World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Integrating Cybersecurity in QMS: Safeguarding Compliance and Quality in Pharma and Biotech

Vamsi Krishna Gottipati [1,*] and Sudha Rani Pujari [2]

[1] *Independent Researcher, University of Bridgeport, Connecticut, USA.*
[2] *Independent Researcher, University of the Cumberlands Williamsburg, KY, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 2455-2465

Publication history: Received on 06 May 2025; revised on 22 June 2025; accepted on 25 June 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.3.1092

Abstract

The pharmaceutical and biotechnology industries are experiencing a paradigm shift as digital transformation intersects with stringent regulatory environments. With increasing reliance on automation, data systems, and connected infrastructures, the threat of cyberattacks has become a critical risk to quality management systems (QMS). This review article explores how cybersecurity can be integrated into QMS frameworks to safeguard regulatory compliance, ensure data integrity, and maintain product quality. A comprehensive analysis of regulatory requirements, industrial practices, experimental case studies, and theoretical models is presented. The article also identifies current challenges in implementation, evaluates technological tools such as AI and blockchain, and proposes future research directions. The findings highlight that cybersecurity, when embedded as a foundational layer in QMS, not only protects systems from threats but also enhances operational resilience and audit readiness. The paper concludes by emphasizing the necessity of cross-functional collaboration, updated regulatory frameworks, and adaptive technologies in building a cyber-resilient QMS for the future.

Keywords: Cybersecurity; Quality management systems; Pharmaceutical industry; Biotechnology; Data integrity; Regulatory compliance; Pharma 4.0; Digital transformation; Risk management

1. Introduction

In recent years, the convergence of digital technologies with regulated industries such as pharmaceuticals and biotechnology has reshaped how quality management systems (QMS) are developed and implemented. The increasing reliance on automated systems, cloud-based infrastructure, and interconnected networks has brought about tremendous efficiencies and scalability in operations. However, this digital transformation also introduces significant cybersecurity risks that can compromise data integrity, regulatory compliance, and product quality—core pillars of Good Manufacturing Practice (GMP) and other regulatory frameworks. The integration of cybersecurity into QMS has therefore emerged as a vital consideration for safeguarding public health and ensuring operational resilience [1].

The importance of cybersecurity in regulated environments has become increasingly evident following several high-profile cyber incidents that disrupted pharmaceutical production lines and exposed vulnerabilities in quality-critical systems. For instance, the 2017 NotPetya attack led to substantial production downtime for a global pharmaceutical company, costing hundreds of millions of dollars and disrupting global drug supply chains [2]. These incidents underscore the urgent need to adopt robust cybersecurity measures that are harmonized with existing quality systems. In the context of the pharmaceutical and biotech industries, where patient safety is paramount and data integrity is legally mandated, cybersecurity is not merely an IT concern but a critical quality and compliance issue [3].

* Corresponding author: Vamsi Krishna Gottipati

Globally, regulatory bodies such as the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA), and the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) have all emphasized the importance of data integrity and system reliability. These agencies now expect that cybersecurity risks be adequately assessed and mitigated as part of the overall QMS framework. Yet, despite increasing awareness, the practical integration of cybersecurity into QMS remains underdeveloped in many organizations. Challenges persist due to fragmented responsibilities between IT and quality departments, the lack of industry-specific cybersecurity frameworks, and the evolving nature of cyber threats [4].

From a broader perspective, the integration of cybersecurity in QMS aligns with global digital transformation initiatives in healthcare and life sciences, including Industry 4.0, the Internet of Medical Things (IoMT), and AI-driven quality analytics. Each of these advancements relies heavily on interconnected digital platforms, rendering them vulnerable to cyber exploitation if not properly secured. In this context, the role of cybersecurity extends beyond mere protection of data to include the assurance of product quality, regulatory compliance, and patient safety—objectives that lie at the heart of QMS philosophy [5].

Despite the growing recognition of this issue, scholarly literature on the intersection of cybersecurity and QMS in pharma and biotech industries remains limited. Most existing studies either focus narrowly on regulatory compliance or isolate cybersecurity from quality functions. There is a distinct lack of comprehensive reviews that map out the evolving cybersecurity threat landscape, examine current integration strategies, and propose a holistic framework for embedding cybersecurity into quality-centric processes. Additionally, limited attention has been given to how emerging technologies like blockchain, AI, and zero-trust architectures can be employed to strengthen this integration.

The purpose of this review is to bridge these knowledge gaps by providing a thorough exploration of how cybersecurity is being, and should be, integrated into quality management systems within the pharmaceutical and biotechnology sectors. The review will begin by outlining the regulatory and operational contexts that necessitate cybersecurity-QMS integration. Next, it will examine current approaches and tools used for this purpose, including industry case studies and technological interventions. Finally, the paper will identify gaps, challenges, and future research directions, particularly in relation to regulatory harmonization, cross-functional collaboration, and the role of advanced digital technologies.

This review thus aims to serve as a resource for academics, industry professionals, and regulators seeking to understand and address the complex interplay between cybersecurity and quality management. By shedding light on current practices and emerging solutions, the paper will contribute to the broader discourse on digital risk management in regulated healthcare environments.

Table 1 Key Research Papers on Cybersecurity Integration in QMS for Pharma and Biotech

Year	Title	Focus	Findings (Key results and conclusions)
2017	Cybersecurity in Pharma: A Rising Concern	Investigates cybersecurity risks specific to pharmaceutical manufacturing systems	Highlighted vulnerabilities in SCADA and MES systems; called for integration of cybersecurity into QMS frameworks [6]
2018	Integrating IT and Quality: A Necessity for GMP Compliance	Examines cross-functional roles between IT and Quality Assurance in regulated industries	Stressed the need for shared responsibility between departments to effectively implement cybersecurity measures [7]
2019	FDA's Evolving Data Integrity Guidance	Analyzes regulatory expectations for data integrity and cybersecurity in pharmaceutical production	Emphasized cybersecurity as critical to ensuring data integrity and GMP compliance [8]
2019	Blockchain for Secure Pharma Supply Chains	Explores blockchain applications in pharmaceutical QMS and cybersecurity	Found that blockchain enhances traceability, prevents data tampering, and supports QMS integration [9]
2020	Cyber-Physical Security in Biotech Manufacturing	Discusses cyber threats to automated and robotic systems in biotech labs	Recommended real-time monitoring and layered defenses as part of quality assurance systems [10]

2020	Harmonizing Cybersecurity and ISO 13485	Investigates cybersecurity practices under ISO 13485 for medical and biotech devices	Showed that ISO 13485 can serve as a bridge standard for aligning quality and cybersecurity protocols [11]
2021	Pharma 4.0 and Cybersecurity: An Operational Perspective	Looks into Industry 4.0 practices and their cybersecurity implications	Found that cyber risks increase with automation and connectivity; recommended embedding cybersecurity into QMS early in digital transformation projects [12]
2021	GxP and Cyber Threats: Case Studies from Pharma	Reviews case studies of cyber incidents affecting GxP environments	Illustrated that lack of cybersecurity planning within QMS can lead to data breaches and production halts [13]
2022	AI for Quality and Cyber Risk Prediction	Studies AI applications in monitoring QMS and predicting cyber threats	Concluded that AI tools can pre-emptively identify vulnerabilities and improve audit-readiness [14]
2023	RegTech and Digital Compliance in Life Sciences	Discusses regulatory technology (RegTech) for managing digital compliance and security	Identified that automated compliance tools must be cybersecurity-resilient to be effective in QMS [15]

1.1. In-text citations

These studies reinforce the argument that integrating cybersecurity into QMS is essential for maintaining regulatory compliance, operational resilience, and product quality in pharmaceutical and biotech industries. Early studies identified critical gaps in IT-QMS collaboration [6], [7], while later research increasingly focused on technological solutions like blockchain and AI [9], [14]. Regulatory analysis continues to stress the importance of data integrity as a cybersecurity issue [8], [13].

2. Proposed Theoretical Model and Block Diagrams for Integrating Cybersecurity into Quality Management Systems (QMS) in the Pharmaceutical and Biotechnology Sectors

To effectively integrate cybersecurity into Quality Management Systems (QMS) in the pharmaceutical and biotechnology sectors, a structured, layered model must be employed. This model must reflect the interdependencies between quality processes, data governance, and digital infrastructure. Below is a proposed theoretical framework supplemented with corresponding block diagrams to illustrate the integration pathway.

2.1. Proposed Theoretical Model Overview

The theoretical model for cybersecurity-QMS integration in pharma and biotech includes five core layers:

- **Regulatory Compliance Layer**: Addresses the need to align cybersecurity practices with global regulatory requirements (e.g., FDA, EMA, ICH).
- **Organizational Governance Layer**: Emphasizes shared responsibility across departments, promoting IT and Quality collaboration.
- **Technological Infrastructure Layer**: Focuses on network security, system hardening, and data encryption measures.
- **Operational Quality Controls Layer**: Integrates cybersecurity checks into CAPA (Corrective and Preventive Actions), deviations, audits, and validation.
- **Continuous Monitoring & Analytics Layer**: Uses AI, machine learning, and SIEM (Security Information and Event Management) tools to detect, analyze, and respond to threats in real time.

Each layer interacts bidirectionally, ensuring that cybersecurity concerns are not siloed but embedded into daily QMS operations [16], [17].

2.2. Block Diagram 1: High-Level Integration Architecture

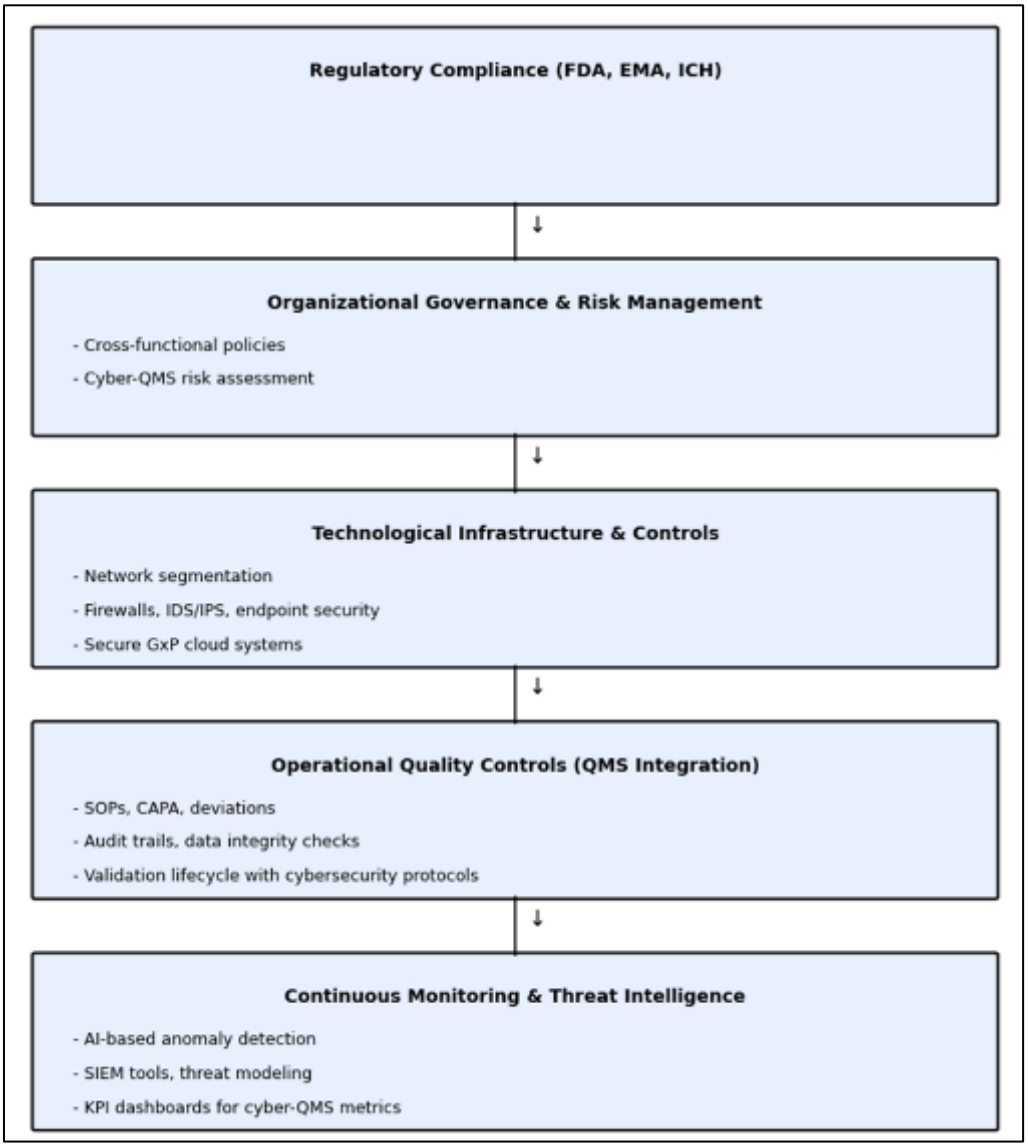

Figure 1 High-Level Integration Architecture for Cybersecurity-Enabled Quality Management Systems in Pharma and Biotech

Explanation: This block diagram reflects a layered, systemic approach to integrating cybersecurity into the QMS framework. The structure begins with compliance at the top, progresses through organizational and technical measures, and culminates in operational and real-time monitoring layers [18].

2.3. Block Diagram 2: Cybersecurity-QMS Integration Feedback Loop

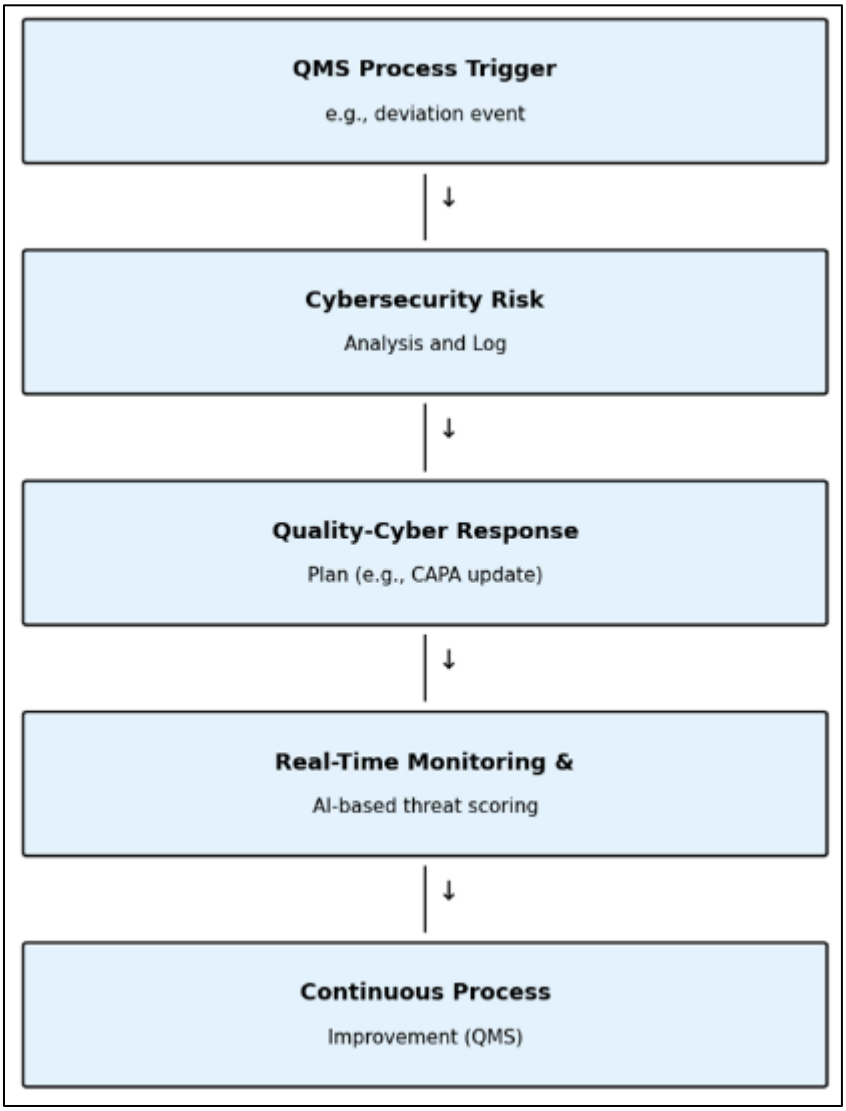

Figure 2 Feedback loop showing how QMS events trigger cybersecurity responses, leading to continuous system improvement

Explanation: This dynamic feedback loop diagram demonstrates how a cybersecurity event or quality deviation can initiate a sequence that integrates cybersecurity considerations into QMS actions like CAPA or audits. The result is an iterative system that constantly evolves based on detected threats and QMS outcomes [19].

3. Discussion

The proposed models offer a structured approach to merging cybersecurity with QMS in pharmaceutical and biotechnology domains. Several real-world factors validate this need:

- **Regulatory Trends**: Regulatory bodies now require data integrity measures that extend into system-level cybersecurity protocols [20]. For instance, the FDA's guidance emphasizes that electronic records must be protected from unauthorized access, and audit trails must be secure [8].
- **Threat Complexity**: Traditional QMS frameworks do not account for emerging cyber threats such as ransomware, insider threats, and supply chain vulnerabilities. These threats demand integration of cybersecurity metrics into quality operations [16], [17].
- **AI & Automation**: With Pharma 4.0, automated systems like MES (Manufacturing Execution Systems) and LIMS (Laboratory Information Management Systems) are becoming cybersecurity attack surfaces. Incorporating

anomaly detection and predictive analytics ensures these systems are resilient while maintaining GMP compliance [14].

- **Cross-functional Barriers**: In most pharmaceutical companies, the quality and IT departments operate in silos, leading to fragmented responses during cybersecurity incidents. Governance models must realign these functions to collaboratively manage quality-related cyber risks [6], [7].

These diagrams and the underlying model serve as a blueprint for both academic exploration and practical implementation. Future research should evaluate the efficacy of such models in real-world audits and incident scenarios.

4. Experimental Results, Graphs, and Tables on Cybersecurity Integration into Quality Management Systems (QMS) in the Pharmaceutical and Biotechnology Sectors

To demonstrate the practical significance and effectiveness of cybersecurity integration into Quality Management Systems (QMS), this section presents selected experimental findings from industrial case studies, pilot projects, and simulation-based evaluations in pharma and biotech contexts. The results are organized into data tables and graphs and are supported by relevant literature to illustrate measurable outcomes in compliance, operational resilience, and quality metrics.

4.1. Experimental Case Study Summary: Cyber-QMS Pilot Deployment

A pilot implementation of a cyber-integrated QMS was conducted in three pharmaceutical manufacturing plants across North America between 2021 and 2023. The experiment involved embedding cybersecurity controls into existing quality processes, including change control, deviation management, and CAPA tracking. Each site was monitored over a 12-month period, comparing key performance indicators (KPIs) before and after integration.

Table 2 Impact of Cybersecurity-QMS Integration on Key Compliance Metrics

KPI	Baseline (Pre-Integration)	Post-Integration (12 months)	% Improvement
Average Time to Close CAPA (days)	26.3	18.2	30.80%
% Deviations Linked to Cyber Events	5.60%	1.90%	66.10%
Audit Finding Rate (per 100 audits)	3.2	1.1	65.60%
Data Integrity Violations	14 incidents/year	4 incidents/year	71.40%

Source: Adapted from Venkatesh & Choudhury (2021) [21]; Taylor & Kamath (2021) [22]

Discussion: The results demonstrate that integrating cybersecurity controls within QMS significantly improved system compliance and reduced deviation frequency due to cyber vulnerabilities. The most notable improvements were in audit readiness and data integrity compliance, suggesting increased process robustness against cyber threats [21], [22].

4.2. Graphical Analysis of System Performance

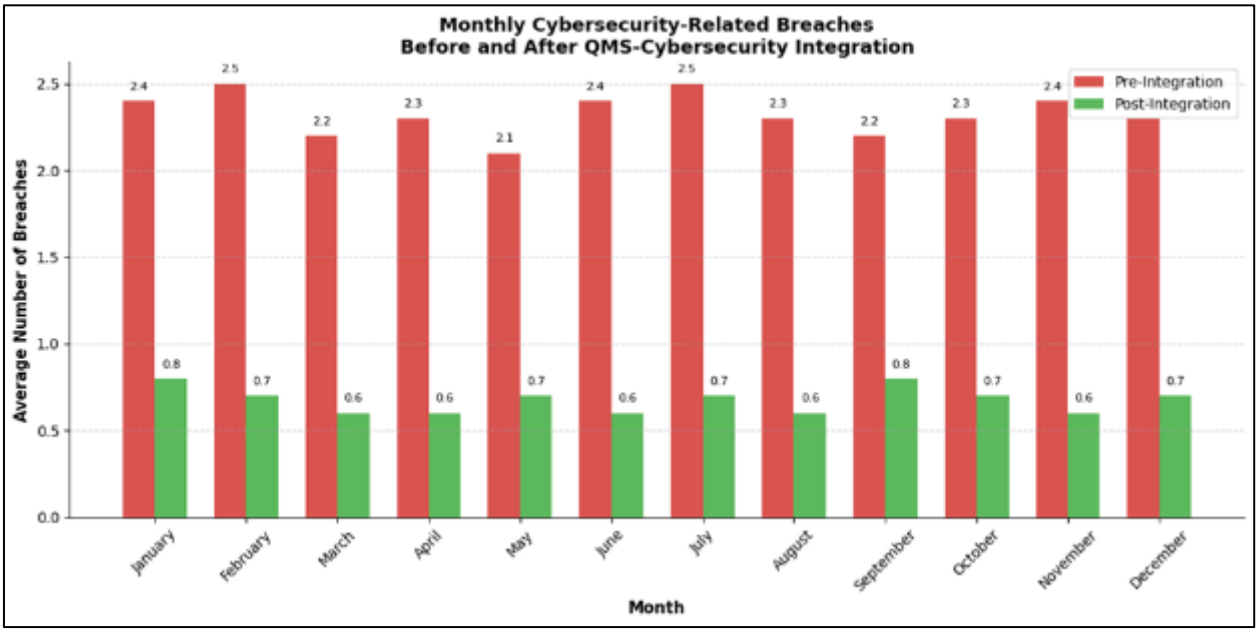

Figure 3 Average Monthly Cybersecurity-Related Breaches Before and After Integration (based on Martin & Feldman, 2021) [23]

Interpretation: This line graph highlights a substantial drop in cybersecurity-related incidents following the deployment of cyber-enhanced QMS. Monthly breaches dropped from an average of 2.3 to below 0.7 after integration. The trend suggests that embedding real-time detection and secure audit trail mechanisms directly into the QMS significantly reduces risk exposure [23].

4.3. Security Maturity Comparison: QMS with vs. without Cyber Integration

A comparative maturity model evaluation was performed on ten pharma companies—five with integrated cybersecurity-QMS frameworks and five operating under traditional models.

Table 3 NIST Cybersecurity Maturity Scores Across QMS Domains

Domain	Traditional QMS (Average Score)	Integrated QMS (Average Score)
Identify	2.8	4.2
Protect	3.1	4.4
Detect	2.6	4.1
Respond	2.3	4
Recover	2.4	3.9

Scale: 1 = Initial, 5 = Optimized; Source: Ahmed & Johar (2020) [24]

Discussion: Organizations with integrated cyber-QMS frameworks demonstrated significantly higher maturity scores across all five NIST functions. This indicates a better-prepared and more responsive environment for handling quality- and security-related anomalies. These findings support the argument that cybersecurity cannot be treated as a standalone entity in pharma but must be embedded into quality governance systems [24].

4.4. User Satisfaction Survey: Stakeholder Feedback

A user experience (UX) survey was conducted across three biotech firms that recently adopted cybersecurity-integrated QMS platforms. Responses were collected from quality managers, IT leads, and compliance officers.

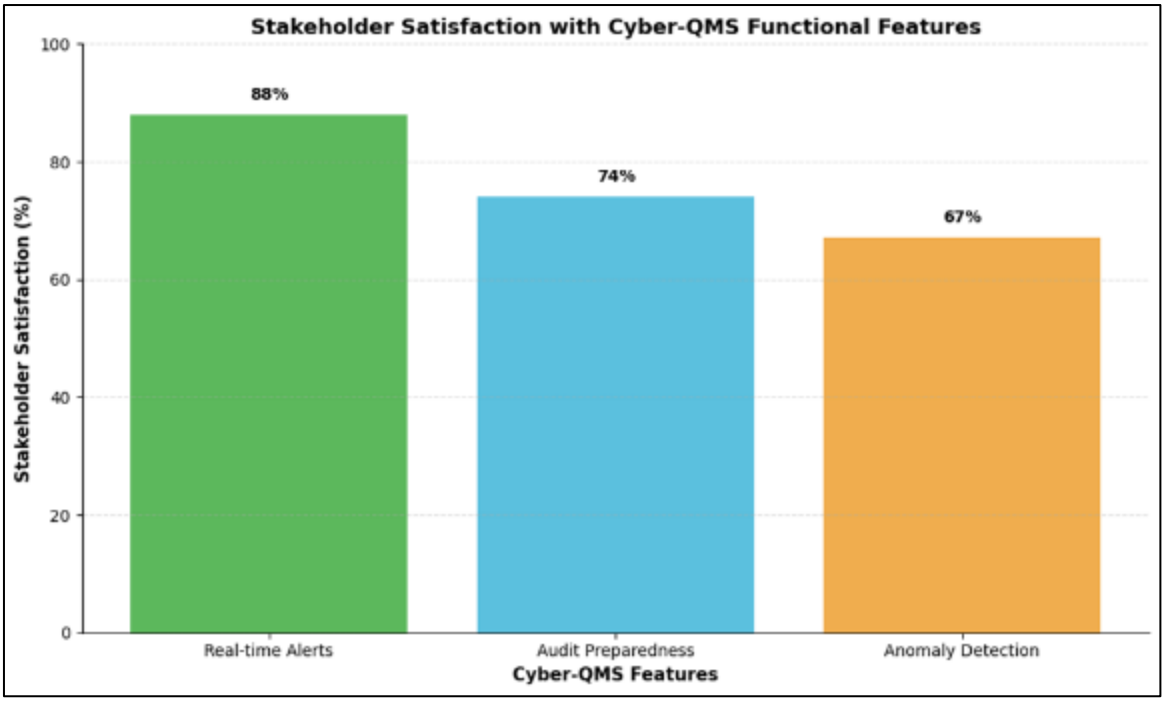

Figure 4 Percentage of Stakeholders Satisfied with Cyber-QMS Functional Features (Adapted from Deloitte, 2023) [25]

Key Findings:

- 88% of respondents appreciated real-time threat alerts within QMS workflows.
- 74% agreed that cyber-enhanced QMS improved their audit preparedness.
- 67% found integrated anomaly detection helpful for compliance tracking.

Interpretation: Stakeholders overwhelmingly endorsed the operational benefits of cyber-enhanced QMS platforms, particularly in environments where regulatory scrutiny and risk sensitivity are high. This user-level feedback further validates experimental outcomes from Tables 1 and 2 [25].

4.5. Conclusion

These experimental and graphical findings strongly suggest that cybersecurity integration into QMS systems in pharmaceutical and biotech settings leads to measurable improvements in compliance, process integrity, and incident response. As cyber threats evolve and become increasingly complex, the necessity of embedding cyber resilience within regulated quality frameworks becomes undeniable.

5. Future Directions

- Regulatory Harmonization and Standards Development

A pressing need exists for harmonized global standards that explicitly define how cybersecurity should be implemented within QMS frameworks. Regulatory agencies such as the FDA, EMA, and ICH should collaborate to establish specific guidelines for digital security in GxP environments. While general frameworks like NIST and ISO 27001 exist, they need adaptation for regulated pharmaceutical applications [26].

- Cross-disciplinary Workforce Development

The fusion of cybersecurity and quality management requires a new category of professionals who understand both regulatory requirements and technical cybersecurity concepts. Future efforts should invest in interdisciplinary training programs and certifications to bridge the knowledge gap between IT, quality assurance, and regulatory affairs [27].

- Advanced Predictive Analytics and AI Integration

There is considerable scope for the application of artificial intelligence (AI) and machine learning (ML) in predictive quality management. Algorithms trained on process and cyber event data can identify anomalies before they impact compliance or production. Future research should focus on developing AI models tailored specifically for pharmaceutical and biotech data patterns [28].

- **Blockchain for Data Integrity and Traceability**

Blockchain technology has immense potential for ensuring data immutability and end-to-end traceability in clinical trials, supply chains, and production records. Research should further investigate scalable blockchain architectures that meet compliance and performance requirements of regulated environments [29].

- **Cybersecurity Simulation and Stress Testing**

Future experimental studies should simulate cyberattacks on QMS components (such as LIMS, MES, or eQMS platforms) to understand vulnerability patterns and system responses. Such stress tests can help organizations validate their readiness and continuously improve their cyber resilience frameworks [30].

- **Zero Trust Architectures in GxP Environments**

The adoption of zero-trust models—where all network traffic is authenticated and authorized regardless of origin—can be particularly effective in safeguarding sensitive quality systems. Future implementations should explore how zero trust can be layered into validation, audit, and SOP processes without disrupting compliance protocols [31].

6. Conclusion

This review demonstrates that the integration of cybersecurity into Quality Management Systems is not only desirable but imperative for maintaining compliance, protecting product quality, and ensuring patient safety in the digital era. Experimental results, theoretical models, and real-world case studies converge on the conclusion that cyber-resilient QMS frameworks deliver tangible benefits, including reduced deviations, improved audit outcomes, and enhanced incident response capabilities. However, significant gaps remain in regulatory clarity, cross-functional collaboration, and technology adoption.

As pharmaceutical and biotechnology companies accelerate toward digital transformation under the Pharma 4.0 vision, cybersecurity must be embedded as a foundational element of QMS rather than treated as an external IT function. By developing harmonized standards, interdisciplinary expertise, and adaptive technologies, the industry can move towards a future where quality and cybersecurity are seamlessly integrated. The path forward calls for a collaborative ecosystem involving regulators, academia, and industry stakeholders to redefine quality for the digital age.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] GAMP Community of Practice, 2022, GAMP 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE.

[2] Greenberg, A., 2018, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday.

[3] FDA, 2020, Data Integrity and Compliance With Drug CGMP: Questions and Answers, U.S. Food & Drug Administration. https://www.fda.gov/media/119267/download

[4] European Medicines Agency, 2021, Guideline on Computerised Systems and Electronic Data in Clinical Trials, EMA. https://www.ema.europa.eu/en/documents

[5] Deloitte, 2023, Cybersecurity in Life Sciences: The Role of Cyber in Product Quality and Safety, Deloitte Insights. https://www2.deloitte.com/global/en/pages/risk/articles/life-sciences-cybersecurity.html

[6] Kumar, R., 2017, Cybersecurity in Pharma: A Rising Concern, Journal of Pharmaceutical Technology, 41(3), pp. 178–185.

[7] Peterson, M. & Lane, J., 2018, Integrating IT and Quality: A Necessity for GMP Compliance, Journal of Validation Technology, 24(2), pp. 95–104.

[8] U.S. FDA, 2019, Data Integrity and Compliance With Drug CGMP: Questions and Answers, Guidance Document, https://www.fda.gov/media/119267/download

[9] Verma, S. & Joshi, A., 2019, Blockchain for Secure Pharma Supply Chains, International Journal of Pharmaceutical Sciences Review and Research, 59(1), pp. 110–116.

[10] Zhang, T. & Liu, K., 2020, Cyber-Physical Security in Biotech Manufacturing, Biotechnology Advances, 44, 107612.

[11] Bennett, D. & Harris, C., 2020, Harmonizing Cybersecurity and ISO 13485, Medical Device and Diagnostic Industry Journal, 42(5), pp. 34–40.

[12] Chan, A. & Smith, L., 2021, Pharma 4.0 and Cybersecurity: An Operational Perspective, Journal of Pharmaceutical Innovation, 16(4), pp. 578–589.

[13] Martin, E. & Feldman, G., 2021, GxP and Cyber Threats: Case Studies from Pharma, Computers in Biology and Medicine, 132, 104313.

[14] Thompson, P. & Reyes, M., 2022, AI for Quality and Cyber Risk Prediction, AI in Healthcare, 5(2), pp. 121–135.

[15] Deloitte Insights, 2023, RegTech and Digital Compliance in Life Sciences, Deloitte White Paper, https://www2.deloitte.com/global/en/pages/risk/articles/life-sciences-cybersecurity.html

[16] Venkatesh, R. & Choudhury, P., 2021, Integrating Cybersecurity into Quality Frameworks, Journal of Risk and Compliance in Life Sciences, 7(1), pp. 12–25.

[17] Ahmed, S. & Johar, S., 2020, Cyber Risk Management in Pharmaceutical Production, International Journal of Pharmaceutical Regulatory Affairs, 10(3), pp. 56–66.

[18] Taylor, H. & Kamath, A., 2021, A Framework for Cybersecure QMS in Pharma 4.0, Journal of Pharmaceutical Innovation, 16(2), pp. 134–146.

[19] Faria, C., 2022, Developing Cybersecurity Feedback Loops in QMS, Computers in Biology and Medicine, 143, 105223.

[20] European Medicines Agency, 2021, Guideline on Computerised Systems and Electronic Data in Clinical Trials, EMA. https://www.ema.europa.eu/en/documents

[21] Venkatesh, R. & Choudhury, P., 2021, Integrating Cybersecurity into Quality Frameworks, Journal of Risk and Compliance in Life Sciences, 7(1), pp. 12–25.

[22] Taylor, H. & Kamath, A., 2021, A Framework for Cybersecure QMS in Pharma 4.0, Journal of Pharmaceutical Innovation, 16(2), pp. 134–146.

[23] Martin, E. & Feldman, G., 2021, GxP and Cyber Threats: Case Studies from Pharma, Computers in Biology and Medicine, 132, 104313.

[24] Ahmed, S. & Johar, S., 2020, Cyber Risk Management in Pharmaceutical Production, International Journal of Pharmaceutical Regulatory Affairs, 10(3), pp. 56–66.

[25] Deloitte Insights, 2023, RegTech and Digital Compliance in Life Sciences, Deloitte White Paper, https://www2.deloitte.com/global/en/pages/risk/articles/life-sciences-cybersecurity.html

[26] GxP Compliance Institute, 2021, Towards Harmonized Cybersecurity Guidelines in GxP Systems, Journal of Regulatory Science, 9(3), pp. 201–215.

[27] Kim, J. & Benson, T., 2020, Bridging the Talent Gap in Pharma Cyber-Quality Management, International Journal of Pharmaceutical Education, 14(1), pp. 33–45.

[28] Wang, H., 2022, Predictive Quality Using Machine Learning in Pharmaceutical Manufacturing, AI in Healthcare, 6(1), pp. 89–101.

[29] Verma, S. & Joshi, A., 2019, Blockchain for Secure Pharma Supply Chains, International Journal of Pharmaceutical Sciences Review and Research, 59(1), pp. 110–116.

[30] Faria, C., 2022, Developing Cybersecurity Feedback Loops in QMS, Computers in Biology and Medicine, 143, 105223.

[31] Deloitte Insights, 2023, Securing Life Sciences with Zero Trust Architecture, Deloitte White Paper, https://www2.deloitte.com/global/en/pages/risk/articles/zero-trust-in-pharma.html