Independent Audit Requirements for Document Custodians – Business Resiliency Supplemental Requirement

Version 1.0

March 2026

Fannie Mae

Table of Contents

1 Document Revision History 2

2 Requirements for Business Resiliency Assessment 3

3 Documents Required for Audit Review 3

4 Guidelines for Audit Review & Results Submission 4

5 Business Resiliency Audit Review 4

1 Document Revision History

Date	Version	Change Description
March 2026	1.0	Initial Creation

2 Requirements for Business Resiliency Assessment

A Business Resiliency Assessment is required to ensure a Document Custodian's operations comply with the requirements 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 (AUP) results, but as a separate document.

3 Documents Required for Audit Review

The Following Documents Are Required to Complete a Full Business Resiliency Assessment of the Document Custodian:		
Areas of Assessment	**Document Type / Acceptable Format(s) and/or Document Purpose:**	**Requirement:**
Business Continuity Plan (BCP) and Testing Evidence	1) Business Continuity Plan (BCP) OR ISO 22301 Certification OR SOC 2 Type 2 AND 2) BCP Test/Exercise Results	BCP within last 12 months ISO Certification within last 36 months SOC 2 Type 2 includes external audit with management approval and no exceptions noted
Disaster Recovery (DR) Plan and Testing Evidence	1) Disaster Recovery Plan OR ISO 27031 Certification OR SOC 2 Type 2 AND 2) DR Test Results	IT Disaster Recovery Plan within last 12 months ISO Certification within last 36 months SOC 2 Type 2 includes external audit with management approval and no exceptions noted

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 Business Resiliency Audit Review

<table>
<tr><td colspan="2">Review the relevant document(s) in 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).</td></tr>
<tr><td>Section 5A: Business Continuity Plan (BCP) & Testing Evidence</td><td>Request and review the BCP and BCP test/exercise results within the last 12 months. Other acceptable forms of testing include:
• ISO 22301 Certification (completed within the last 36 months)
• SOC 2 Type 2 (Includes an external audit with no exceptions noted)</td></tr>
<tr><td></td><td>Obtain and review either of the documents referenced above:

1. Provide the following:
a. Management Signoff/approval.
Approval attached? Yes ____ No ___ (Explain)

b. Evidence of demonstrated recovery strategies (Loss of facility, technology, personnel, and third-party).
Evidence attached? Yes ____ No ___ (Explain)

c. Roles and responsibilities.
Evidence attached? Yes ____ No ___ (Explain)

d. Business impact analysis.
Evidence attached? Yes ____ No ___ (Explain)

e. Communication Strategy.
Evidence attached? Yes ____ No ___ (Explain)

1. Testing results to evidence successful execution of Document Custodian BCP and remediation action. Include exercise/testing activities and/or actual disruption that proves activation of BCP (if any).
Results attached? Yes ____ No ___ (Explain)</td></tr>
</table>

	2. Provide the Recovery Time Objective (RTO) or Service Level Agreement (SLA) times for all services that directly support Fannie Mae. Results attached? **Yes** ____ **No** (Explain)
Section 5B: Disaster Recovery (DR) Plan & Testing Evidence	The Independent Auditor must request and review the DR Plan and DR test/exercise performed within the last 12 months. Another acceptable form of testing includes: • SOC 2 Type 2 (Includes an external audit with no exceptions noted)
	Provide the Document Custodian DR Plan to ensure compliance with Fannie Mae requirements. 1. Provide evidence that demonstrates appropriate preparedness in the event of system or application failure, including: a. Description of technology used to support and facilitate business with Fannie Mae and Strategy Scenarios for recovery (dispersion, critical communication, , etc.) Evidence attached? **Yes** ____ **No** _____ (Explain) b. Procedure/Recovery Steps Evidence attached? **Yes** ____ **No** _____ (Explain) c. Recovery Teams Evidence attached? **Yes** ____ **No** _____ (Explain) d. Roles and Responsibilities Evidence attached? **Yes** ____ **No** _____ (Explain) e. RTO and Recovery Point Objective (RPO) Evidence attached? **Yes** ____ **No** _____ (Explain) f. Management signoff with date Evidence attached? **Yes** ____ **No** _____ (Explain) 2. Provide testing results (performed within the last 12 months) of the IT/DR exercise/testing activities or actual disruption or material change, if any. Results attached? **Yes** ____ **No** _____ (Explain) Has there been any disruption, including a Cybersecurity Incident, within the last 12 months? **Yes** ____ **No** _____ (Explain) a. If **"Yes"** – provide a high-level After Action summary of the incident including: i. How it was identified ii. Steps taken to triage, contain, and remediate the incident iii. Decisioning around notifying the affected consumers, customers or third parties 3. Provide physical locations(s) (city, state, and country) for operations which support Fannie Mae services including data centers, operation centers and headquarters. Response attached? **Yes** ____ **No** _____ (Explain)

	a. Describe the specific services performed for Fannie Mae at each location. Response attached? **Yes** ____ **No** _____ (Explain) 4. Describe the type of technology that supports the services provided to Fannie Mae. (e.g. PaaS, SaaS, DaaS, IaaS) Response attached? **Yes** ____ **No** _____ (Explain) 5. Review and confirm that the technology supporting the services provided to Fannie Mae has the following recovery capabilities. a. In region redundant architecture (e.g. Multi-availability zones) **Yes** ____ **No** _____ (Explain) b. In-region resiliency and cross-region connectivity between business applications to include data backup. **Yes** ____ **No** _____ (Explain) c. Geographically distributed recovery capability (geographically distributed defined as at least 250 miles in separation) **Yes** ____ **No** _____ (Explain)
Section 5C: Subcontractors / Third Parties as Participants in Business Continuity Testing	Respond to the following questions regarding the participation of subcontractors or third parties as it relates to the Document Custodian Business Continuity Testing.
	1. Do you currently include third parties and subcontractors in your Business Continuity Testing? **Yes** ____ **No** _____ (Explain) 2. Do you engage any third parties or subcontractors that: a. Perform critical business functions that have high impact and are important and necessary to the work you do for Fannie Mae? **Yes** ____ **No** _____ b. Does the third Party or subcontractor provide data center operation? **Yes** ____ **No** _____ i. If **“Yes”**, for each third party or subcontractor, provide: 1. Name 2. Type of service provided 3. Data available to them 4. Location where third party of subcontractor performs the service. 3. Do you have contingency plans that include: a. Loss of Facility: **Yes** ____ **No** _____ (Explain) b. Loss of Technology: **Yes** ____ **No** _____ (Explain) c. Loss of Personnel: **Yes** ____ **No** _____ (Explain)

	d. Loss of Third Party (If applicable) **Yes** ____ **No** _____ (Explain) e. Recovery strategies in place for loss of third parties or subcontractors should they be unable to provide the required services to Fannie Mae? **Yes** ____ **No** _____ (Explain) 4. Have there been any disruptions, including any Cybersecurity Incident or data loss, with any of the third parties or subcontractors identified above within the last 12 months? **Yes** ____ **No** _____ (Explain) 5. Are any of the third Parties or subcontractors listed above providing any activities including support functions from an offshore location? **Yes (see #6)** ____ **No** _____ (Explain) 6. If 'yes' to 5 above, does the Business Continuity Plan address recovery strategies in the event that an offshore third party provider or subcontractor cannot deliver services that are critical to the function of the Document Custodian? **Yes** ____ **No** _____ (Explain)