Seller/servicer risk self-assessment

Enterprise Risk Management

Enterprise risk management (ERM) in any business refers to the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying events or circumstances relevant to the organization's objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

In this document

Resources

- *Selling Guide* A4-1, Maintaining Seller/Servicer Eligibility
- STAR Program Reference Guide – Risk Management

The "Three Lines of Defense" Model

And other key principles of effective risk management

An effective risk management strategy may follow the "three lines of defense" model:

1. Business units and operations
   - Identify, assess, respond to, and monitor/report on risks.
   - Adhere to risk appetite, policies, standards, and limits/thresholds.

2. ERM, compliance, and support functions
   - Set standards for the first line of defense to manage and oversee risks.
   - Perform independent oversight and monitoring, and aggregate reporting on risk.
   - Develop and maintain the company's integrated risk management program.

3. Internal audit
   - Perform independent, systematic evaluation of the effectiveness of the internal controls employed by management.

An ERM strategy can answer three basic business questions:

1. Should we do it (aligned with business strategy, risk appetite, culture, values, and ethics)?

2. Can we do it (people, processes, structure, and technology capabilities)?

3. Did we do it (assessment of expected results, continuous learning, and a robust system of checks and balances)?
   - The types of risk exposure are not much different across varying business types and strategies:
     - Credit
     - Liquidity
     - Strategic/business/reputation
     - Market
     - Operational
     - Compliance/legal/regulatory
     - Financial
     - Capital adequacy
     - Digital/cybersecurity

Self-Assessment Checklist

Recommended

- ☐ An ERM framework is in place and aligned with business strategy, risk appetite, culture, values, and ethics.
- ☐ ERM function is in place.
- ☐ ERM committee is in place.
- ☐ Annual risk assessments are completed by all business units in an effort to support ERM.
- ☐ Corrective action processes are in place when issues are identified from enterprise risk oversight.
- ☐ An escalation process is in place to notify senior management of issues cited and status of corrective action.
- ☐ Enterprise risk and operational oversight of the following functions is in place:
  - Originations — retail and/or third-party originations
  - Servicing and sub-servicing, as applicable
  - Regulatory Compliance
  - Change Management
  - Vendor Management
  - Quality Control — origination and servicing quality control
  - Underwriting
  - Appraisal Management
  - Internal Audit
- ☐ Key steps to developing an ERM plan:
  - Consider a phased approach: Developing or significantly updating an ERM program requires active engagement from leadership as well as on-the-ground operational teams, which can feel overwhelming. To make it more manageable, consider developing the program in phases.
  - Leadership commitment: Leadership must be not only supportive but also fully engaged in the process.
  - Identify risks: Before conducting a risk assessment, the organization must identify and define categories of risk, levels of risk, and risk tolerances.
  - Comprehensive risk assessment: Conduct reviews to identify current risks by using past risk identification projects and internal/external audit findings. Rank the collective risks identified (most risky/least risky). This should also include identification of potential risks.
  - Regular and transparent reporting: Develop easy-to-understand dashboard reports.
  - Organizational alignment: Risk prioritization and mitigation strategies must align.
  - Communication protocols: Identification of risk does not stop when the project or audit ends — be sure to have a plan to remind staff members of your ERM strategy and to escalate potential emerging risks.

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 **required documentation, common findings, and corrective actions listed** below are specific to the topic of this risk self-assessment, Enterprise Risk Management.

Required documentation for a review

- Policies and procedures for the ERM framework, including the three lines of defense (if applicable)
- Policies and procedures that describes the overall risk management framework and governance used to manage internal controls and control exceptions for each line of defense (if applicable)

Common findings

- The seller/servicer did not provide the required documentation for Fannie Mae to complete an assessment.
- The seller/servicer must incorporate processes, controls, policies, and procedures to ensure consistency in Enterprise Risk Management.

Corrective actions

Corrective actions should require implementation of required policies and procedures, the identification of a control function to ensure they are updated on a regular basis, training for responsible parties, and validation that the required activities are completed in line with Fannie Mae *Selling* and/or *Servicing Guide* requirements.

WHAT'S NEXT?

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