 9: Tradeoffs between cybersecurity measures and diagnostic throughput.

The survey also explored the delicate balance between security and operational demands by asking how often trade-offs are made between cybersecurity measures and diagnostic throughput. As Figure 9 illustrates, such compromises are common, with 37.5% of respondents making them ‘sometimes’ and another 25% making them ‘often.’

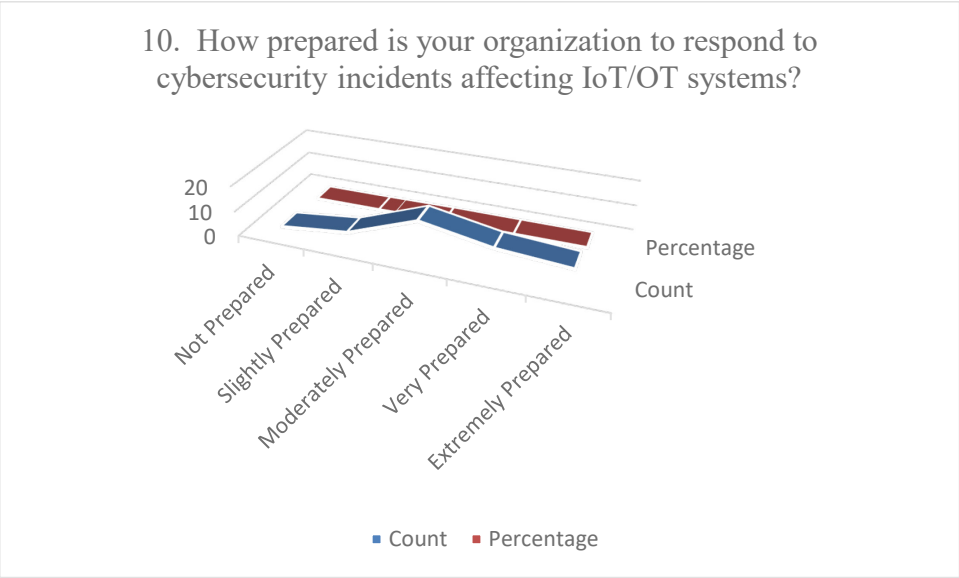

Figure 10. Question 10: Organizational preparedness of IT / OT systems towards cybersecurity incident response.

Organizational preparedness for incidents affecting IoT and OT systems is a critical indicator of resilience. When asked about this, 45% of participants felt their organization was "moderately" to "extremely" prepared. The detailed breakdown of these confidence levels is shown in Figure 10.

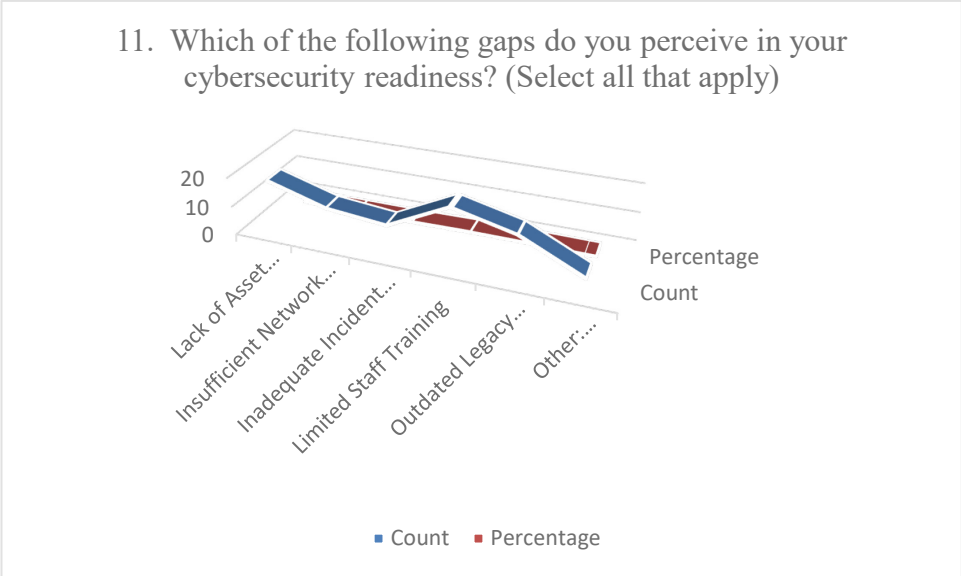

Figure 11. Question 11: Gaps perceived in cybersecurity readiness.

To pinpoint specific weaknesses, participants were asked to identify the most significant gaps in their organization's cybersecurity readiness. According to the data in Figure 11, the most commonly perceived gaps are limited staff training (50%), a lack of complete asset inventory (45%), and the presence of outdated legacy systems (37.5%).

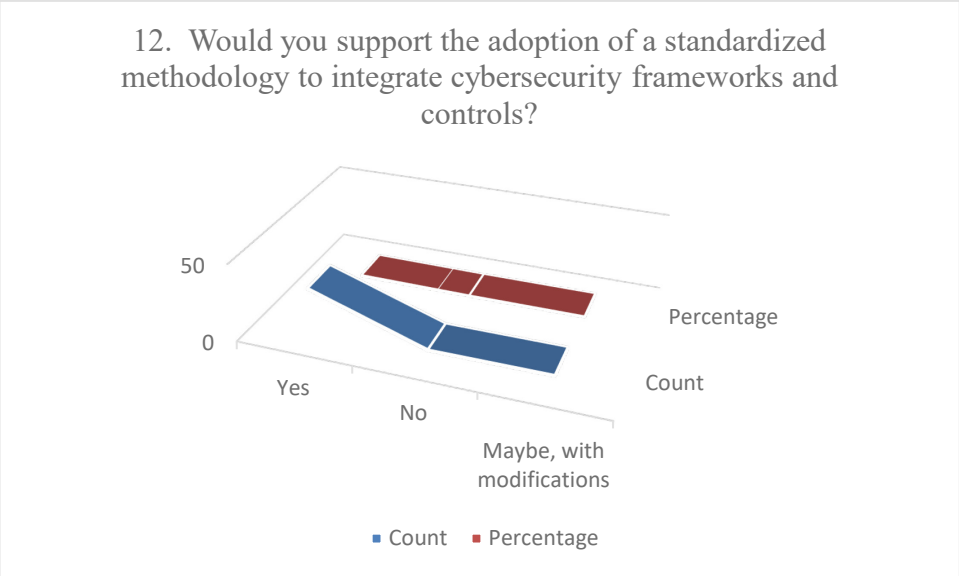

Figure 12. Question 12: Adoption of standardized methodology to integrate CSF and controls.

Participants were asked whether they would support the adoption of a standardized methodology to better integrate the various cybersecurity frameworks and controls. As demonstrated in Figure 12, there is overwhelming support for this idea, with 75% of respondents answering "Yes."

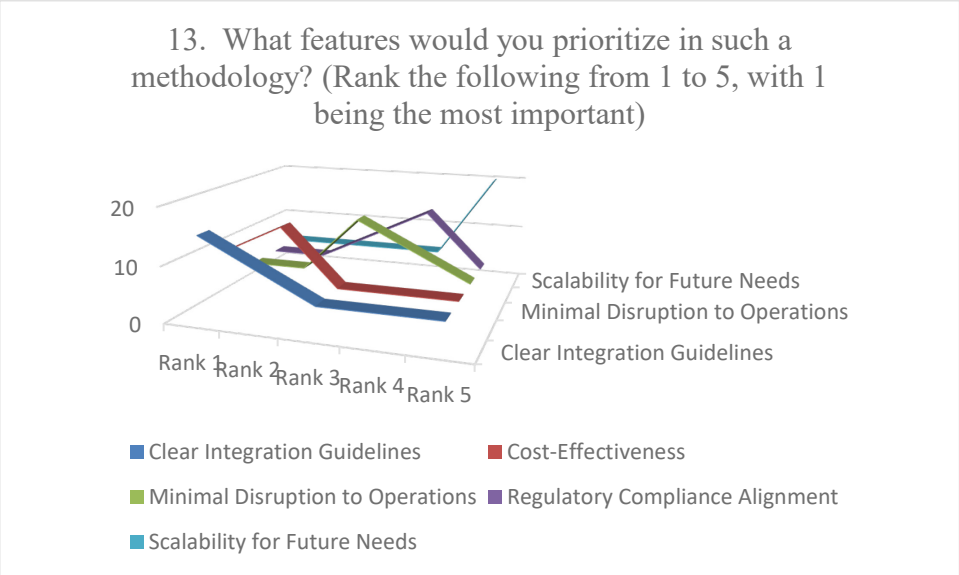

Figure 13. Question 13: Features to prioritize this methodology.

Following the strong support for a standardized methodology, the next question asked participants to rank the features they would prioritize in such a system. The ranking results, displayed in Figure 13, show that "Clear Integration Guidelines" was the highest priority, followed by "Cost-Effectiveness."

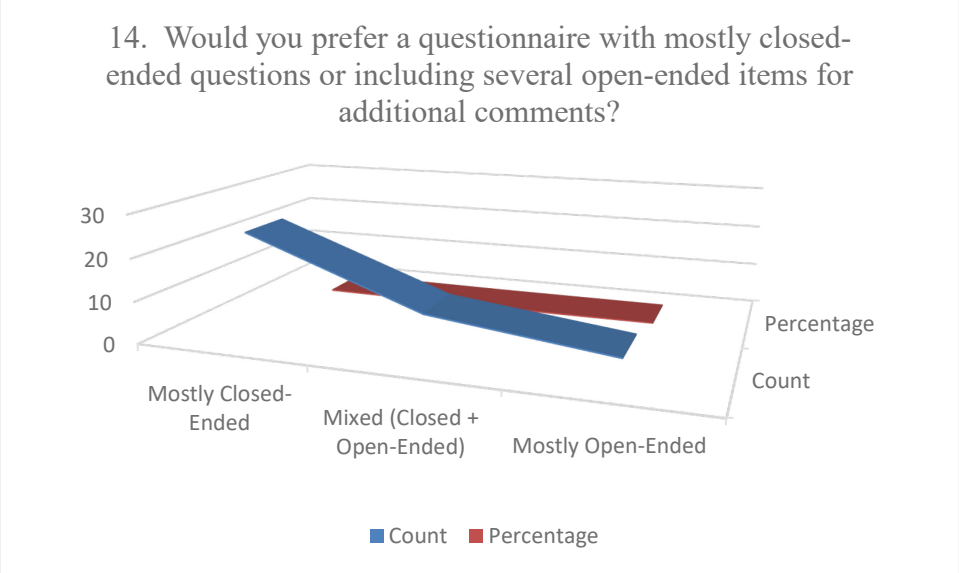

Figure 14. Question 14: preferring Closed-ended questions or open-ended for additional comments.

Finally, to gather feedback for future research, the questionnaire asked about the preferred format for such surveys. As seen in Figure 14, a majority of participants (62.5%) preferred a format with mostly closed-ended questions, though a significant 25% favored a mixed approach that also includes open-ended items for additional comments.

4.5 Findings from literature review

The integrated framework approach provides strategic clarity for addressing inconsistent risk management and fragmented security postures in laboratory environments (Shaaban and Schauer, 2025). The lack of cohesive strategy leads to disjointed cybersecurity measures across IT and OT systems, with

inconsistent implementation creating gaps in security control coverage (Ahmed and Tonoy, 2025).

NIST CSF 2.0 offers a flexible, high-level framework suitable for diverse industries, while NIST SP 800-82 and IEC 62443 provide detailed guidance for securing industrial automation and operational technology systems. This unified approach addresses both field-level vulnerabilities and policy-level governance (Biswas, 2024).

NIST SP 800-82 is particularly effective for OT laboratory environments, offering comprehensive guidance for securing Industrial Control Systems (ICS), Distributed Control Systems (DCS), and SCADA systems (Volk, 2024). The framework emphasizes access control, security architecture, system integrity, and incident response, providing a holistic approach to mitigating cybersecurity risks in OT environments (Menzel, Hurink, and Remke, 2025).

4.6 Results

The critical role of cybersecurity risk management is evaluated and administered from the literature review for safeguarding organizations against evolving digital threats. The commonly used frameworks include the NIST Cybersecurity Framework, ISO/IEC 27001, and HITRUST CSF, that provides a number or various structured methodologies for identifying, assessing, and mitigating the possible cyber risks. In other words, this can be said that the frameworks have to handle the flaws and criticism to manage lack of customization in industrial specific customization.

To integrate unique operational contexts for the existing processes, organizations frequently handle challenges for examining and implementing the framework under certain situations. In addition, there is a huge need to update and administrate the frameworks for enhancing sophistication in dealing with cyber threats and technological advancements. Therefore, it is identified from the organizational objectives and cybersecurity strategies to foster security

awareness in the organizational culture. The system and framework can enhance effectiveness through management efforts to mitigate identified risks.

Each mapped control was assessed and scored for effectiveness using the following rating system:

Effective – Fully implemented and enforced across the environment

Partially Effective – Implemented but with inconsistencies or coverage gaps

Not Effective – Either not implemented or non-functional in practice

These effectiveness scores were directly used to assign risk levels and guide remediation planning.

Control Effectiveness	No. of Controls	Description
Effective	179	Demonstrated through documentation, interviews, and field validation
Partially Effective	101	Operational but inconsistent; requires strengthening
Not Effective	29	Significant deficiencies; high-risk exposure

Table 1. Effectiveness Scores of Controls.

Identify (ID): Asset Management (ID.AM) scored the lowest (1.78) due to a lack of centralized inventories. Risk Strategy and Governance (ID. RA, ID.IM) were weak due to fragmented ownership and rare cross-functional reviews.

Protect (PR): Access Control (PR.AC) showed moderate implementation. Awareness and Training (PR.AT) scored the highest (3.00) with regular campaigns.

Detect (DE): Continuous Monitoring (DE.CM) and Adverse Events (DE.AE) domains were critically underdeveloped (average 1.67).

Respond (RS): Incident response roles and documentation existed but lacked drills and stakeholder coordination (avg 2.00).

Recover (RC): Recovery strategies were documented but lacked clarity, testing, and site readiness.

The maturity model was derived from the NIST CSF's Implementation Tiers:

Tier 1: Partial – Ad hoc risk management with undocumented or uncoordinated controls

Tier 2: Risk Informed – Risk decisions acknowledged, but inconsistently implemented

Tier 3: Repeatable – Controls are documented, tested, and managed

Tier 4: Adaptive – Controls adapt dynamically to threat intelligence and business priorities

ACME's average maturity across all domains was Tier 2.24, placing it between Tier 2 and early Tier 3, with highest maturity observed in training and policy enforcement, and lowest in monitoring, detection, and recovery functions.

The integration revealed overlapping controls, especially in areas such as:

- **Access Control (AC)**: Shared between all three frameworks
- **Incident Response (IR)**: NIST CSF and SP 800-82 overlap
- **Configuration Management (CM)**: Strong alignment between IEC 62443-3-3 and NIST SP 800-82

This mapping helped eliminate duplicative efforts and informed ACME's decision to centralize several functions such as logging, identity management, and security documentation. A centralized risk register linked to control effectiveness should be maintained. Weak domains require investment: Detect (SIEM, IDS), Respond (playbooks, escalation), Recover (BC/DR testing). Cross-framework implementation allows flexibility in adapting to healthcare regulations (HIPAA, GDPR) while ensuring ICS-specific coverage (Kortemaa, 2025).

The increase in the integration of cybersecurity risk management informs effectiveness in the strategic decision-making processes. This indicates the need for security considerations to inform better organizational strategy. In this regard, valuable guidance is offered for healthcare sector, and it is found that there is a need for industry-specific and more-specific approaches for addressing the complex and dynamic nature of contemporary cybersecurity challenges (Shaaban, and Schauer, 2025).

Access control and change management formed the backbone of any mature security program, yet the assessment revealed these foundational elements were poorly implemented across ACME's environment. Laboratory users possessed largely unrestricted abilities to alter system configurations without oversight or approval processes. This uncontrolled access destroyed any possibility of maintaining reliable audit trails and made it nearly impossible to trace the source of system problems or security incidents (Carello, 2025).

End users throughout the laboratory maintained full administrative rights to install any software they chose on critical diagnostic workstations. During interviews, multiple technicians confirmed they routinely downloaded and installed utility programs, browser extensions, and productivity tools without any approval process or security review. The continued use of shared accounts across departments represented another critical failure - these generic logins eliminated individual accountability and would make forensic investigation nearly impossible following any security incident. Most troubling was the complete absence of a defined separation of duties, with single individuals holding both operational and administrative privileges that should never coexist. These combined weaknesses earned a high-risk classification due to their potential for enabling both accidental mishaps and deliberate insider attacks (Volk, 2024).

Interviews and survey questionnaires with cybersecurity professionals revealed several key insights into current risk management practices. Participants consistently recognized cybersecurity as a strategic priority, emphasizing the need to align security initiatives with business objectives for comprehensive risk

mitigation. Professionals advocated for a proactive stance, including continuous monitoring and real-time threat of intelligence to anticipate emerging risks before they escalate into breaches. However, significant challenges emerged around resource allocation. Despite cybersecurity's critical importance, organizations often lack adequate budget and skilled personnel, which impedes effective strategy implementation. Additionally, participants stressed the need for ongoing training and awareness programs to foster a security-conscious organizational culture. While there is strong recognition of cybersecurity's importance, persistent challenges in resource allocation and continuous education must be addressed to enhance organizational resilience against cyber threats.

4.7 Discussion

The evolving landscape of cybersecurity necessitates a strategic approach to risk management, integrating both technological frameworks and human-centric strategies. While established frameworks like NIST, ISO 27001, and HITRUST provide structured methodologies for identifying and mitigating cyber risks, their effectiveness is contingent upon organizational context and resource allocation.

The NIST Cybersecurity Framework, for instance, is lauded for its comprehensive approach, encompassing identification, protection, detection, response, and recovery. However, its success hinges on the organization's commitment to continuous improvement and adaptation to emerging threats. Similarly, ISO 27001 offers a systematic approach to information security management, yet its implementation can be resource-intensive, posing challenges for organizations with limited budgets. HITRUST, with its focus on healthcare and related sectors, demonstrates a strong track record, with certified organizations experiencing a 99.41% breach-free rate in 2024.

Survey findings corroborate these insights, revealing that while organizations recognize the importance of cybersecurity frameworks, challenges persist in their implementation. Resource constraints, both financial and human, are

frequently cited as significant barriers. Moreover, a lack of advanced tools and technologies hampers the ability to address emerging cyber risks effectively. Training and awareness also emerge as critical components, with a significant portion of respondents acknowledging the need for continuous education to mitigate human-related vulnerabilities (Bilgin Metin et al., 2024).

Interviews with cybersecurity professionals further emphasize the necessity of aligning cybersecurity initiatives with organizational objectives. A proactive stance, characterized by continuous monitoring and real-time threat intelligence, is advocated to anticipate and counteract emerging risks. However, the challenge of resource allocation remains prevalent, with many professionals noting that despite the critical nature of cybersecurity, adequate resources are often lacking.

In conclusion, while established cybersecurity frameworks provide valuable guidance, their effectiveness is contingent upon organizational commitment, resource allocation, and continuous adaptation to the evolving threat landscape. Addressing challenges related to resource constraints, adopting advanced tools, and fostering a culture of continuous education are imperative steps toward enhancing cybersecurity resilience. Organizations must recognize that cybersecurity is not merely a technical issue but a strategic imperative that requires holistic and sustained efforts.

4.8 Reflection on Process and Professional Learning

Undertaking this cybersecurity risk assessment of ACME Inc.’s IoT/OT test lab environment has been a transformative learning experience. The exercise involved applying theoretical knowledge of NIST CSF 2.0, NIST SP 800-82, and IEC 62443 in real-world scenarios, illuminating the intersection of policy, technology, and human behavior within critical infrastructure. This experience has deepened the understanding of the complexities involved in securing hybrid healthcare environments and highlighted the importance of a structured approach to cybersecurity.

4.9 Lessons Learned on Framework Integration

One of the most important insights gained from this research was the complementary nature of the three frameworks. While NIST SP 800-82 focused on Industrial Control Systems (ICS)-specific control categories, IEC 62443 offered granular segmentation and defense-in-depth architecture principles. NIST CSF, on the other hand, served as an overarching maturity model that allowed for structured alignment and roadmap development. By integrating these frameworks, it was possible to map controls across both preventive and detective domains, conduct comparative maturity analysis using CSF tiers, and translate highly technical findings into business-relevant risks. This experience reaffirmed that no single framework is sufficient when evaluating modern hybrid environments. A layered approach enables better coverage, compliance, and communication across stakeholders.

4.10 Professional Growth and Stakeholder Engagement

Engaging with cross-functional teams during interviews and walkthroughs exposed the critical importance of stakeholder communication in cybersecurity. Translating framework controls into language that OT engineers, lab technicians, and compliance officers could understand was essential for buy-in and implementation success. Key takeaways include aligning technical assessments with operational workflows, ensuring that documentation is enforceable and understood, and communicating risk in terms of business continuity and service integrity. This learning has sharpened both technical risk analysis capabilities and stakeholder management skills, which are indispensable for any future cybersecurity leader.

4.11 Future Professional Applications

Looking ahead, the knowledge acquired through this project can be directly applied in roles related to Governance, Risk, and Compliance (GRC)

implementation in OT/IoT contexts, cybersecurity consulting for critical infrastructure, and Security Operations Center (SOC) maturity modeling and SIEM optimization. It also reinforces the value of cross-framework audits, especially in environments where regulations like HIPAA, NIS2, and ISO 27001 intersect with industrial cybersecurity.

4.12 Additional Insights and Domain-Specific Observations: IoT vs. OT Risk Differentiation

The distinction between IoT and OT in ACME's test lab setting was essential in shaping the remediation roadmap. IoT devices, such as telemetry sensors and environmental monitors, primarily serve as observational roles. Their compromise could result in false diagnostics or telemetry manipulation. OT systems, on the other hand, control laboratory workflows and physical operations. A failure here could bring diagnostic processes to a halt. Understanding these differences allowed tailored control strategies to address the unique risks associated with each domain.

4.13 Operational and Cultural Barriers in Implementation

During the assessment, resistance to change and lack of cross-functional coordination were consistent with themes. Engineering teams often lacked incentives to prioritize cybersecurity, viewing it as disruptive to productivity. Meanwhile, compliance personnel lacked technical visibility, hindering effective collaboration. Challenges identified included misaligned incentives between IT and OT teams and unclear accountability for shared assets. Proposed mitigation strategies involved establishing a Cybersecurity Steering Committee with representatives from each department who would align control metrics with operational Key Performance Indicators (KPIs). These measures aimed to foster a unified approach to cybersecurity across the organization.

4.14 Vendor and Third-Party Risk Insights

Vendor access was inconsistent and often over privileged, with several remote support tools lacking activity logging or session capture capabilities. This contradicted the principles of least privilege and traceability. Risks included potential backdoor entry by third parties and lack of enforcement regarding patch delivery timelines. Recommendations included using time-bound VPN access, requiring session recordings, and mandating third-party adherence to the organization's cybersecurity policies. Aligning these practices with frameworks like NIST 800-53 and IEC 62443 ensured a comprehensive approach to managing vendor and third-party risks.

4.15 Data Lifecycle and Information Protection Gaps

Data protection controls were not consistent across IoT and OT devices. While diagnostic result data was encrypted in transit, telemetry data remained unencrypted. Weaknesses observed included lack of standardized data classification and no tracking of data at rest beyond the main data center. Remediation strategies involved classifying data by sensitivity, encrypting data at rest and in motion, and periodically auditing data access logs. These measures aimed to enhance data security and compliance with frameworks like NIST CSF and IEC 62443.

4.16 Incident Response Preparedness Assessment

Although the organization had a documented Incident Response (IR) plan, it was not tested in OT environments. Furthermore, responsibilities during cyber events were not clearly defined for IoT/OT asset custodians. Gaps identified included a lack of tabletop or red team exercises and limited visibility of OT traffic in the Security Operations Center. The remediation path involved

including OT/IoT scenarios in IR drills and implementing passive OT traffic monitoring and baselining. Aligning these activities with NIST CSF and NIST SP 800-82 frameworks ensures a structured and comprehensive approach to incident response preparedness.

5 Conclusion

The comprehensive cybersecurity risk assessment conducted for ACME Inc.'s genomic diagnostic laboratory uncovered critical insights into the hybrid IoT/OT security landscape. Grounded in internationally recognized standards-NIST CSF 2.0, NIST SP 800-82, and IEC 62443, the investigation identified systemic weaknesses and provided a structured roadmap for remediation. Each section of this thesis has incrementally contributed to building a complete understanding of the lab's security posture, risks, and capabilities. Qualitative research design was employed in the study to understand the complex phenomenon related to the management of cybersecurity and handling risks in the field through evaluating the natural environment. It allowed us to examine the interaction of staff to maintain and perceive the working of IoT/OT devices in various constraints. In addition, it allowed to examine the relationships of vendor, safety concerns, regulatory obligations, framework expectations, and diagnostic throughput. However, the questionnaire and semi-structured interviews allowed capture of deep and broad perspectives.

The critical role of cybersecurity risk management is evaluated from the literature review for safeguarding organizations against evolving digital threats. The commonly used frameworks, namely the NIST Cybersecurity Framework, ISO/IEC 27001, and HITRUST CSF, provide several structured methodologies for identifying, assessing, and mitigating the possible cyber risks. In other words, this can be concluded that the frameworks must handle the flaws and criticism to manage lack of customization in industrial specific customization.

The challenges that organizations frequently encounter when examining and implementing the framework involve integrating unique operational contexts into the existing process. In addition, there is a huge need for updating and administrating frameworks for enhancing sophistication in dealing with cyber threats and technological advancements. Therefore, it is identified from the organizational objectives and cybersecurity strategies to foster security awareness in the organizational culture. The system and framework are

capable of enhancing effectiveness through management efforts to mitigate the identified risks.

Key conclusions drawn from this assessment are as follows:

Integrated Framework Application Yields Strategic Clarity: By leveraging NIST CSF's maturity tiers, NIST 800-82's industrial focus, and IEC 62443's layered defense approach, ACME's lab was evaluated across strategic, operational, and technical dimensions. The combination of these frameworks enabled a nuanced understanding of both policy-level governance and field-level vulnerabilities. IoT and OT Require Segregated but Interoperable Controls: The assessment established that IoT devices, being observational and data-oriented, are prone to unmonitored access, weak encryption, and misconfiguration. OT systems, meanwhile, are critical to laboratory operations and must be prioritized for availability, resilience, and fault tolerance. Segmenting these environments with dedicated policies is essential. Gaps are cultural as well as technical: operational inertia, lack of cybersecurity ownership, and inadequate collaboration between departments significantly contribute to risk. Cultural improvements, such as training, stakeholder alignment, and governance restructuring, are as vital as deploying technological safeguards.

Vendor and Third-Party Oversight is a Persistent Weakness: Inconsistent access controls, lack of session logging, and undefined cybersecurity expectations for vendors remain ongoing challenges. These issues can only be addressed through policy enforcement, updated contracts, and supply chain governance frameworks. Control Mapping highlights a rong road ahead: With 125 control gaps-29 of them high-risk-the lab's maturity level is in the early Tier 2 stage. While foundational practices exist, execution is inconsistent and largely reactive. A transition to Tier 3 (repeatable) and beyond will require sustained governance, investment in tooling, and a unified security architecture.

Resilience Hinges on Validated Continuity Planning: Business Continuity and Disaster Recovery (BC/DR) gaps were particularly concerning. The absence of

backup validation, failover capabilities, and disaster testing simulations places the lab’s operations and compliance at risk.

Maturity Is Achievable Through Road mapped Remediation: The prioritized work streams ranging from RBAC implementation and centralized logging to configuration management and SIEM deployment form a structured pathway for progressive maturity. Quick wins and long-term strategies have both been defined.

In conclusion, this thesis provides not only a diagnostic of ACME’s cybersecurity weaknesses, but also a transformative strategy rooted in industry standards. The integrated framework approach proved invaluable in enabling a complete and contextualized understanding of security across hybrid IoT/OT environments. If fully implemented, the recommendations will place ACME in a position of proactive defense, regulatory alignment, and operational continuity-a benchmark for secure healthcare diagnostics in the digital era.

References

Abergos, V.J. and Medjek, F., 2024. A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN. Journal of Cybersecurity and Privacy, 4(4), pp. 910-937. //doi.org/10.3390/jcp4040042 https://www.mdpi.com/2624-800X/4/4/42

Ahmed, I. and Tonoy, A.A.R., 2025. Cybersecurity In Industrial Control Systems: A Systematic Literature Review On AI-Based Threat Detection For SCADA And IOT Networks. ASRC Procedia: Global Perspectives in Science and Scholarship. https://doi.org/10.63125/1CR1KJ17 https://academia.edu/download/122973631/Ammar_Procedia_v1i1250115.pdf

Ansari, K., Lamb, C., Brulles, R.J., Cryar, R., Sanghvi, A., Hatic, D., Moiseyenko, Y., Varriale, R., Tsiropolou, E., Tsikteris, S. and Jun, M., 2024. Assessment and Coordination of EVSECybersecurity Standards (No. SAND2024-12438). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). https://www.osti.gov/servlets/purl/2462940

Biswas, H., 2024, August. Cyber Security in Power Grid Networks, At the Crossover Domain Intersection. In 2024 IEEE 5th India Council International Subsections Conference (INDISCON) (pp. 1-6). IEEE. DOI: 10.1109/INDISCON62179.2024.10744312 https://ieeexplore.ieee.org/abstract/document/10744312/

Bucelli, M., Blakseth, S.S., Andersson, L.E., Montañés, R.M. and Jøsang, A., 2025. Cybersecurity Risk Management for Digital Twins: A Case Study from the Offshore Oil and Gas Industry. Available at SSRN 5214450

Carello, M.P., 2025. Enhancing cybersecurity framework adoption: methodologies and techniques for contexts specific implementations (Doctoral dissertation, Sapienza University of Rome). https://tesidottorato.depositolegale.it/handle/20.500.14242/190279

Chairopoulou, S., 2024. Cybersecurity in industrial control systems: a roadmap for fortifying operations (Master's thesis, University of Piraeus). http://dx.doi.org/10.26267/unipi_dione/3975 https://dione.lib.unipi.gr/xmlui/handle/unipi/16553

Choi, B.H., 2025. NIST's Software Un-Standards. Geo. L. Tech. Rev., 9, p.65. https://heinonline.org/HOL/LandingPage?handle=hein.journals/gtltr9&div=5&id=&page=

Dohin, A., Zkik, K., Akilal, A., Omar, M. and Akli, H., 2025. Machine Learning for Industrial Iot Cybersecurity: A Systematic Review. Available at SSRN 5388573. http://dx.doi.org/10.2139/ssrn.5388573 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5388573

Edwards, J., 2024. A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=PiMeEQAAQBAJ&oi=fnd&pg=PR19&dq=An+Integrated+Risk+Management+Approach+Using+(NIST+CSF-2.0,+NIST+800-82,+IEC+62443)+Frameworks&ots=xqUGGlqCvj&sig=QsSCoa6cyVMGTm71GnEuRWjp4V8

Halawi Ghoson, N., Benfriha, K., Meyrueis, V., Guiltat, T. and El Zant, C., 2025. ShieldFlow: A novel framework for OT cybersecurity in the context of industry 4.0. International Journal of Information Security, 24(4), p.162. https://doi.org/10.1109/JAS.2024.124635 https://link.springer.com/article/10.1007/s10207-025-01083-3

Hossain, S.T., Yigitcanlar, T., Nguyen, K. and Xu, Y., 2024. The Role of Artificial Intelligence in Tackling Cybersecurity Threats in Smart Cities: A Systematic Review. Applied Sciences, 14(13), p.5501. https://doi.org/10.3390/electronics13214226 https://www.mdpi.com/2079-9292/13/21/4226

Kaliappan, P., Sudha, S. and Shankar, D., 2024, July. International Standards for Cybersecurity in Smart Devices for the Power Sector. In 2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST) (pp. 1-5). IEEE. https://ieeexplore.ieee.org/abstract/document/10717531 DOI: 10.1109/ICCIGST60741.2024.10717531

Kortemaa, J., 2025. Developing a venerability Management Service for an automation system based on the cyber resilience act.

https://trepo.tuni.fi/bitstream/handle/10024/228245/KortemaaJarkko.pdf?sequence=2

Lill, I.B., Doleh, Y. and Katzenbeisser¹, S., 2025, July. Exposing the Gaps: The State of Supply Chain Coverage in Current Security. In Information Security Education. Empowering People Through Information Security Education: 17th IFIP WG 11.8 World Conference, WISE 2025, Maribor, Slovenia, May 21–23, 2025, Proceedings (Vol. 742, p. 203). Springer Nature. https://books.google.com.pk/books?hl=en&lr=&id=SRh0EQAAQBAJ&oi=fnd&pg=PA203&dq=An+Integrated+Risk+Management+Approach+Using+(NIST+CSF-2.0,+NIST+800-82,+IEC+62443)+Frameworks&ots=T-1-UQ6SlJ&sig=7sJDSCDwW5E_91X1eMC0G5R0bc8&redir_esc=y#v=onepage&q&f=false

Malatji, M., 2023, January. The Influence of Organizational Cybersecurity Policies on Cybersecurity Maturity. In 2023 International Conference on Cyber Management and Engineering (CyMaEn) (pp. 117-122). IEEE. DOI: 10.1109/CyMaEn57228.2023.10051114 . https://ieeexplore.ieee.org/abstract/document/10051114

Menzel, V., Hurink, J. and Remke, A., 2025. Real-world case studies for a process-aware IDS. Energy Informatics, 8(1), p.86. . https://link.springer.com/article/10.1186/s42162-025-00545-1

Metin, B., Özhan, F.G. and Wynn, M., 2024. Digitalisation and Cybersecurity: Towards an Operational Framework. Electronics, 13(21), p.4226. https://doi.org/10.3390/electronics13214226 https://www.mdpi.com/2079-9292/13/21/4226

Mexis, N., Lill, B., Doleh, Y. and Katzenbeisser, S., 2025, May. Exposing the Gaps: The State of Supply Chain Coverage in Current Security Standards. Cham: Springer Nature Switzerland. . https://link.springer.com/chapter/10.1007/978-3-031-94924-1_14

Paul, A. A.(2025). Fortifying Maritime Cyber Defence Through Secure Ship Zones and Network Safeguards https://www.utupub.fi/bitstream/handle/10024/182475/Paul_Anjana_Thesis.pdf?sequence=1

Progoulakis, I., Dagkinis, I.K., Dimakopoulou, A., Lilas, T., Nikitakos, N. and Psomas, P.M., 2024. Cyber–Physical Security Assessment for Maritime Vessels: Study on Drillship DP System Using American Petroleum Institute Security Risk Analysis and Bow-Tie Analysis. Journal of Marine Science and Engineering, 12(10), p.1757. DOI:10.3390/jmse12101757 https://www.proquest.com/openview/f9b8e28e8a28f1ae3a0cc1c4144b79e6/1?pq-origsite=gscholar&cbl=2032377

Rahman, A., et al., 2024. Applications of Artificial Intelligence (AI) for Protecting Software Supply Chains (SSCs) in the Defense Industrial Base (DIB). SOAR CSIAC. https://csiac.dtic.mil/wp-content/uploads/2024/02/SOAR_CSIAC_Applications-of-Artificial-Intelligence-AI-for-Protecting-Software-Supply-Chains-SSCs-in-the-Defense-Industrial-Base-DIB_032724-contract.pdf

Reuben-Owoh, B. and Haig, E., 2025. A Systematic Review of Voluntary Cybersecurity Standards and Frameworks: B. Reuben-Owoh, E. Haig. International Journal of Information Security, 24(5), p.206.

Riurean, S., Fîță, N.D., Păsculescu, D. and Slușariuc, R., 2025. Securing Photovoltaic Systems as Critical Infrastructure: A Multi-Layered Assessment of Risk, Safety, and Cybersecurity. Sustainability, 17(10), p.4397.https://doi.org/10.1007/s10207-025-01121-0 https://www.mdpi.com/2071-1050/17/10/4397

Salihu, A. and Dervishi, R., 2024, October. Evaluating the Impact of Risk Management Frameworks on IT Audits: A Comparative Analysis of COSO, COBIT, ISO/IEC 27001, and NIST CSF. In 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE) (pp. 1-8). IEEE.DOI: 10.1109/ICECCE63537.2024.10823548 https://ieeexplore.ieee.org/abstract/document/10823548

Shaaban, A. and Schauer, S., 2025, May. Bridging Theory and Practice for Enhanced Cybersecurity Awareness in Critical Infrastructures. In Proceedings of the International ISCRAM Conference. DOI:

https://doi.org/10.59297/n12nnd95

http://ojs.iscram.org/index.php/Proceedings/article/view/144

Sishuba, T., Edoun, E.I. and Pradhan, A., 2024. A Systematic Review of the Implementation of IT and OT Cybersecurity Standards in an IT/OT Converged Environment. In 7th European Industrial Engineering and Operations Management Conference (IEOM). DOI: 10.46254/EU07.20240093 https://ieomsociety.org/proceedings/2024germany/93.pdf

Volk, M., 2024. A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures. Electrotechnical Review/Elektrotehniski Vestnik, 91(3). https://ev.fe.uni-lj.si/3-2024/Volk.pdf

Weitoish, T., 2025. US Cybersecurity and Enhancing SCADA Systems and Critical Infrastructures (Doctoral dissertation, Capitol Technology University). https://www.proquest.com/openview/327fae09c194ed554970a406455446e8/1?pq-origsite=gscholar&cbl=18750&diss=y

Search | *CSRC*. (2026). Nist.gov. https://csrc.nist.gov/publications/draft-pubs#800-82r2

Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics*, *13*(21), 4226. https://doi.org/10.3390/electronics13214226

Agenda Center. (2026). Mylakealfred.com. https://www.mylakealfred.com/AgendaCenter

Appendix 1: Interview questions

- How do you currently align cybersecurity strategies with the business objectives of the diagnostic laboratory, especially considering patient safety, regulatory compliance, and operational continuity?

1. To what extent have you integrated NIST CSF 2.0, NIST SP 800-82, and IEC 62443 into your laboratory's cybersecurity program? What challenges have you faced in harmonizing these frameworks?
2. What metrics or indicators do you use in order **Cybersecurity** strategy forto measure the effectiveness of existing IoT/OT/IT controls in reducing risk, especially those specific to diagnostic lab operations?
3. How is responsibility for cybersecurity shared among different units (e.g. IT, OT, clinical engineering, lab management)? How do you ensure clear accountability?
4. What trade-offs do you find yourselves making between security, business continuity, and diagnostic throughput? How are decisions made in balancing these?
5. How do regulatory requirements (medical devices, data privacy, patient safety) influence your cybersecurity priorities and investment decisions?
6. Can you describe your expectations for a remediation roadmap or integrated methodology? What features (prioritization, feasibility, cost estimation, minimal disruption) would make it most useful for you?
7. In your view, how ready is the laboratory to respond to IoT/OT-specific cyber threats (e.g. attack surface from networked sensors, legacy OT devices)? What gaps do you perceive?
8. What stakeholder feedback or pilot testing would you consider sufficient validation for any proposed method or roadmap?
9. What organizational culture, training, or resource changes would be needed to support shifting from reactive incident response to proactive resilience and prevention?

Interview responses

Participant A:

1. “We ensure the cybersecurity strategy is tightly integrated with patient safety and diagnostic throughput. Any proposed control is assessed first for impact on sample processing times. Regulatory compliance, especially MHRA and GDPR, is embedded in policy. For operational continuity, we have fallback plans and redundant systems to avoid downtime.”

- “We have adopted some parts of CSF 2.0 for governance, IEC 62443 for OT device requirements, and SP 800-82 where our lab uses automation/industrial control systems. The main challenge is reconciling differences: IEC’s device level security vs SP 800-82’s process safety, and conflicting terminologies. Also, vendor lock-in some OT/IoT devices refuse firmware modifications.”

1. “We track mean time between failures, number of unpatched vulnerabilities per device, number of security incidents, and average time to patch. For IoT/OT-specific risk, we monitor number of unauthorized access attempts to OT segments, network latency / packet drops post-segmentation, and uptime of critical diagnostic instruments.”

- “We have a cybersecurity steering committee: lab management, IT head, OT engineering lead, and compliance. Clinical engineering handles device security; IT handles network/security on IT side. OT/IoT engineers are responsible for device security controls. Clear documentation exists, and responsibilities are tied to roles in job descriptions.”
- “Sometimes patching during working hours is too disruptive, so we schedule during off-peak hours, even if risk exposure is greater temporarily. Diagnostic throughput is prioritized over minor security enhancements when time is tight. Decisions are made via risk-assessment: consider impact on patients, cost, effort, then board approval.”

- “Regulations are very strong drivers. MHRA medical device regulation requires us to report vulnerabilities and maintain post-market surveillance. GDPR obliges us to ensure data confidentiality and privacy. Patient safety rules mean we cannot disable safety modes even if a security risk suggests altering a device’s default behavior.”
- “We expect a mitigation roadmap to be prioritized: start with high-impact, low-disruption controls. It should estimate cost and time, indicate dependencies, and legal/regulatory implications. Also, feasibility in terms of vendor cooperation, staff training, and minimal interruptions to diagnostic flow.”
- “Overall readiness is moderate. We have segmented networks and basic monitoring, but we lack advanced anomaly detection, full visibility into firmware versions on all OT/IoT devices. Legacy devices pose a large gap. We also lack reliable asset inventory for many sensors.”

2. “Pilot testing of proposed methodology in one operational unit would be sufficient initially. Stakeholders: clinical staff, lab management, engineering, IT. Validation metrics: reduction in known vulnerabilities, improved patch time, minimal disruptions post-implementation, audit compliance results.”
3. “We need a culture shift: security is not just an IT issue. Staff at all levels (OT engineers, lab technicians) need awareness training. More resources needed: dedicated OT security expertise, budget for replacement of legacy devices. Also improved governance: regular reviews, accountability, and aligning incentives so that staff value prevention over only reacting to incidents.”

Participant B:

- “We view cybersecurity as business enablers. Patient safety is not negotiable. Strategic investments are made with oversight from executive

leadership. We map cybersecurity strategy to reduce risk while ensuring diagnostic results are delivered accurately and on time."

- "We are partially compliant with all three frameworks. CSF covers our overall risk governance; IEC supports our vendor contracts and OT device security; SP 800-82 is referenced for ICS security in lab automation lines. Harmonizing is difficult: duplication of controls, different risk scales, misaligned requirements for device patching schedules."
- "Key KPIs include a number of unplanned device outages, compliance audit findings, time to respond to security incidents, number of devices failing security scans, and frequency of security reviews. For OT/IoT: count of devices without firmware vendor support, number of network segmentation violations."
- "Responsibility is split. The CISO owns an overall policy. OT engineering owns OT device security and operations. IT security handles networking, monitoring, and policy enforcement. Lab management ensures operational priorities are met. Accountability is maintained via quarterly reports to the board and through SLA-type agreements between units."
- "Trade-offs often involve cost vs security. We sometimes delay replacing legacy equipment because the cost and downtime would impact throughput. We sometimes reduce the scope of security testing if it delays the release of diagnostic assays. But for major risks we don't compromise patient safety comes first."

1. "Regulatory requirements dictate much of our priority. We must comply with UK MDR/IVDR / MHRA for medical devices; GDPR for data privacy; safety standards for diagnostics. They shape procurement, security requirements of vendors, and how rapidly we push security patches or upgrades."
2. "The roadmap should be phased: identify quick wins, then more involved changes. Prioritize based on risk, regulatory exposure, and operational criticality. Must include cost estimates, staff resource requirements, and clear timeline, with minimal disruption to services."

3. “We are reasonably prepared for common threats like unauthorized network access, but less so for supply chain threats or zero-day vulnerabilities in embedded OT devices. Legacy devices with proprietary firmware are a big concern. Also limited monitoring visibility in some OT zones.”

- “Feedback should come from all relevant functions: lab scientists, clinical engineering, IT, and regulatory affairs. Pilot testing should involve a small lab group before full rollout. Success metrics: performance impact negligible, security incidents reduced, compliance audit scores improved.”
- “We need to invest in the workforce: hire OT security specialists, and train existing staff. Strengthen cross-unit communication. Cultivate a culture that values security proactively, not waiting for incidents. Also build better incentives for security reporting.”

Participant C:

1. “From an engineering standpoint, the strategy is designed around device reliability, availability, and safety. We map control design to regulatory requirements and work with operations to schedule maintenance or updates with minimal interference.”
2. “We try to apply IEC 62443 device level requirements, SP 800-82 for process safety in lab control systems, and CSF for governance and high-level risk. Harmonizing is a struggle because OT devices often have restricted update capabilities; terms in frameworks conflict; sometimes no vendor support.”

- “We measure MTTR (mean time to repair), number of irregular network traffic events, and number of devices out of compliance during internal audits. Also track device downtime due to security interventions, so we can ensure throughput isn’t compromised.”

3. “Responsibilities are very clearly mapped: I handle OT/IoT devices; IT handles network; clinical engineering handles calibration and safety; lab

management signs off on any change that might affect diagnostic result timings. We have RACI charts to ensure accountability."

4. "Trade-offs: calibration validation vs updating firmware; sometimes a patch might affect measured accuracy, so we delay. We sometimes accept slightly lower security for significantly higher availability. Decisions are made collaboratively with risk scoring."
5. "Regulation pushes us: MHRA and UKCA device regulatory standards force us to maintain device security. Data protection rules require secure storage/transmission of lab data. Patient safety laws require that device modifications don't introduce hazards."

- "In the roadmap methodology, I'd like visibility on device classification, inventory, criticality, and dependency. Prioritization should consider risk, regulatory urgency, and ease of deployment. Minimal disruption is critical, so wherever possible, changes should be implemented outside diagnostic hours."
- "Readiness: we have many basic controls in place but lack advanced detection and response. Gaps: legacy OT/IoT devices, limited vendor transparency, limited logging/telemetry on some devices, no test environment for implementing updates."

6. "Stakeholder feedback from device users (lab technicians, diagnosticians), engineering, compliance, and vendor partners is necessary. Pilot tests on a single lab line or unit are useful. Evidence of success: seamless operations post-change, no increase in error rates, measurable reduction in vulnerabilities."
7. "Training lab staff to understand cybersecurity basics; OT engineers need deeper security training; better tools for device management and logging; more resources for continuous monitoring; stronger leadership support to give security priority even when throughput pressures exist."

Participant D:

- “We align cybersecurity strategy by mapping legal requirements (MDR, IVDR, GDPR) to security policy. Patient safety is central. Business objectives include maintaining accreditation, avoiding regulatory penalties, and ensuring continuous diagnostic service. So, strategy includes regulatory compliance, incident response, and uptime protection.”

1. “We use CSF 2.0 for risk governance; SP 800-82 inform ICS operational safety; and IEC 62443 for vendor/device security. Challenges: overlaps, unclear scope in device certification, some framework parts don’t consider diagnostic lab specificity, and some vendor resistance to letting us configure devices as needed.”
2. “We look at regulatory audit findings, number of non-conformities, time to close compliance gaps, percentage of devices tested for vulnerabilities, downtime caused by security events, and incident response times.”

- “Clear accountability is achieved via compliance, clinical engineering, and IT security. The regulation office owns regulatory risk; lab management owns operational risk. Cross-functional governance boards help ensure responsibility sharing and decisions are documented.”

3. “Trade-offs are most visible when implementing controls that could delay diagnostic delivery. For example, enhanced security monitoring might slow some devices or require taking them offline temporarily. We weigh cost, risk, regulatory exposure, and select controls with least impact on throughput.”

- “Regulations not only mandate certain controls but also enforce reporting of incidents. So, we prioritize investments that help us satisfy regulation (e.g. device security, data encryption) while also improving safety. Patient safety regulations often overrule pure cost considerations.”
- “Expect roadmap to be pragmatic. Early stages should cover high regulatory risk items, low cost, and low disruption. Later phases for more complex OT/IoT improvements. Features like cost estimation, risk-based

prioritization, vendor dependency mapping, and compliance mapping are essential."

- "We are somewhat ready: we have policies, audits, and some segmentation. But gaps: legacy devices, supply chain risks, lack of full visibility of IoT sensors, limited capability in incident detection for OT zones, limited budget for replacing non-compliant devices."

4. "Feedback from regulatory authorities, lab inspectors, clinical staff, and technicians. Pilot testing needs to demonstrate compliance and safety retention. Metrics such as audit pass rate, reduction in vulnerabilities, and user experience post-deployment."
5. "We need improved culture: security to be considered in procurement, device lifecycle, and daily operations. Training in regulatory obligations for technical staff. Need for dedicated resources: compliance, legal, security engineering. Leadership support to ensure security investment remains a priority."

Participant E:

1. "Clinical engineering ensures the safety and performance of medical/diagnostic devices. Our strategy bridges clinical and technical: we ensure devices meet validation standards, maintain calibration, and integrate security controls that don't interfere with diagnostic accuracy."
2. "We rely on IEC 62443 for device security, SP 800-82 for process control in lab automation. CSF is used more by leadership for risk management and audit. The harmonization is challenging because many medical device vendors certify under different standards, and legacy devices often can't support required firmware updates."
3. "We measure error rates, device downtime, number of security alerts vs false positives, patch roll-out success rate, compliance in internal safety/security audits, and user feedback about disruptions to diagnostic activities."

- “Clinical engineering takes responsibility for device safety and maintenance; IT handles networks; security policy is overseen by lab management. Accountability mapped through operational procedures and maintenance schedules. Any change affecting diagnostics must go through engineering review and signoffs.”

4. “Trade-offs: security measures must not impair diagnostic accuracy. Sometimes turning off non-essential communication on devices is restricted because of monitoring requirements. We sometimes delay patching until calibration can be re-verified. Balancing is done via risk assessment that includes consideration of diagnostic error or patient harm.”

- “Patient safety is regulated strictly. Device regulations require pre-market and post-market obligations. Data privacy influences how we transmit results. We must ensure any device firmware changes do not break calibration or validation that regulators require.”

5. “Remediation roadmap should indicate which devices are most critical, specify phased replacement of legacy devices, cost estimations, regulatory impact, minimal service downtime, and ideally vendor support or supply contracts for critical spare parts.”
6. “Readiness: good on paper, we have many managed devices, network isolation, audit procedures. Gaps: many small IoT sensors are not inventoried; limited logging on device firmware; seldom do we have test environments for OT patches.”

- “I think if we pilot the methodology in a single lab module, e.g. molecular diagnostics, it would show whether diagnostics accuracy is maintained while security improves. Feedback from diagnosticians about turnaround time, error rates, and staff satisfaction are important.”
- “Need regular training for engineering and technician staff in cybersecurity principles. More resource allocation for security tools and periodic maintenance. Need a mindset shift: security should be considered early in design or procurement, not retrofitted.”

Participant F:

- “In my role, we align cybersecurity with business objectives by mapping IoT device risk to lab workflows. Devices critical to patient diagnostics get the highest priority. Safety and compliance come first; operational continuity is ensured via redundancy and fallback systems.”

1. “We try to apply IEC for device security, SP 800-82 for lab OT processes, and CSF for policy & governance. Challenges: IoT devices often come from vendors that don’t provide necessary security patches; scale of devices makes inventory hard; frameworks assume high uniformity which we don’t have.”

- “We monitor the number of IoT devices with open vulnerabilities, time to patch, number of incidents per device class, network traffic anomalies, and percentage uptime of critical instruments. Also measure device failure rates attributable to security controls.”

2. “IoT security is a shared responsibility: device vendors, engineering, IT, and lab operations all have roles. We have responsibility matrices; incidents or non-compliance reported across units. Regular inter-department meetings help maintain accountability.”
3. “Trade-offs include delaying updates to avoid disrupting diagnostics; restricting device communication can reduce functionality; security scanning sometimes slows networks. We balance via risk scoring and test pilots of security changes before full deployment.”

- “Regulations push us to use secure communications, incident reporting, and ensure devices are safe for clinical use. Device regulations and data protection both impose obligations. Also, reimbursement or certification may depend on cybersecurity posture.”

4. “The remediation roadmap should provide clarity on which device types to prioritize, cost & vendor dependency, fallback options, timelines, and minimal disruption to diagnostics. Also be dynamic: adaptable if threat landscape or regulatory demands change.”

5. “We are partially ready: network segmentation and device firewalls are in place, but detection and response in OT/IoT space are weaker. Gaps: legacy IoT sensors, limited telemetry, lack of unified monitoring platform, capacity to respond 24/7.”
6. “Pilot testing in a representative lab unit(s), feedback from engineering, clinicians, device users. Metrics: reduction in incidents, patch compliance, minimal diagnostic delays, maintained reliability of device performance.”
7. “We need frequent security awareness training; build expertise in OT/IoT systems; invest in security tools; leadership support for investing in resilience; embed security in procurement contracts, lifetime maintenance of devices.”

Participant G:

- “We align cybersecurity strategy by coordinating clinical leads to avoid impacting diagnostic error rates or turnaround time. Our IT strategy includes regulatory obligations, business continuity plans, and contingency for system outages.”
- “We have CSF embedded risk policy, SP 800-82 in lab automation control software, and references to IEC for contract terms with device vendors. We struggle with framework parts that conflict or are vague, especially the device behavior clauses in IEC vs SP 800-82’s process safety parts.”
- “We measure system uptime, number of security patches applied on schedule, incidents of unauthorized access, and compliance audit scores. For diagnostic lab operations: how many devices failed availability requirements, time to recover, and data integrity incidents.”

1. “Cybersecurity responsibilities: IT handles network, cyber policy; clinical engineering handles device hardware; lab management owns operations and service delivery. We use SLAs, and accountability is tracked through incident tracking and performance reports.”

- “The biggest trade-offs are between patching frequency vs downtime and adding security monitoring vs performance for diagnostic instruments. Decisions made via risk acceptance meetings, if cost or disruption too high, we find compensating controls.”

2. “Regulatory requirements are central. We can’t deploy updates that break compliance. Data privacy laws mean we must encrypt data in transit and at rest. Medical device regulation means any firmware change must be validated. Patient safety overrides cost concerns.”
3. “Roadmap should include device inventory, classification of criticality, vendor assessment, cost/time of changes, risk reduction estimates, minimal diagnostic disruption, alignment with regulatory deadlines.”
4. “Readiness is mixed: strong in IT side, weaker in OT/IoT. Gaps: lack of visibility of networked sensors, some older devices unsupported, weak monitoring/logging in OT subnets, insufficient threat intelligence for IoT threats.”

- “Stakeholder feedback should include lab users, engineers, clinicians, and regulatory affairs. Pilot in one lab area, measure performance, error rate, security incident rate, user satisfaction, and regulatory compliance metrics.”

5. “Need culture of collaboration, training IT and clinical staff, allocate budget, better tools, leadership buy-in to make security a priority, integrate security into procurement and lifecycle planning.”

Participant H:

1. “Our strategy is driven by ensuring research diagnostics are reproducible, safe, timely, and compliant. Cybersecurity controls are designed not to impede experimental workflows, but to ensure data integrity and safety.”

- “We use parts of all three frameworks: CSF for risk maturity, SP 800-82 for automation and OT safety, IEC 62443 for new device procurement.

Challenge: research labs change equipment rapidly; older equipment is often non-standard; documentation often lacking."

2. "Metrics: number of security policy violations, audit findings, instrument availability, rate of failed validation runs, time to isolate compromised devices. Also researcher satisfaction if security controls are causing delays."

- "Responsibility: lab management, IT security, and engineering share duties. We hold regular meetings where cross-team accountability is reviewed. Roles are defined in project charters, and change approvals require multiple signoffs."

3. "Trade-offs: for example, restricting remote access to devices sometimes slows collaboration; applying strict controls can delay experiments or new test deployments. We try to apply security in phases, allow temporary exceptions with compensating controls."
4. "Regulation in research diagnostics is somewhat less severe than clinical diagnostics, but data privacy and safety regulations still matter. Funding requirements often require compliance. We ensure data handling meets GDPR; some experiments require MHRA oversight if using diagnostic kits."

- "We want an integrated methodology that can flex to different research units, show high-impact, low-cost steps first, including vendor compatibility, minimal disruption. Also clear mapping of framework controls to lab workflow."
- "Readiness: Moderate. We have good procedures and policies; monitoring is less mature. Gaps: legacy devices, ad-hoc IoT deployment in small labs, limited staffing for continuous monitoring."

5. "Pilot studies in specific research units; feedback from researchers, engineering, safety officers. Validation would include security improved, minimal delays in experiments, positive researcher feedback, cost estimates that are realistic."

6. “Training of all lab staff in cybersecurity; better documentation; dedicated support for cybersecurity; recognizing security in performance measures; leadership that communicates security importance.”

Participant I:

1. “From network side, we align cybersecurity with business by ensuring that network latency, device connectivity, and diagnostic traffic are prioritized. Cybersecurity controls are assessed by their impact on network performance and uptime, and regulatory compliance is baked in through audits.”
2. “We use CSF for governance and risk scoring, IEC 62443 for network and device hardening, SP 800-82 for operational safety in automation. The challenge is that some device vendors don’t support secure protocols; some frameworks assume patch-cycles we cannot meet because device uptime is critical.”
3. “Metrics: network downtime, packet loss or latency induced by security measures; number of non-encrypted communications; number of audit findings; time to isolate network faults; detection/response time to network intrusion in OT subnets.”

- The “IT department handles networks; OT team handles device-level connectivity; lab management oversees overall service level. We define responsibilities in network diagrams and operational plans; incidents are logged, owners assigned immediately.”

4. “Trade-offs: security measures that introduce latency (e.g. deep packet inspection) may slow diagnostics; shutting off ports for security may break functionality; patching may require a device reboot that we cannot do mid-procedure. We often go for network isolation, limiting exposure rather than full shutdown.”

- “Regulatory influence is high: device communication security is required by medical device laws; data privacy requires secure handling; failures to

meet regulations can lead to withdrawal of certification. These drive our priority list."

5. "Roadmap should lay out which network segments / devices to isolate first, cost of upgrades, timeline, test phases, minimal disruption windows, fallback procedures. Also include regulatory mapping and vendor dependencies."
6. "Readiness: decent, but we lack full threat detection on the OT network; logging is sparse on some devices; legacy protocols are used; no central OT security operations center; limited continuous monitoring."
7. "Stakeholder feedback from device users, lab operations, engineering; pilot testing in a smaller OT network segment; metrics: no drop in throughput, network stability, security incident occurrence; ease of maintenance."
8. "Need more training in OT-network security; better tools for network visibility; more staff dedicated to OT security; culture where network changes are reviewed for security early; leadership to commit to resources and budget."

Participant J:

1. "Our alignment is through documentation, validation, and QA processes. Cybersecurity strategy must ensure that diagnostic results are reliable, safe, and compliant. QA cycles include cybersecurity checks; business objectives around quality, safety, and regulatory compliance guide strategy."
2. "We have incorporated elements of CSF (risk management, governance), SP 800-82 (operational safety where systems are industrial or automated), IEC 62443 (vendor/device security during procurement). Difficulties come in gaps in device vendor documentation; some controls are not applicable to older devices; resource constraints."

3. “Metrics: number of audit non-conformities, corrective actions outstanding, number of validated devices with full security configuration, percent compliance to internal policy, incident frequency, downtime during diagnosis, quality error rate.”
4. “QA works with clinical engineering and IT; device maintenance, training, policy enforcement shared. Accountability tracked via QA reports; root-cause analyses assign responsibility; management reviews assume oversight.”
5. “Trade-offs: sometimes security protocols add steps to QA or validation which slows release of diagnostic reports; sometimes controls might change device functionality slightly, requiring revalidation. We make decisions via QA board, weighing risk severity vs impact on quality/speed.”
6. “Regulations are central: compliance with ISO standards, medical device regulations, data protection, patient safety laws all influence investments. QA functions often ensure those investments are mapped to regulatory requirements.”
7. “Expect roadmap to include crosswalk of required regulatory vs framework controls, cost/time/trouble to achieve each, clear order of implementation that considers quality and regulatory risk, minimal impact on diagnostic release schedules.”
8. “We are ready in many procedural and policy areas but less so in technical monitoring and response. Gaps: real-time telemetry, firmware integrity checking, legacy device vulnerability, vendor cooperation for security patches.”
9. “Pilot in a QA-critical diagnostic procedure / lab unit; feedback from technical staff, QA, and clinicians; success metrics: minimal errors, maintained quality, measurable security improvement.”
10. “Need continual awareness training, integrate security into validation protocols, more resources for QA & cybersecurity collaboration, leadership buy-in so that security is part of quality metrics, not afterthought.”

Closed-ended questionnaire

1. **How well does your cybersecurity strategy align with patient safety objectives?**
    a. ☐ Very Poorly
    b. ☐ Poorly
    c. ☐ Neutral
    d. ☐ Well
    e. ☐ Very Well
2. **How well does your cybersecurity strategy align with regulatory compliance requirements (e.g., MHRA, UKCA, GDPR)?**
    a. ☐ Very Poorly
    b. ☐ Poorly
    c. ☐ Neutral
    d. ☐ Well
    e. ☐ Very Well
3. **How well does your cybersecurity strategy support operational continuity (e.g., avoiding diagnostic downtime)?**
    a. ☐ Very Poorly
    b. ☐ Poorly
    c. ☐ Neutral
    d. ☐ Well
    e. ☐ Very Well
4. **Which of the following cybersecurity frameworks have you formally implemented? (Select all that apply)**
    a. ☐ NIST Cybersecurity Framework (CSF)
    b. ☐ NIST SP 800-82 (Guide to Industrial Control Systems Security)
    c. ☐ IEC 62443 (Industrial Automation and Control Systems Security)

d. ☐ ISO/IEC 27001 (Information Security Management Systems)

e. ☐ Other: _____

f. ☐ None

5. **How challenging is it to harmonize cybersecurity controls across these frameworks?**

a. ☐ Not Challenging

b. ☐ Slightly Challenging

c. ☐ Moderately Challenging

d. ☐ Very Challenging

e. ☐ Extremely Challenging

6. **Which metrics do you currently use to assess the effectiveness of IoT/OT/IT cybersecurity controls? (Select all that apply)**

a. ☐ Number of Security Incidents

b. ☐ Time to Patch Vulnerabilities

c. ☐ System Uptime

d. ☐ Compliance Audit Results

e. ☐ User Access Control Logs

f. ☐ Other: _____

7. **How effective are your current cybersecurity controls in mitigating risks specific to diagnostic lab environments?**

a. ☐ Not Effective

b. ☐ Slightly Effective

c. ☐ Moderately Effective

d. ☐ Very Effective

e. ☐ Extremely Effective

8. **Is responsibility for cybersecurity clearly defined and shared among IT, OT, clinical engineering, and lab management?**

a. ☐ Yes

b. ☐ No

c. ☐ Partially

9. **How often do you make trade-offs between cybersecurity measures and diagnostic throughput?**

a. ☐ Never

b. ☐ Rarely

c. ☐ Sometimes

d. ☐ Often

e. ☐ Always

10. **How prepared is your organization to respond to cybersecurity incidents affecting IoT/OT systems?**

a. ☐ Not Prepared

b. ☐ Slightly Prepared

c. ☐ Moderately Prepared

d. ☐ Very Prepared

e. ☐ Extremely Prepared

11. **Which of the following gaps do you perceive in your cybersecurity readiness? (Select all that apply)**

a. ☐ Lack of Asset Inventory

b. ☐ Insufficient Network Segmentation

c. ☐ Inadequate Incident Response Plans

d. ☐ Limited Staff Training

e. ☐ Outdated Legacy Systems

f. ☐ Other: _____

12. **Would you support the adoption of a standardized methodology to integrate cybersecurity frameworks and controls?**

a. ☐ Yes

b. ☐ No

c. ☐ Maybe, with modifications

13. **What features would you prioritize in such a methodology? (Rank the following from 1 to 5, with 1 being the most important)**

    a. ___ Clear Integration Guidelines

    b. ___ Cost-Effectiveness

    c. ___ Minimal Disruption to Operations

    d. ___ Regulatory Compliance Alignment

    e. ___ Scalability for Future Needs

14. **Would you prefer a questionnaire with mostly closed-ended questions or including several open-ended items for additional comments?**

    a. ☐ Mostly Closed-Ended

    b. ☐ Mixed (Closed + Open-Ended)

    c. ☐ Mostly Open-Ended

Questionnaire responses

1. **How well does your cybersecurity strategy align with patient safety objectives?**

Response Option	Count	Percentage
Very Poorly	2	5%
Poorly	3	7.5%
Neutral	10	25%
Well	15	37.5%
Very Well	10	25%

2. **How well does your cybersecurity strategy align with regulatory compliance requirements (e.g., MHRA, UKCA, GDPR)?**

Response Option	Count	Percentage
Very Poorly	1	2.5%
Poorly	2	5%
Neutral	8	20%
Well	18	45%
Very Well	11	27.5%

3. **How well does your cybersecurity strategy support operational continuity (e.g., avoiding diagnostic downtime)?**

Response Option	Count	Percentage
Very Poorly	3	7.5%
Poorly	4	10%
Neutral	9	22.5%
Well	14	35%
Very Well	10	25%

4. **Which of the following cybersecurity frameworks have you formally implemented? (Select all that apply)**

Framework	Count	Percentage
NIST Cybersecurity Framework (CSF)	25	62.5%
NIST SP 800-82	15	37.5%
IEC 62443	18	45%
ISO/IEC 27001	20	50%
Other: _____	5	12.5%
None	4	10%

5. **How challenging is it to harmonize cybersecurity controls across these frameworks?**

Response Option	Count	Percentage
Not Challenging	5	12.5%
Slightly Challenging	8	20%

Moderately Challenging	15	37.5%
Very Challenging	10	25%
Extremely Challenging	2	5%

6. **Which metrics do you currently use to assess the effectiveness of IoT/OT/IT cybersecurity controls? (Select all that apply)**

Metric	Count	Percentage
Number of Security Incidents	30	75%
Time to Patch Vulnerabilities	28	70%
System Uptime	35	87.5%
Compliance Audit Results	22	55%
User Access Control Logs	18	45%
Other: _____	6	15%

7. **How effective are your current cybersecurity controls in mitigating risks specific to diagnostic lab environments?**

Response Option	Count	Percentage
Not Effective	3	7.5%
Slightly Effective	5	12.5%
Moderately Effective	15	37.5%
Very Effective	12	30%
Extremely Effective	5	12.5%

8. **Is responsibility for cybersecurity clearly defined and shared among IT, OT, clinical engineering, and lab management?**

Response Option	Count	Percentage
Yes	20	50%
No	10	25%
Partially	10	25%

9. **How often do you make trade-offs between cybersecurity measures and diagnostic throughput?**

Response Option	Count	Percentage
Never	5	12.5%
Rarely	10	25%
Sometimes	15	37.5%
Often	7	17.5%
Always	3	7.5%

10. **How prepared is your organization to respond to cybersecurity incidents affecting IoT/OT systems?**

Response Option	Count	Percentage
Not Prepared	2	5%
Slightly Prepared	5	12.5%
Moderately Prepared	15	37.5%
Very Prepared	10	25%
Extremely Prepared	8	20%

11. **Which of the following gaps do you perceive in your cybersecurity readiness? (Select all that apply)**

Gap	Count	Percentage
Lack of Asset Inventory	18	45%
Insufficient Network Segmentation	12	30%
Inadequate Incident Response Plans	10	25%
Limited Staff Training	20	50%
Outdated Legacy Systems	15	37.5%
Other: _____	5	12.5%

12. **Would you support the adoption of a standardized methodology to integrate cybersecurity frameworks and controls?**

Response Option	Count	Percentage
Yes	30	75%
No	5	12.5%
Maybe, with modifications	5	12.5%

13. **What features would you prioritize in such a methodology? (Rank the following from 1 to 5, with 1 being the most important)**

Feature	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
Clear Integration Guidelines	15	10	5	5	5
Cost-Effectiveness	10	15	5	5	5
Minimal Disruption to Operations	5	5	15	10	5
Regulatory Compliance Alignment	5	5	10	15	5
Scalability for Future Needs	5	5	5	5	20

14. **Would you prefer a questionnaire with mostly closed-ended questions or including several open-ended items for additional comments?**

Response Option	Count	Percentage
Mostly Closed-Ended	25	62.5%
Mixed (Closed + Open-Ended)	10	25%
Mostly Open-Ended	5	12.5%