SELLER/SERVICER RISK SELF-ASSESSMENT

Business Continuity and Disaster Recovery

Business continuity procedures are defined as plans to continue operations if adverse conditions occur, such as a storm, fire, or crime. The plan must include moving or recovering operations in another location if a disaster occurs at a worksite or data center.

Disaster recovery is defined as a documented process or set of procedures to recover and protect a business's information technology infrastructure in the event of a disaster.

IN THIS DOCUMENT

RESOURCES

- *Selling Guide* A4-1-01, Maintaining Seller/Servicer Eligibility

ONE SELLER/SERVICER'S STORY

We have a successful and well-run business, but we feel vulnerable to external risk factors. For example, a recent hurricane caused a loss of power at our headquarters. Our employees couldn't access the company network remotely, forcing our business to close until power was restored. We could have minimized significant business loss if we had a contingency plan in place to ensure critical business operations. What elements go into an effective business continuity plan to protect our business from unexpected events or disasters?

Self-Assessment Checklist REQUIRED

BUSINESS CONTINUITY

- ☐ All sellers/servicers must have business continuity procedures in place that include:
  - Identification of critical functions and resources required to continue operations in the event of a business disruption or disaster.
  - Identification of alternate processing facilities.

DISASTER RECOVERY

- ☐ All sellers/servicers must have disaster recovery procedures in place that include:
  - Identification of critical functions and resources required to continue operations in the event of a business disruption or disaster.
  - Provisions for off-site retention of critical systems and data file resources.
  - Alternate network and telecommunication capabilities.

ADDITIONAL CHECKLIST ITEMS RECOMMENDED

- ☐ Business continuity policies and procedures, including procedures for updating and testing the business continuity plans.
- ☐ Retention of the documentation of the most recent tests of the business continuity plan, including date(s) and lessons learned.
- ☐ A business continuity cybersecurity incident response strategy.
- ☐ A process to ensure all employees have access to the business continuity steps for their department.
- ☐ A process to retain current employee contact information to support notification in the event of the implementation of the business continuity plan.
- ☐ An automated process to notify employees of the implementation of the business continuity plan.
- ☐ Disaster recovery policies and procedures, including procedures for updating and testing the business continuity plans.
- ☐ Retention of the most recent tests of the disaster recovery plan, including date(s) and lessons learned.
- ☐ Key vendors retain and understand the business continuity and disaster recovery activities.
- ☐ A process to test business continuity and disaster recovery plans simultaneously on an annual basis.

Common Findings and Documentation

MORTGAGE ORIGINATION RISK ASSESSMENT (MORA) AND SERVICER TOTAL ACHIEVEMENT AND REWARDS (STAR)

Fannie Mae conducts regular reviews to evaluate compliance with our guidelines and assess operational risks. Reviews are conducted by a team that operates independently of customer account relationship management in Fannie Mae's Single-Family mortgage business. A Mortgage Origination Risk Assessment (MORA) or Servicer Total Achievement and Rewards™ (STAR™) review is intended to be a joint activity conducted by the review team with the active participation of your organization.

The **common findings** and **required documentation** listed below are specific to the topic of this risk self-assessment, Business Continuity and Disaster Recovery.

COMMON FINDINGS

- The seller/servicer does not maintain a comprehensive written business continuity and/or disaster recovery plan(s).
- The seller/servicer does not regularly update their business continuity and/or disaster recovery plan(s).
- The seller/servicer does not regularly test their business continuity and/or disaster recovery plan(s).

REQUIRED DOCUMENTATION FOR A REVIEW

- Business Continuity/Disaster Recovery/Resilience Plan (BCP) — This plan identifies all business functions and prioritizes them in order of criticality analyzes related interdependencies among business processes and systems and assesses a disruption's impact through established metrics. The plan should define recovery priorities and resource dependencies for critical processes.
- Business Impact Analysis (BIA) — The BIA identifies all business functions and prioritizes them in order of criticality analyzes related interdependencies among business processes and systems and assesses a disruption's impact through established metrics. The BIA should define recovery priorities and resource dependencies for critical processes.
- BCP test evidence — Validation that recovery time objectives are met as defined in the BIA and stated in the BCP and dated within the last 12 months (rolling).
- After action reviews and plans — The documented activities identified after plan testing and/or activation of the plan. This should include root cause and accountability, controls reviewed and proposed changes, target completion timeframes, and tracking of the action plan's activities.
- Third-party vendor contingency plans — The supporting plans to assess critical third-party service providers' susceptibility to multiple event scenarios and verify third parties' resilience capabilities. This should include options to continue business operations, including the ability to move outsourced processes either in-house or to another third-party service provider. This should also include time parameter(s) for contracted service(s) and data confidentiality, integrity, and availability.

WHAT'S NEXT?

Use the insights you've gained — especially any gaps identified in your practices and processes — to create a customized action plan.