RESEARCH ARTICLE

JENER Journal of Empirical and Non-Empirical Research
Volume 2, Issue 1, Page 334-342 | Article No. 39
DOI: 10.4898/jener.v2i1.a39
ISSN: 7895-9216
Journal homepage: https://jenerjournal.com

JENER Journal
JENER Journal of Empirical and Non-Empirical Research

# Risk-Based Framework for Determining Audit Trail Review Frequency in Pharmaceutical, Biotechnology, and Medical Device Industries

Leo Stewart[1*]

[1]*Department of Quality Assurance, Independent Researcher, London, UK*
*Corresponding Author: Leo Stewart

**APA Citation and Referencing:** Stewart, L. (2026). Risk-Based Framework for Determining Audit Trail Review Frequency in Pharmaceutical, Biotechnology, and Medical Device Industries. *JENER Journal of Empirical and Non-Empirical Research*, 2(1), 334-342

ARTICLE INFORMATION

**Article history:**
Published on 27th Jan 2026

**Keywords:**
Audit Trail Review
Data Integrity
Risk-Based Approach
21 CFR Part 11
GAMP 5
Pharmaceutical Manufacturing
Computer System Validation
Quality Risk Management

ABSTRACT

Audit trail review has emerged as a critical component of data integrity assurance in regulated industries, yet regulatory guidance provides limited specificity regarding review frequency determination. Organizations struggle to balance compliance requirements with operational efficiency when establishing audit trail review schedules across diverse computerized systems, analytical instruments, and manufacturing equipment. This research article proposes a comprehensive risk-based framework for determining appropriate audit trail review frequencies across multiple system types in pharmaceutical, biotechnology, and medical device manufacturing environments, with primary focus on FDA regulatory expectations. A systematic literature review was conducted examining regulatory guidance documents, industry position papers, and peer-reviewed publications addressing audit trail review practices. Risk assessment methodologies from ICH Q9 were adapted to develop a framework integrating system criticality, data impact, and technical control effectiveness as primary determinants of review frequency. The proposed framework establishes a tiered approach categorizing systems into four review frequency levels: continuous/concurrent (with data review), periodic high-frequency (weekly to monthly), periodic moderate-frequency (monthly to quarterly), and periodic low-frequency (quarterly to annually). A decision tree incorporating system GxP impact, data criticality, and technical control maturity enables organizations to systematically assign appropriate review frequencies. Application examples across computer systems, analytical instruments, and manufacturing equipment demonstrate framework utility. Implementation of a documented, risk-based approach to audit trail review frequency determination enables organizations to focus resources on high-impact systems while maintaining regulatory compliance. The framework provides a defensible methodology that aligns with current FDA expectations for data integrity management and supports efficient allocation of quality assurance resources.

## 1. Introduction

Data integrity has become one of the most scrutinized aspects of regulatory compliance in pharmaceutical, biotechnology, and medical device industries. Regulatory authorities worldwide have consistently emphasized that ensuring the accuracy, completeness, and reliability of data is fundamental to protecting patient safety and product quality [1]. Central to data integrity assurance is the audit trail, defined as a secure, computer-generated, time-stamped electronic record enabling reconstruction of events relating to the creation, modification, or deletion of electronic records [2].

The regulatory expectation for audit trail functionality is well established through 21 CFR Part 11, which requires the use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records [3]. However, while regulations clearly mandate the existence and proper configuration of audit trails, they provide considerably less specificity regarding the frequency and methodology for reviewing these records. This regulatory gap has created significant uncertainty within industry regarding how often audit trails should be examined and what constitutes an adequate review process.

The FDA's Data Integrity and Compliance with Drug CGMP Questions and Answers guidance document acknowledges this challenge by stating that if the review frequency for data is not specified in CGMP regulations, organizations should determine the review frequency using knowledge of their processes and risk assessment tools [2]. The guidance further specifies that risk assessments should include evaluation of data criticality, control mechanisms, and impact on product quality. This risk-based approach aligns with the broader regulatory philosophy articulated in ICH Q9, which promotes proportionate application of quality risk management principles based on the significance of potential harms [4].

Despite this guidance, many organizations continue to struggle with practical implementation. A common industry challenge involves determining whether audit trails should be reviewed with every data review instance, at defined periodic intervals, or through some combination of approaches tailored to system type and data criticality [5]. This variability stems partly from the diversity of systems requiring audit trail review, ranging from enterprise resource planning systems and laboratory information management systems to chromatography data systems and manufacturing execution systems, each presenting unique considerations for review frequency determination.

The audit trail has become an integral part of pharmaceutical quality systems due to current international regulatory demands associated with data integrity expectations [6]. Between 2017 and 2022, the FDA issued more than 160 warning letters citing data integrity deficiencies, with approximately half of all GMP warning letters in 2018 including a data integrity component [7]. Quality needs to be built into systems and processes throughout the product lifecycle, and audit trail functionality serves as a key source helping manufacturers minimize risk while maintaining the reliability and security of electronic data [8]. These enforcement trends underscore the critical importance of establishing robust review practices.

The objective of this research article is to propose a comprehensive, risk-based framework for determining appropriate audit trail review frequencies that can be applied across the spectrum of computerized systems, analytical instruments, and manufacturing equipment found in regulated manufacturing environments. The framework integrates established risk assessment methodologies with practical considerations for implementation, providing organizations with a systematic approach to this critical compliance challenge.

## 2. Regulatory Framework and Guidance

### *2.1 FDA 21 CFR Part 11 Requirements*

The foundation for audit trail requirements in FDA-regulated industries is established in 21 CFR Part 11, Electronic Records; Electronic Signatures, promulgated in 1997. Section 11.10(e) specifically addresses audit trails, requiring that persons using closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls including the use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records [3]. The regulation further stipulates that record changes shall not obscure previously recorded information and that audit trail documentation shall be retained for a period at least as long as required for the subject electronic records.

Importantly, 21 CFR Part 11 establishes the requirement for audit trail existence and retention but does not prescribe specific review frequencies or methodologies. The FDA's 2003 guidance on Part 11 scope and application clarified that the kinds of operator actions that need to be covered by an audit trail are generally those important enough to memorialize in the electronic record itself [9]. This guidance introduced the concept of risk-based determination, recommending that organizations consider the need to comply with predicate rule requirements and conduct justified and documented risk assessments to determine the potential effect on product quality, product safety, and record integrity when deciding how to apply audit trail controls.

### *2.2 FDA Data Integrity Guidance*

The FDA's December 2018 guidance document, Data Integrity and Compliance with Drug CGMP Questions and Answers, provides the most specific agency guidance on audit trail review practices [2]. This document explicitly addresses review frequency, stating that audit trail review is similar to assessing cross-outs on paper when reviewing data. Personnel responsible for record review under CGMP should review the audit trails that capture changes to data associated with the record as they review the rest of the record.

The guidance establishes a foundational principle that audit trail review should occur concurrent with associated data review when such review frequencies are specified in regulations. For example, production and control records, including their audit trails, must be reviewed and approved by the quality unit as part of batch release [10]. However, the guidance also acknowledges that not all audit trail reviews need occur at this frequency, stating that organizations should determine appropriate review frequency using process knowledge and risk assessment tools when regulatory specifications are absent.

Critical factors identified in the FDA guidance for risk assessment include data criticality in terms of its impact on decision making and product quality, effectiveness of control mechanisms in preventing unauthorized changes, and the overall impact on product quality if data integrity were compromised [2]. This risk-based framework aligns with the agency's broader shift toward science-based and risk-proportionate regulatory approaches. Research examining FDA warning letters and Form 483 observations has demonstrated that data integrity violations frequently involve data falsification, poor retention practices, and electronic record manipulation, highlighting the importance of comprehensive audit trail review procedures [11].

### *2.3 GAMP 5 Second Edition Guidance*

The International Society for Pharmaceutical Engineering (ISPE) published the second edition of GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems in July 2022, representing the most significant update to this foundational industry guidance in fourteen years [12]. GAMP 5 Second Edition maintains the risk-based approach of its predecessor while providing updated guidance on audit trail requirements and review practices relevant to modern computerized systems.

GAMP 5 emphasizes that data audit trails, as required by various regulations, record operator actions that create, modify, or delete GMP records during normal operation and should be clearly distinguished from other system and technical logs [12]. This distinction is important for review frequency determination, as system logs capturing administrative functions may warrant different review schedules than data audit trails capturing GxP-critical record modifications.

The GAMP Records and Data Integrity Guide provides additional context, stating that audit trail review should be performed by an individual who has an understanding of the business process and the impact of the actions recorded [13]. This guidance

emphasizes that audit trail reviews serve as an effective means of verifying that changes are made by authorized users and for detecting potential data integrity issues. The document supports a risk-based approach to determining review frequency while acknowledging that critical audit trails related to batch operations should be reviewed prior to batch release.

*2.4 ICH Q9 Quality Risk Management*

ICH Q9 Quality Risk Management, revised in 2023 as Q9(R1), provides the overarching framework for risk-based decision making in pharmaceutical quality systems [4]. While not specifically addressing audit trail review, ICH Q9 establishes principles and methodologies directly applicable to determining review frequencies.

The guideline defines risk as the combination of the probability of occurrence of harm and the severity of that harm, providing a conceptual foundation for evaluating audit trail review requirements [4]. ICH Q9 presents multiple risk assessment tools applicable to review frequency determination, with Failure Mode and Effects Analysis (FMEA) being particularly relevant due to its structured approach to evaluating severity, probability, and detectability. Pharmaceutical regulations do not prescribe a specific procedure for determining risk; however, application of ICH Q9 methodologies is recommended, with FMEA being the most common method used in the pharmaceutical industry for risk scoring [14].

A key principle from ICH Q9(R1) relevant to audit trail review frequency is that the level of effort, formality, and documentation of quality risk management processes should be commensurate with the level of risk [4]. This proportionality principle supports differentiated review frequencies based on system criticality and data impact, avoiding the resource-intensive approach of applying identical review requirements across all systems regardless of risk profile.

*2.5 PIC/S Data Integrity Guidance*

The Pharmaceutical Inspection Co-operation Scheme (PIC/S) published Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments in 2021, providing harmonized guidance across member regulatory authorities [15]. This document specifically addresses audit trail review frequency, establishing that critical audit trails related to each operation should be independently reviewed with all other records related to the operation and prior to review completion of the operation.

Significantly, PIC/S guidance distinguishes between critical and non-critical audit trails, stating that non-critical audit trail reviews can be conducted during system reviews at a pre-defined frequency [15]. This distinction provides regulatory support for differentiated review schedules based on data criticality, a principle central to the framework proposed in this article.

*2.6 WHO Technical Report Series Guidelines*

The World Health Organization (WHO) Technical Report Series No. 1033, Annex 4 provides international guidance on data integrity applicable to pharmaceutical manufacturers worldwide [16]. This guideline emphasizes that all GxP relevant audit trails should be enabled when software is installed and remain enabled at all times, with periodic verification to ensure the audit trail remains enabled throughout the data lifecycle.

The WHO guidance reinforces the principle that the effort and resources applied to assure the integrity of data should be commensurate with the risk and impact of a data integrity failure [16]. This proportionality principle supports the risk-based framework for review frequency determination, enabling organizations to allocate review resources based on system criticality and data impact rather than applying uniform requirements across all systems.

**3. Literature Review: Current Industry Practices and Challenges**

*3.1 Variability in Industry Approaches*

Current industry practices for audit trail review frequency demonstrate significant variability, reflecting the lack of prescriptive regulatory requirements and the diversity of organizational contexts. Research from the International Consortium for Innovation and Quality in Pharmaceutical Development (IQ) Working Group documented that data arising from activities such as GLP studies, cleaning verification, clinical product release, and stability were considered greater impact and may trigger audit trail review, while activities such as method validation may have an indirect effect on product quality and may be considered less impactful [5].

Industry position papers on audit trail review in clinical data systems have noted that pharmaceutical companies increasingly rely on third-party service vendors to provide technologies, many of which may have less experience with the regulatory landscape [17]. This emphasizes the importance of organizations assessing audit trail review capability within electronic systems and implementing mitigations when system functionality or operational processes are insufficient.

Research on audit trail requirements for digitalized regulated laboratories highlighted that second person review of electronic data requires critical examination of pertinent audit trail entries of each analysis performed using a computerized system [18]. The application of ALCOA++ principles (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available, and Traceable) to audit trail entries provides a structured framework for effective review, though the frequency of such review remains subject to organizational risk assessment [18].

*3.2 Challenges in Frequency Determination*

Several challenges complicate audit trail review frequency determination in practice. First, the volume of audit trail data generated by modern computerized systems can be substantial, making comprehensive review of every entry impractical for many organizations [19]. Manufacturing execution systems, chromatography data systems, and enterprise resource planning platforms may generate thousands of audit trail entries daily, necessitating risk-based prioritization of review efforts.

Second, the interpretation of what constitutes adequate review varies across organizations and regulatory inspectors. Industries need to rely more on risk-based approaches to the review of audit trails and establish more nimble and flexible standards to complement compliance efforts [8]. Regulatory audits have highlighted that quality needs to be built into systems and processes throughout the product lifecycle, emphasizing the importance of systematic approaches to audit trail review.

Third, organizational structures and resource constraints influence practical implementation. Regulatory authorities have continued to highlight data integrity as a key quality control laboratory issue, with warning letters citing inadequate audit trail review procedures as contributing factors to data integrity violations [20]. In 2024, a significant proportion of FDA warning letters cited data integrity issues, often tied to missing audit trails or uncontrolled changes [21]. Research examining FDA warning letters between fiscal years 2007 and 2018 documented persistent patterns of data integrity violations, reinforcing the need for systematic approaches to audit trail review [22]. These enforcement actions underscore the importance of establishing documented, defensible approaches to review frequency that can withstand regulatory scrutiny.

### *3.3 Risk Assessment Methodologies*

Multiple risk assessment methodologies have been applied to audit trail review frequency determination. The FMEA approach, widely used in pharmaceutical quality risk management, provides a structured framework for evaluating risk factors [4]. When applied to audit trail review, FMEA considers the severity of potential data integrity failures, the probability of such failures occurring given existing controls, and the detectability of failures through current review processes.

Decision tree approaches have been developed where data types are categorized and the need for audit trail review considered based on system characteristics and data impact [5]. This approach serves as a risk assessment determining the need for procedural controls, with controls documented within qualification packages for new equipment or in change management systems for equipment updates.

Risk filtering tools described in ICH Q9 have also been applied, enabling organizations to compare and rank risks across multiple systems to prioritize review resources [4]. These tools typically incorporate weighting factors reflecting organizational priorities and regulatory requirements, generating relative risk scores used for ranking systems and determining appropriate review frequencies.

The challenge of ensuring data integrity is becoming more complex with the growing amount of data generated given increasing adoption of process analytical technology, advanced automation, and machine learning tools [23]. This evolution toward Industry 4.0 requires adaptation of traditional audit trail review approaches to address new data types and system architectures while maintaining regulatory compliance.

## 4. Proposed Risk-Based Framework for Review Frequency Determination

### *4.1 Framework Overview*

The proposed framework establishes a systematic approach to determining audit trail review frequency based on three primary risk factors: system GxP impact classification, data criticality assessment, and technical control effectiveness evaluation. Integration of these factors through a structured assessment process yields a recommended review frequency tier, providing organizations with a defensible, documented methodology for compliance.

The framework recognizes that audit trail review serves two distinct purposes requiring potentially different approaches [24]. First, review concurrent with data review ensures that specific record modifications are examined in context with the associated GxP records, enabling detection of problematic changes before decisions based on that data are finalized. Second, periodic system-level review evaluates overall patterns of system use, administrative changes, and security configurations that may not be apparent from individual record reviews.

### *4.2 System GxP Impact Classification*

The first dimension of the framework involves classifying systems according to their GxP impact, building upon the software categorization approach established in GAMP 5 [12]. For audit trail review frequency purposes, systems are classified into four impact levels:

High Impact Systems directly affect product quality decisions or patient safety. Examples include chromatography data systems generating release testing data, manufacturing execution systems controlling critical process parameters, and electronic batch record systems documenting production activities. For these systems, audit trail integrity failures could directly result in release of non-conforming product or incorrect manufacturing decisions.

Medium-High Impact Systems support GxP-critical processes with indirect effects on product quality. Examples include laboratory information management systems managing sample workflows, document management systems controlling GMP documentation, and environmental monitoring systems tracking facility conditions. Failures in these systems could contribute to quality issues but typically require additional failures before directly affecting product.

Medium Impact Systems perform GxP-relevant functions with limited direct quality impact. Examples include training management systems tracking personnel qualifications, calibration management systems scheduling equipment maintenance, and deviation management systems documenting quality events. These systems support the quality infrastructure but do not directly generate product quality data.

Low Impact Systems have minimal GxP relevance or operate in contexts where alternative controls provide adequate oversight. Examples include administrative scheduling systems, non-GxP data analysis tools, and infrastructure monitoring systems. While audit trail functionality may be present, review requirements are minimal.

*4.3 Data Criticality Assessment*

The second framework dimension evaluates the criticality of data processed or generated by each system. Data criticality reflects the potential consequences if data integrity were compromised, considering both patient safety and regulatory compliance implications [2].

Release-Critical Data directly supports product release decisions, including finished product testing results, in-process testing at critical control points, stability data supporting shelf life, and cleaning verification results. Compromise of this data could directly result in release of unsafe or ineffective product.

Compliance-Critical Data supports regulatory compliance without directly affecting release decisions. Examples include environmental monitoring data, equipment qualification records, and training documentation. While important for demonstrating compliance, compromise of this data is less likely to directly affect product quality.

Supporting Data provides context or supports quality system functions without directly affecting compliance or release. Examples include investigation documentation, trend analysis data, and supplier qualification records. This data supports quality decision-making but is typically verified through multiple sources.

Administrative Data has minimal quality or compliance significance. Examples include scheduling information, resource allocation data, and general communications. While audit trails may capture changes to this data, review requirements are minimal.

*4.4 Technical Control Effectiveness*

The third framework dimension evaluates the effectiveness of technical controls in preventing or detecting unauthorized data modifications. Systems with robust technical controls may require less frequent manual review, while systems with limited controls require more intensive oversight [5].

Comprehensive Controls include role-based access with principle of least privilege, mandatory electronic signatures for critical actions, automated audit trail generation that cannot be disabled, and technical prevention of data deletion. Systems with comprehensive controls present lower risk and may support reduced review frequencies.

Standard Controls include user authentication, basic role-based access, automated audit trail generation, and restricted administrative access. These controls meet regulatory requirements but may not prevent all potential integrity issues.

Limited Controls include basic user authentication and audit trail functionality but lack advanced features such as electronic signatures or robust access controls. Systems with limited controls require more intensive review to compensate for technical gaps.

Minimal Controls lack fundamental features such as automated audit trails or robust access management. These systems typically require remediation to meet regulatory expectations, and until remediation is complete, intensive procedural controls including frequent review are necessary.

*4.5 Frequency Determination Matrix*

Integration of the three framework dimensions yields recommended review frequency tiers. Table 1 presents the frequency determination matrix, with review frequency increasing as system impact, data criticality, or control limitations increase.

Table 1: Audit Trail Review Frequency Determination Matrix

| System Impact | Data Criticality | Technical Controls | Recommended Review Frequency |
|---|---|---|---|
| High | Release-Critical | Comprehensive | Concurrent with data review |
| High | Release-Critical | Standard | Concurrent with data review |
| High | Release-Critical | Limited | Concurrent + Weekly system review |
| High | Compliance-Critical | Comprehensive | Weekly to Monthly |
| High | Compliance-Critical | Standard | Weekly |
| Medium-High | Release-Critical | Comprehensive | Concurrent with data review |
| Medium-High | Release-Critical | Standard | Concurrent with data review |
| Medium-High | Compliance-Critical | Comprehensive | Monthly |
| Medium-High | Compliance-Critical | Standard | Weekly to Monthly |
| Medium | Compliance-Critical | Comprehensive | Monthly to Quarterly |
| Medium | Compliance-Critical | Standard | Monthly |
| Medium | Supporting | Comprehensive | Quarterly |
| Medium | Supporting | Standard | Monthly to Quarterly |
| Low | Any | Any | Quarterly to Annually |

*4.6 Decision Tree for Frequency Assignment*

The framework includes a decision tree to guide systematic frequency assignment (Figure 1). The decision tree poses sequential questions regarding system characteristics, leading to recommended frequency assignments.

Decision Tree Logic:

1. Is the system used for GxP-regulated activities?
    - No → Audit trail review not required for GxP compliance
    - Yes → Proceed to Question 2
2. Does the system generate or process data directly supporting product release decisions?
    - Yes → Audit trail review concurrent with data review required; proceed to Question 3 for system-level review frequency
    - No → Proceed to Question 3
3. What is the system's GxP impact classification?
    - High Impact → Proceed to Question 4
    - Medium-High Impact → Proceed to Question 5
    - Medium Impact → Proceed to Question 6
    - Low Impact → Quarterly to annual system-level review
4. For High Impact systems: What is the technical control maturity?
    - Comprehensive → Monthly system-level review
    - Standard → Weekly to monthly system-level review
    - Limited → Weekly system-level review plus remediation plan
5. For Medium-High Impact systems: What is the data criticality?
    - Release-Critical or Compliance-Critical → Monthly system-level review
    - Supporting → Monthly to quarterly system-level review
6. For Medium Impact systems: What is the data criticality?
    - Compliance-Critical → Monthly to quarterly system-level review
    - Supporting or Administrative → Quarterly system-level review

## 5. Application Across System Types

### *5.1 Computer Systems*

Computer systems encompass a broad category including laboratory information management systems (LIMS), electronic quality management systems (eQMS), enterprise resource planning (ERP) systems, and document management systems (DMS). Application of the framework to these systems requires consideration of their diverse functions and data types.

For LIMS managing analytical testing workflows, the system typically processes release-critical data and falls within the high impact classification. Concurrent audit trail review with data review is recommended for results supporting release decisions, with monthly system-level review to evaluate administrative changes, user access modifications, and overall usage patterns [18].

For eQMS platforms managing deviations, CAPAs, and change controls, the system processes compliance-critical data supporting quality decision-making. Medium-high impact classification with monthly to quarterly system-level review is typically appropriate, with more frequent review during periods of intensive system use such as product launch or following significant quality events.

For ERP systems with GxP modules such as inventory management or batch traceability, application of the framework requires evaluation of specific module functions. Modules directly supporting batch release may require concurrent review, while modules supporting administrative functions may warrant quarterly review [12].

### *5.2 Analytical Instruments*

Analytical instruments including chromatography systems, spectrophotometers, dissolution apparatus, and particle analyzers generate data directly supporting product quality decisions. These systems typically fall within high impact classification with release-critical data.

For chromatography data systems, regulatory expectations clearly establish that audit trail review should occur concurrent with data review prior to batch release [5]. This includes review of integration parameter changes, reprocessing activities, and any modifications to analytical results. Monthly system-level review should evaluate administrative changes, method modifications, and user access patterns.

For standalone instruments such as balances, pH meters, and conductivity meters, the framework application depends on data criticality and system connectivity. Instruments integrated with LIMS or other networked systems may leverage centralized audit trail review, while standalone instruments require individual consideration. For instruments generating release-critical data, concurrent review remains appropriate; for instruments generating supporting data, quarterly review may suffice [18].

### *5.3 Manufacturing Equipment*

Manufacturing equipment including process control systems, programmable logic controllers (PLCs), and packaging line systems present unique considerations for audit trail review. These systems directly affect product quality through control of critical process parameters.

For manufacturing execution systems (MES) controlling batch production, high impact classification with release-critical data applies. Audit trail review should occur concurrent with batch record review, examining any parameter modifications, alarm acknowledgments, or manual interventions during production. Monthly system-level review should evaluate recipe changes, equipment configurations, and administrative modifications [19].

For process control systems managing continuous manufacturing or utility systems supporting production, the framework recommends weekly to monthly system-level review depending on criticality. Systems controlling critical utilities such as water for injection or clean steam warrant more frequent review than systems controlling non-critical utilities.

*5.4 Utility Systems*

Utility systems including building management systems, environmental monitoring systems, and water treatment systems support manufacturing operations without directly controlling product-contact processes. Application of the framework typically yields medium impact classification with compliance-critical data.

For environmental monitoring systems tracking cleanroom conditions, monthly system-level review is recommended to evaluate alarm patterns, excursion management, and any modifications to monitoring parameters. Concurrent review of audit trails is recommended when investigating environmental excursions affecting batch disposition.

For water treatment systems generating water for pharmaceutical use, the criticality depends on water classification. Systems generating water for injection warrant more frequent review than systems generating purified water, reflecting the higher patient safety implications of water for injection quality failures.

## 6. Implementation Considerations

*6.1 Documentation Requirements*

Implementation of the risk-based framework requires comprehensive documentation supporting regulatory defense. Essential documentation elements include the risk assessment methodology, rationale for frequency assignments, and evidence of review completion [2].

The risk assessment should be documented in a controlled format, typically within the computerized system validation documentation or as a standalone data integrity assessment. The assessment should identify the system under evaluation, document the classification decisions for each framework dimension, and record the resulting frequency assignment with supporting rationale.

Review completion should be documented through controlled records, which may include checklists, electronic review logs, or notations within quality system databases. Documentation should identify the reviewer, review date, scope of review, and any findings requiring follow-up. For systems with concurrent review requirements, documentation typically occurs within the batch record or analytical report being reviewed.

*6.2 Roles and Responsibilities*

Clear assignment of roles and responsibilities supports effective framework implementation. Key roles include system owners responsible for ensuring review completion, reviewers performing the actual audit trail examination, and quality assurance personnel providing oversight [13].

System owners should ensure that review schedules are established, resources are allocated for review completion, and any findings are appropriately addressed. For enterprise systems, system ownership may reside within IT functions with quality assurance oversight; for laboratory instruments, ownership typically resides within laboratory management.

Reviewers should possess adequate understanding of the business processes supported by the system and the significance of potential audit trail findings. Training on audit trail review should address system-specific considerations, common finding types, and escalation procedures for significant discoveries.

Quality assurance should provide oversight of framework implementation, including periodic verification that reviews are completed as scheduled and findings are appropriately addressed. Quality assurance may also perform independent review of high-risk systems to verify primary review adequacy.

*6.3 Training Considerations*

Effective audit trail review requires reviewers to understand both technical aspects of audit trail interpretation and quality implications of potential findings [25]. Training programs should address system-specific audit trail formats, interpretation of common entry types, recognition of potentially problematic patterns, and escalation procedures.

Training should emphasize the distinction between routine entries reflecting normal system use and entries potentially indicating data integrity concerns. Routine entries may include standard data modifications with appropriate justification, user login and logout activities, and system-generated automatic entries. Potentially concerning entries may include modifications without adequate justification, activities outside normal working hours, repeated modifications to the same data, or patterns suggesting circumvention of controls.

*6.4 Periodic Framework Review*

The risk-based framework should be periodically reviewed to ensure continued appropriateness of frequency assignments. Triggers for framework review include changes to system functionality, modifications to data use, regulatory guidance updates, and findings from regulatory inspections.

Annual review of frequency assignments is recommended as a minimum, with more frequent review following significant changes. Review should consider whether actual review findings support the assigned frequency, whether resource allocation remains appropriate, and whether regulatory expectations have evolved.

## 7. Discussion

### *7.1 Practical Implications*

The proposed framework provides organizations with a structured methodology for addressing the challenging question of audit trail review frequency. By integrating system impact, data criticality, and technical control effectiveness, the framework enables differentiated approaches that focus resources on highest-risk systems while maintaining adequate oversight of lower-risk systems.

Implementation of the framework supports regulatory compliance by demonstrating a documented, risk-based approach to review frequency determination. Regulatory guidance consistently emphasizes that risk-based approaches should be documented and justified, and the framework provides the structure necessary to meet this expectation [2]. Organizations can reference the framework and associated risk assessments when responding to regulatory inquiries regarding audit trail review practices.

The framework also supports operational efficiency by avoiding the resource-intensive approach of applying identical review frequencies across all systems. Organizations with limited quality assurance resources can prioritize review efforts on high-impact systems while maintaining compliant oversight of lower-impact systems through less frequent review schedules.

### *7.2 Alignment with Regulatory Expectations*

The framework aligns with current FDA expectations as articulated in the Data Integrity guidance, which emphasizes risk-based approaches to review frequency determination [2]. The framework's emphasis on data criticality, control mechanisms, and quality impact directly reflects the factors identified in FDA guidance for risk assessment.

The framework also aligns with PIC/S guidance distinguishing between critical and non-critical audit trails, supporting differentiated review schedules based on data significance [15]. The tiered frequency approach mirrors the PIC/S distinction between audit trails requiring review prior to operation completion and those suitable for periodic system-level review.

### *7.3 Limitations*

Several limitations should be acknowledged. First, the framework provides general guidance that must be adapted to specific organizational contexts, system configurations, and regulatory requirements. Organizations operating under multiple regulatory jurisdictions may need to reconcile framework recommendations with jurisdiction-specific expectations.

Second, the framework assumes that systems have functional audit trail capabilities meeting regulatory requirements. Systems lacking adequate audit trail functionality require remediation before the framework can be effectively applied [20].

Third, the framework addresses review frequency but does not comprehensively address review methodology or scope. Organizations must develop system-specific procedures defining what audit trail elements require review and how review should be documented.

### *7.4 Future Directions*

Future development of audit trail review practices may incorporate automated review tools leveraging artificial intelligence and machine learning capabilities. Such tools could potentially identify anomalous patterns across large audit trail datasets, enabling more efficient review while maintaining or improving detection capability [26].

Additionally, ongoing regulatory dialogue may yield more specific guidance on review frequency expectations. Organizations should monitor regulatory communications and update framework applications as guidance evolves. The increasing adoption of cloud-based systems and advanced automation in pharmaceutical manufacturing will require continued adaptation of audit trail review approaches to address new technological paradigms while maintaining data integrity [23].

## 8. Conclusion

Determination of appropriate audit trail review frequency represents a significant challenge for organizations in pharmaceutical, biotechnology, and medical device industries. Regulatory guidance establishes clear expectations for audit trail functionality and review but provides limited specificity regarding review frequency, creating uncertainty and variability in industry approaches.

The risk-based framework proposed in this article provides a systematic methodology for frequency determination integrating system GxP impact, data criticality, and technical control effectiveness. The framework establishes four review frequency tiers ranging from concurrent review with data review for high-impact systems with release-critical data to quarterly or annual review for low-impact systems with administrative data.

Application of the framework across computer systems, analytical instruments, and manufacturing equipment demonstrates its utility for diverse system types encountered in regulated manufacturing environments. Implementation considerations including documentation requirements, roles and responsibilities, and training needs support practical deployment of the framework within organizational quality systems.

The framework aligns with current regulatory expectations emphasizing documented, risk-based approaches to data integrity management. Organizations implementing the framework can demonstrate a defensible methodology for review frequency determination while optimizing resource allocation across their system portfolio.

Ongoing evolution of regulatory expectations, technological capabilities, and industry practices will necessitate periodic framework review and refinement. Organizations should monitor regulatory communications and incorporate emerging guidance into framework applications to maintain alignment with evolving expectations.

**References**


[1] U.S. Food and Drug Administration. (2018). Data integrity and compliance with drug CGMP: Questions and answers guidance for industry. https://www.fda.gov/media/119267/download

[2] U.S. Food and Drug Administration. (2018). Data integrity and compliance with drug CGMP: Questions and answers guidance for industry. Silver Spring, MD: FDA.

[3] U.S. Food and Drug Administration. (1997). 21 CFR Part 11: Electronic records; electronic signatures. Code of Federal Regulations, Title 21.

[4] International Council for Harmonisation. (2023). ICH Q9(R1): Quality risk management. Geneva: ICH.

[5] Lippke, J., Mongillo, J., Cullen, T., Metz, C., Harasewych, K., & Benamira, F. (2022). A harmonized approach to performing a risk-based audit trail review. Pharmaceutical Technology, 46(9), 48-53.

[6] Patel, B., & Patel, J. J. (2025). Risk-based approach for audit trail in pharmaceutical industry: Ensuring data integrity under FDA and EU regulations. International Journal of Management IT and Engineering, 15, 18-31. https://doi.org/10.5281/zenodo.17245470

[7] Chauhan, V. (2023). Data integrity in pharmaceuticals: Empowering trustworthy decisions from source to success via registration dossier. Association of Clinical Research Professionals. https://acrpnet.org/2023/08/15/data-integrity-in-pharmaceuticals/

[8] Sharma, A., & Thakur, N. (2022). Audit trail in pharma: A review. Asian Journal of Pharmaceutical Research, 12(4), 281-286. https://doi.org/10.52711/2231-5691.2022.00045

[9] U.S. Food and Drug Administration. (2003). Guidance for industry: Part 11, electronic records; electronic signatures - scope and application. Silver Spring, MD: FDA.

[10] U.S. Food and Drug Administration. (2008). 21 CFR Part 211: Current good manufacturing practice for finished pharmaceuticals. Code of Federal Regulations, Title 21.

[11] Ullagaddi, P. (2024). Safeguarding data integrity in pharmaceutical manufacturing. Journal of Advances in Medical and Pharmaceutical Sciences, 26(8), 64-75. https://doi.org/10.9734/jamps/2024/v26i8708

[12] International Society for Pharmaceutical Engineering. (2022). GAMP 5: A risk-based approach to compliant GxP computerized systems (2nd ed.). Tampa, FL: ISPE.

[13] International Society for Pharmaceutical Engineering. (2020). GAMP good practice guide: Records and data integrity. Tampa, FL: ISPE.

[14] GMP Compliance. (2025). Risk-based determination of the scope and frequency of audit trail reviews. https://www.gmp-compliance.org/gmp-news/risk-based-determination-of-the-scope-and-frequency-of-audit-trail-reviews

[15] Pharmaceutical Inspection Co-operation Scheme. (2021). PI 041-1: Good practices for data management and integrity in regulated GMP/GDP environments. Geneva: PIC/S.

[16] World Health Organization. (2021). WHO Technical Report Series No. 1033, Annex 4: Guideline on data integrity. Geneva: WHO.

[17] Society for Clinical Data Management. (2024). Audit trail review: A key tool to ensure data integrity. SCDM Industry Position Paper.

[18] McDowall, R. D., & Lotfinia, M. (2025). Audit trail requirements for a digitalized regulated laboratory. Technology Networks. https://www.technologynetworks.com/informatics/articles/audit-trail-requirements-for-a-digitalized-regulated-laboratory-401729

[19] SeerPharma. (2025). Efficient audit trail review for PIC/S GMP Annex 11 compliance. https://blog.seerpharma.com/efficient-audit-trail-review-for-pic/s-gmp-annex-11-compliance

[20] European Pharmaceutical Review. (2024). FDA warning letters highlight data integrity issues. https://www.europeanpharmaceuticalreview.com/news/219951/fda-warning-letters-highlight-data-integrity-issues/

[21] Laboratorios Rubio. (2025). Data integrity in pharmaceutical compliance: A 2025 guide. https://www.laboratoriosrubio.com/en/data-integrity-pharmaceutical-compliance/

[22] Rogers, C. A., Ahearn, J. D., & Bartlett, M. G. (2020). Data integrity in the pharmaceutical industry: Analysis of inspections and warning letters issued by the Bioresearch Monitoring Program between fiscal years 2007-2018. PDA Journal of Pharmaceutical Science and Technology, 73(4), 342-353. https://doi.org/10.5731/pdajpst.2018.009407

[23] Goldrick, S., Duber, E., Ghaderi, A., Maddox, I., Sheridan, R., & Sherlock, J. P. (2023). Data integrity within the biopharmaceutical sector in the era of Industry 4.0. Biotechnology Journal, 18(10), 2300111.

[24] Integrity Consulting. (2024). Applying critical thinking to audit trail review. https://integrity.net/news/applying-critical-thinking-2

[25] Freyr Solutions. (2025). GMP audit trail review: What health authorities expect in 2025. https://www.freyrsolutions.com/blog/gmp-audit-trail-review-what-health-authorities-expect-in-2025

[26] IntuitionLabs. (2025). Automating audit trail compliance for 21 CFR Part 11 & Annex 11. https://intuitionlabs.ai/articles/audit-trails-21-cfr-part-11-annex-11-compliance