# Independent Audit Requirements for Document Custodians – Information Security Supplemental Requirement

## Version 1.0

## March 2026

Fannie Mae®

**Table of Contents**

# 1 Document Revision History

| Date | Version | Change Description |
|---|---|---|
| March 2026 | 1.0 | Initial Creation |
| | | |

## 2 Requirements for Information Security Assessment

An Information Security Assessment is required to ensure the Document Custodian operations comply with requirements as outlined in the *Fannie Mae Information Security and Business Resiliency Supplement* ("ISBR") published on fanniemae.com. The independent auditor must address all questions, including obtaining evidence as required. Any gaps or findings must be included in a report to the Document Custodian at the conclusion of the audit. Results of the assessment must be submitted to Fannie Mae concurrently with the Annual Independent Audit results but as a separate document.

## 3 Documents Required for Audit Review

| **The Following Documents Are Required to Complete a Full Information Security Assessment of the Document Custodian**: | | |
|---|---|---|
| **Area of Assessment** | **Document Type / Acceptable Format(s) and/or Document Purpose:** | **Requirement:** |
| Independent Third-Party Assessment* or Audit Report with coverage for appropriate information security controls<br>**OR**<br>Industry recognized certification -with statements of applicability | • SSAE 18/SOC 1<br>• AT 101/SOC 2<br>• Independent audit or assessment report from either external organization or an internal organization not responsible for the execution of information security controls | Audits/assessments reports under review must have been conducted within the last 12 months |
| | • ISAE<br>• ISO<br>• IEC 27001<br>• CyberGRX Report- provided by exchange providers | |
| Access Management Control | Documentation including technical measures that reflect the prevention of:<br>• Unauthorized user access to system<br>• Unauthorized user access to Confidential Information, which includes Fannie Mae Confidential Information (as those terms are defined in the ISBR) | |
| Access Control Policies for:<br>MFA Password Management | • Documents evidencing Multi-Factor Authentication (MFA) implementation | |

| **The Following Documents Are Required to Complete a Full Information Security Assessment of the Document Custodian**: | | |
|---|---|---|
| **Area of Assessment** | **Document Type / Acceptable Format(s) and/or Document Purpose:** | **Requirement:** |
| | • Documents evidencing password management | |
| Policies or procedures evidencing on-boarding processes for employee candidates and contractors that will have access to Fannie Mae Confidential Information or Fannie Mae systems | Documentation must include:<br>• Steps for completing background verifications<br>• Evidence related to background check records<br>• Code of Conduct policies<br>• Examples of training records | Access includes direct or indirect means such as application programming interface or interfaces that allow for such integration to the Fannie Mae system |
| Evidence of Information Security Awareness Training | • Information security awareness training policies and procedures | Training required for all employees, contractors and other authorized parties working through the Company with access to Fannie Mae Confidential Information or Fannie Mae Systems. |
| Physical and Environmental Protection Policy & Procedures | • Supporting documentation as evidence of physical and environmental protection guidelines | |
| Where systems or applications are utilized in the performance and delivery of Document Custodian related action | Obtain:<br>• Independent third-party provided network/system/application penetration test results, or summary reports of test results for tests performed on networks, applications, systems and/or system components used to store, access process or transmit Confidential Information or those connected to a Fannie Mae system<br>• Relevant vulnerability scanning /testing results | Penetration test results from testing conducted within the last 12 months |
| Incident Response Plans | • Policies, standards and procedures for incident response plan;<br>• Test results of incident plan testing; OR<br>• Results of actual incidents that occurred within 12-month period | Results for testing of the incident response plan performed within last 12 months |

| **The Following Documents Are Required to Complete a Full Information Security Assessment of the Document Custodian**: | | |
|---|---|---|
| **Area of Assessment** | **Document Type / Acceptable Format(s) and/or Document Purpose:** | **Requirement:** |
| Asset Management Controls | • Policies, Standards or Procedures | |
| Encryption Standard | • Documentation addressing the cryptographic protection of data (both at rest and in transit). | |

***Note:** The independent assessment report must be performed by a qualified independent auditor not affiliated with the Company where "Company" means any entity that is expressly identified as being subject to this Supplement, including SF Lenders, MF Lenders, Document Custodians and Integrators (also referred to as third-party solution providers).

## 4 Guidelines for Audit Review & Results Submission

| **Review all Sections** | **Results:** | **Action Needed** |
|---|---|---|
| **1** | Gaps, Findings or Response = "No" | Provide additional explanation. |
| **2** | No Gaps or Findings Identified | Indicate as "No Gaps or Findings". |
| **3** | Requirements Not Applicable to Document Custodian | Indicate as **"N/A"**, provide explanation. |
| **4** | Responses Indicated as "Non-Compliance", "No" or "N/A" | Provide additional explanation. |
| **5** | Results that Meet Compliance – Respond as "Yes" or "Compliant" | No explanation required. |

## 5 Information Security Audit Review

| Review the relevant document(s) from Section 3 above to respond to questions below. Use guidance in Section 4 to provide responses. Include attachments as necessary. For additional attachments, please clearly label responses to the corresponding question(s). |
|---|

| | |
|---|---|
| **Section 5A: Access Management** | Review the Independent Third-Party Assessment or Audit Report and/or the Access Management Control Documentation. |
| | Validate the following:<br><br>1. Does the Access Control Policy exist?<br>a. Does evidence exist that confirms the access controls were tested or attested?<br>i. Were there major or significant deficiencies or failures noted in the report?<br>1. If yes, please include failures or deficiencies and any documented management responses if provided, in the auditor's response to Fannie Mae.<br>2. If no policy exists, then a "Finding" must be logged in the auditor's response to Fannie Mae.<br>2. Are there processes in place to grant/approve users access to system and data?<br>**Yes** ____ **No** ___ (Explain)<br><br>3. Are there processes in place for performing periodic user access reviews?<br>**Yes** ____ **No** (Explain)<br><br>4. Are there processes in place to deactivate user access to:<br>a. Systems: **Yes** ____ **No** ____ (Explain)<br>b. Data: **Yes** ____ **No** ____ (Explain)<br>**c.** Documentation containing Confidential Information: **Yes** **No** ____ (Explain) |
| **Section 5B: Human Resource Security** | Review the Independent Third-Party Assessment or Audit Report and/or any Onboarding Processes for Employees and Contractors or additional Evidence of Information Security Awareness Training. |
| | Validate the following – does the Document Custodian:<br><br>1. Have a formal on-boarding process that includes background verifications for all candidates/contractors that will have access to Fannie Mae confidential information or systems?<br>**Yes** ____ **No** _____ (Explain) **N/A** ____ (Explain)<br><br>2. Have a Code of Conduct or similar policies, standards and procedures to protect Confidential Information and systems for records management?<br>**Yes** ____ **No** _____ (Explain) **N/A** ____(Explain)<br><br>3. Conduct Information Security awareness training for all employees, contractors and authorized parties working on their behalf that have access to Fannie Mae information or systems at least annually?<br>**Yes** ____ **No** _____ (Explain) **N/A** ____(Explain) |
| **Section 5C: Audit and Accountability** | Review the Independent Third-Party Assessment or Audit Report and/or any systems that are utilized to deliver Document Custodian related services. |
| | Validate the following exist:<br>1. Enabled logging to track user activities for:<br>a. Applications **Yes** ____ **No** _____ (Explain)<br>b. Platforms: **Yes** ____ **No** _____ (Explain) |

| | |
|---|---|
| | c. Network Devices: **Yes** ____ **No** _____ (Explain)<br><br>2. A centralized log management system for collecting access and event logs.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. Processes to ensure event logs are reviewed at least once a week.<br>**Yes** ____ **No** _____ (Explain)<br><br>4. Controls that ensure only authorized personnel have access, modification and deletion rights to event logs.<br>**Yes** ____ **No** _____ (Explain) |
| **Section 5D: Vulnerability Patch Management** | Review evidence, assuming systematic usage of applications, systems, platforms, or networks in the delivery of document custodial related services. |
| | Validate the following:<br>1. The Document Custodian has implemented a monitoring program that identifies, analyzes and remedies vulnerabilities.<br>**Yes** ____ **No** _____ (Explain)<br><br>2. There are processes in place to ensure vulnerability scanning takes place following system / application changes include validation steps ensuring previously applied system and/or application patching remains.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. There is a process in place that differentiates the criticality of patches and remediation status be based on a risk-based schedule and per the Document Custodian's policies, procedures or standards addressing patch management.<br>**Yes** ____ **No** _____ (Explain)<br><br>4. The independent third-party penetration test results report includes if vulnerabilities were captured and if patching was applied.<br>**Yes** ____ **No** _____ (Explain) |
| **Section 5E: Physical and Environmental Controls** | Review documentation evidence for Physical and Environmental Protection Policy & Procedures and/or the Independent Third-Party Assessment. |
| | Validate the Document Custodian has the following:<br>1. A documented physical security program that governs the building/facilities.<br>**Yes** ____ **No** _____ (Explain)<br><br>2. Implemented process to ensure only authorized personnel have access to buildings and facilities, with periodic (annual) reviews.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. Process to remove physical and logical access immediately upon the voluntary or involuntary departure of an authorized individual and/or an individual no longer needing access to physical space.<br>**Yes** ____ **No** _____ (Explain) |

| | |
|---|---|
| | 4. Environmental Controls to prevent and mitigate the disruption to operations and data integrity (as applicable) caused by natural disasters or human-caused incidents.<br>**Yes** ____ **No** _____ (Explain) |
| **Section 5F: Incident Management and Response** | Review the Incident Response Plan to provide validation. |
| | Validate the Document Custodian has the following:<br>1. Incident response plans that consist of incident response policies, standards and procedures that include:<br>a. Identified required resources for the plan, including the management support needed to effectuate the incident response.<br>b. Identified roles and responsibilities.<br>c. A mobilization contact and call trees.<br>d. Severity assessment requirements.<br>e. Log recording steps and processes for evidence collection.<br>f. Steps for executing incident response capabilities.<br>**Yes** ____ **No** _____ (Explain)<br><br>2. A formal written notification process in place for all incidents, including cybersecurity and physical information-related incidents, that may disrupt operations that could potentially impair, or impact business.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. Process to validate that notification was provided to Fannie Mae and impacted parties per applicable requirements within the required notification timeframe for all known related incidents including cybersecurity and physical information-related incidents<br>4. **Yes** ____ **No** _____ (Explain) |
| **Section 5G: Asset Management** | Review the Asset Management documentation to provide validation. |
| | Validate that the Document Custodian:<br>1. Has a formal policy, standard or procedure that:<br>a. Address the development and maintenance of secure configuration baselines or infrastructure components,<br>b. Tracks and verifies physical and software assets (if utilized in the delivery of services) including the removal and addition of assets, and,<br>c. Conducts periodic maintenance on systems and technology to ensure protections and systems remain up to date with latest supported version and settings.<br>**Yes** ____ **No** _____ (Explain) |
| **Section 5H: Data Protection and System Security** | Review the Independent Third-Party Assessment or Audit Report and/or Encryption Standard or other documentation to provide validation. |
| | Validate the following exists in Document Custodian operations: |

| | |
|---|---|
| | 1. Electronic forms of documents secured by Document Custodian maintain encryption while at-rest and in-transit (if applicable).<br>**Yes** ____ **No** _____ (Explain)<br><br>2. Systems and communications protection controls are in place to help maintain the confidentiality and integrity of information at-rest and in-transit.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. Has implemented technical security measures designed to detect, mitigate, and prevent malicious and unauthorized use of technology assets.<br>**Yes** ____ **No** _____ (Explain)<br><br>4. Keeps all software up to date with supported versions according to the Company software update policy, standard, or procedure.<br>**Yes** ____ **No** _____ (Explain)<br><br>5. Has an established threat management process with steps to manage security threats as they are identified.<br>**Yes** ____ **No** _____ (Explain)<br><br>6. Maintain formal data management and encryption use policy, standards or procedures and prohibit use of outdated technologies which have identified vulnerabilities or are no longer supported by the software developer.<br>**Yes** ____ **No** _____ (Explain)<br><br>7. Encryption of electronic data stored on end user devices, (laptops, tablets, cell phones) to protect data if devices are lost or stolen.<br>**Yes** ____ **No** _____ (Explain)<br><br>8. Maintain a data loss prevention / transmission protection process that includes data loss prevention controls and a corresponding management process to identify Confidential Information stored on media and if applicable outgoing transmission over public communication.<br>**Yes** ____ **No** _____ (Explain)<br><br>9. Has implemented and maintains preventive controls and intrusion detection designed to identify potential threats and security compromises.<br>**Yes** ____ **No** _____ (Explain) |
| **Section 5I: Network Security and Management** | Review the Independent Third-Party provided network/system application penetration test results/summary report or the Independent Third-Party Assessment or Audit Report to provide validation. |
| | Validate that the Document Custodian operation has:<br>1. A strategy and controls to protect network security and monitor network traffic.<br>**Yes** ____ **No** _____ (Explain)<br><br>2. A strategy and controls to authenticate wireless network users and restrict unauthorized users.<br>**Yes** ____ **No** _____ (Explain)<br><br>3. Independent network penetration testing conducted regularly to identify vulnerabilities and attack vectors. |

| | |
|---|---|
| | **Yes** ____ **No** _____ (Explain) |
| **Section 5J: Supply Chain Risk Management** | Validate the existence of the following through documentation review:<br>1. An established vendor Risk Management / Third Party Risk Management Program to include policies, standards and procedures to measure and assess risk and impacts to business operations supporting the delivery of services to a Company's use of vendors.<br>**Yes** ____ **No** _____ (Explain)<br><br>2. An agreement in place with each vendor that covers adequate considerations for security consistency and in compliance with the requirements noted in this supplement.<br>**Yes** ____ **No** _____ (Explain) |