Internal Audit Department
NeighborWorks® America

Audit Review of

Enterprise Risk Management

Project Number: NW.CORP.ERM.2024

Audit Review of Enterprise Risk Management

Table of Contents

TO: Members of the NeighborWorks America Audit Committee
of the Board of Directors

FROM: Frederick Udochi, Chief Audit Executive

CC: Marietta Rodriguez, President & Chief Executive Officer
Susan Ifill, Executive Vice President & Chief Operating Office
Nakeasha Sanders-Small, Executive VP, General Counsel/Corporate Secretary
Kemba Edmonds, Executive Vice President, Chief Financial Officer
Arturo Weldon, Executive Vice President & Chief Information Officer

RE: **Enterprise Risk Management**

DATE: October 31, 2024

Function Responsibility and Internal Control Assessment
Audit Review of Enterprise Risk Management

Business Function Responsibility	Report Date	Period Covered
Corporate	October 31, 2024	September 2021 through March 2024
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations		(b) (5)
Reliability of Financial Reporting		**Not Applicable**
Compliance with Applicable Laws and Regulations		**Not Applicable**

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

[1] **Legend for Assessment of Internal Control Structure: 1. Generally Effective:** The level and quality of the process is satisfactory. Some areas still need improvement. **2. Inadequate:** Level and quality of the process is insufficient for the processes or functions examined and require improvement in several areas. **3. Significant Weakness:** Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.

Executive Summary of Observations, Recommendations and Management Responses

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
Observation 1: ERM Framework Last Updated in 2019, Update and Review Frequency Unclear Internal Audit noted the most recent version of the ERM Framework obtained was as of 2019, five years ago. Typically, processes are periodically updated and formally documented in policies and procedures. The absence of periodical updates could potentially lead to Framework obsolescence and misalignment with the governance structure and current environmental trends. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 1: Review and Update ERM Framework on a Periodic Basis** Management should expand the ERM Framework into more detailed and descriptive policies and procedures that are updated at pre-defined intervals, at least annually, and communicated to staff. Management may also want to consider the governance structure of the ERM Committee such that dedicated resources are included to allow for consistent focus on policy, procedures, and the	**Yes**	Management will refresh an Enterprise Risk Committee that will draft an ERM Committee Charter and take responsibility for reviewing and updating the ERM Framework with a focus on policy and procedure and will provide an update to Senior Leaders on any changes that result.	06/30/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
		dissemination of this information.				
Observation 2: Absence of an ERM Charter Internal Audit noted the lack of an ERM charter. In the absence of an ERM Charter, roles and responsibilities of participants in the ERM Governance structure were unclear. In addition, there appears to be limited dedicated capacity and resources. The lack of dedicated ERM resources increases the risk that the organization will not be able to mature past the current state towards further enhancements to increased efficiencies and effectiveness. Availability of resources plays a part in how successful and sustainable an ERM program develops. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 2: Development of ERM Charter** The development of an ERM charter would facilitate the establishment of dedicated ERM governance. This should include at a minimum all critical assurance providers. Participants should have clearly defined roles and responsibilities that are documented and well communicated. Management should plan on dedicating more resources to ERM in order to access risk management expertise for the necessary skills	**Yes**	As part of the reconstitution of the NeighborWorks ERM Framework, a charter will be developed. Given budgetary constraints, existing staff will be identified to support the charter that is developed by the Enterprise Risk Committee.	06/30/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
		to further develop and implement ERM.				
Observation 3: Enterprise Risk Not Imbedded in Strategic Planning Process Internal Audit noted consideration of enterprise level risks are not included in the organization's strategic planning process. In addition, when developing divisional goals with consideration to enterprise risk, specific thresholds have not been set for risk criteria (risk tolerance). Risk assessments are not consistently conducted at the department level outside of Internal Audit's annual risk assessment. In the instances that risk assessments are conducted by departments, the frequency is inconsistent, the process is not standardized, and the risk assessment may not be documented. In most	**Yes**	**Recommendation 3: Explore the feasibility of Integrating Enterprise Level Risk at the Strategic Planning Stage** Recognizing that this would also need to be championed by the Board, Management should explore the feasibility of integrating enterprise level risk at the Strategic Planning stage. Risk identified at the enterprise level that would have an impact on accomplishing the organization's goals/objectives should be communicated downwards in order for departments/divisions to have a context for considering potential	**Yes**	For the FY25-FY27 Strategic Plan, enterprise risk was imbedded in the planning process. The ERM Committee (as reconstituted) will take steps to ensure enterprise risk is part of the strategic planning process going forward as well.	06/30/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
cases, for risks that are identified in the risk assessments, risk logs are not maintained, risk responses are not developed and documented, and key risk indicators are not consistently developed. If enterprise risks are not considered at the strategic planning stage, then there could potentially be the risk of not formally identifying or addressing the risk at the enterprise level and departmental/divisional level. **Risk Rating**: (b) (5)		risks which may become enterprise risks. Risk assessment should occur at least annually along with pre-determined risk tolerance thresholds for identified enterprise level risks. This would further facilitate the conduct of risk assessments and encourage staff in identifying and addressing enterprise risks should they occur or change.				
Observation 4: Inadequate Risk Criteria in ERM Framework The ERM Framework does not provide for risk criteria (risk thresholds and metrics) an essential component of ERM. Risk criteria enable the	**Yes**	**Recommendation 4: Enhance Current Framework with Risk Criteria** Management should, in the short term, develop and document risk criteria in order to	**Yes**	Risk Criteria will be designed and implemented as part of the ERM Risk Framework at NeighborWorks.	03/31/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline

effective evaluation and prioritization of the [2]risk assessment and mitigation process.
 	
In addition, Internal Audit identified that staff have mixed views about risk criteria including whether or not it has been defined and how it is communicated to staff. Most staff do not have a clear understanding of how risk criteria are used to identify risk or the process of reviewing the risk criteria. Most do not agree that the language used surrounding risk is consistent across the organization.
 	
The absence of clearly defined risk criteria can lead to inadequate risk identification and assessment. Additionally, inconsistent risk language across the organization makes accurately analyzing the risk
		maintain a consistent common language. This should include:
		
		• Risk thresholds
		• Risk metrics
		• Other metric definitions
		  o High
		  o Moderate
		  o Low
		  o Zero
		
		Management should integrate risk criteria into existing ERM processes and procedures, including regularly reviewing and refining risk criteria to ensure effectiveness.				

[2] Risk criteria are an adopted set of standards, measures, or expectations in enterprise risk management used to determine the significance of a risk assessed.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
more difficult, which can result in less effective decision making. **Risk Rating**: (b) (5)						
Observation 5: Definition and Communication of Risk Appetite in the ERM Framework The ERM Framework does not define the organization's risk appetite, another essential component for effective risk management and strategic decision making. The survey results indicated that staff are generally made aware of the Board's risk appetite in specific circumstances. If the risk appetite/tolerance levels are unclear, then the risk responses may not be in alignment with the strategic objectives and risk tolerance levels the	**Yes**	**Recommendation 5: Establish a Risk Appetite Statement as part of the ERM Charter** Establish a Risk Appetite Statement defining: • Overall risk tolerance • Risk categories and thresholds • Acceptable risk levels • Communicate risk appetite to stakeholders and risk owners	**Yes**	Management will establish a Risk Appetite Statement as part of the ERM Framework.	06/30/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
organization is willing to accept or tolerate. An organization's risk appetite/tolerance levels should be addressed by senior management and the board. It is documented and communicated with the ERM committee to facilitate risk taking and decision making. **Risk Rating**: [redacted]		Management should regularly review and refine risk appetite to ensure effectiveness.				
Observation 6: Reporting and Escalation of Identified Enterprise Level Risk While Internal Audit identified that there was a general awareness of the requirements for reporting enterprise level risk exposure, it was subsequently determined that: • The level of understanding of these requirements varies.	**Yes**	**Recommendation 6: Stakeholder Buy-In through Training and Awareness** We recommend that the Corporation educate stakeholders on the importance of ERM through training and communication sessions. Management should provide additional training on the early alert system,	**Yes**	Enterprise Risk Committee will incorporate a plan to educate staff as appropriate to improve general awareness of the requirements to report enterprise level risks. A communications plan will also be developed to include updates to the Audit Committee/Board.	12/31/2025	Internal Audit accepts Management's response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
• It is unclear whether enterprise risks identified in division risk assessments are consistently escalated to the ERM Committee. • Understanding of how an enterprise level risk should be escalated and reported to the ERM Committee via early alert system appears inconsistent. • No reporting of ERM activities to the BOD or Audit Committee Staff should be aware of how to identify and report enterprise level risk. When enterprise risks are not reported through the early alert system, it increases the likelihood of the risk not being		work to increase awareness of alternate reporting mediums (such as the anonymous reporting system, the newly created function of the VP Ethics and Compliance), and detail how and when these alternate mediums can be used. Management should also work towards developing a common language of risk in the definition and use of terms. In addition, ERM activities should be reported to the BOD or Audit Committee				

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response and Timeline
not being escalated timely or not captured at all. **Risk Rating**: (b) (5)						

Risk Rating Legend

Risk Rating: High
A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation's reputation.

Risk Rating: Moderate
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

Risk Rating: Low
A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

Management Responses to The Audit Review of: Enterprise Risk Management		
# Of Responses	**Response**	**Recommendation #**
6	Agreement with the recommendation(s)	1, 2, 3, 4, 5, 6
	Disagreement with the recommendation(s)	

Background

NeighborWorks America (NWA) began formalizing and implementing an Enterprise Risk Management (ERM) structure in 2016. The implementation commenced with the conduct of a risk assessment and identification of risk groupings by an external consultant engaged by the Corporation. Based on the result of this activity, a risk assessment and risk grouping were presented to the Senior Leadership Team (SLT) in June 2017. An ERM framework was ultimately developed internally with feedback from the Non-Profit Risk Management Center and was last updated in 2019.

While the Board has overall responsibility for ensuring that risks are managed, Internal Audit has an assurance role in ERM. This role requires that Internal Audit remain independent and objective. In this role, Internal auditors evaluate the effectiveness and contribute to the improvement of the risk management process (IIA Standard 2120 – Risk Management)[3]. The results of evaluations provide an understanding of the organization's risk management processes, their effectiveness, and overall risk management maturity.

Since maturity levels, approaches, strategies, and focus of risk management-related functions often depend on the organization's size and complexity; life cycle and stakeholder structure there is no one size fits all. There are numerous risk management frameworks currently available and regardless of which framework is used there are a number of elements which are present in an effective and efficient ERM. As a result, the goal is not to achieve an optimum level but to have an ERM maturity level that effectively and efficiently meets the needs of the organization. Strategies may vary however, based on commonly known attributes of mature risk management structures, benchmarking the current state of the organization's risk management against a risk management maturity model can help to identify areas of opportunity for growth, reducing risk and increasing effectiveness and efficiency.

Objective

The objective of this review was to obtain reasonable assurance that ERM has been incorporated into business systems to facilitate effective identification of internal and external risks as it affects the strategic goals and objectives of the corporation.

Scope

September 2021 through March 2024

Methodology

Internal Audit held a kick-off meeting with the ERM Executive Sponsor (Chief Financial Officer) and the ERM Senior Advisor (SVP, Organizational Assessment Division) to obtain a high-level understanding of the ERM process. Both individuals were also interviewed separately to gain more in-depth insight into the program and its policies and procedures from their individual perspectives. Documentation related to the ERM process was obtained and reviewed

[3] The IIA International Professional Practices Framework (IPPF) 2017 edition

including but not limited to draft enterprise risk assessment, risk groupings, emails, ERM Framework, and various quarterly business review presentations.

In addition, two surveys were conducted to benchmark the current state of the organization's ERM program; One for Senior Vice Presidents and another for select managers identified as participating in the ERM processes. The questions were developed using the Institute of Internal Auditors (IIA) Practice Guide[4]. Internal Audit collaborated with the Corporate Strategy & Impact (CSI) team to refine the survey methodology and questions, administration of the surveys, and assistance in the interpretation of survey results.

The analysis of the surveys, combined with interviews, and review of documentation were used to assess the current level of ERM maturity and identify opportunities for improvement to the current process.

Below are the observations and recommendations that resulted from the testing performed.

Observations and Recommendations

Observation 1: ERM Framework Last Updated in 2019, Update and Review Frequency Unclear

Internal Audit noted the most recent version of the ERM Framework obtained was as of 2019, five years ago. Typically, processes are formally documented in policies and procedures. The frequency and method of review and updates are documented and occur on a regular periodic basis.

While the framework does identify the frequency of a certain task, the framework documents the process at a high level and does not include the level of detail that typical policies and procedures provide. For instance, the framework does not specifically identify who is responsible for updates to policies and procedures or the cadence that reviews and updates are required. Outside of the ERM Framework and a few paragraphs in the Administrative Manual, the process does not appear to capture in detail formal policies and procedures. As a result, the "how to" or "procedural processes" of the tasks identified in the framework were absent.

The absence of periodical updates could potentially lead to Framework obsolescence and misalignment with the governance structure and current environmental trends. This increases the risk that corresponding policies and procedures may not be regularly reviewed and updated. In addition, the policies and procedures may not be reflective of the circumstances currently in the environment.

Recommendation 1: Review and Update ERM Framework on a Periodic Basis

Management should expand the ERM Framework into more detailed and descriptive policies and procedures. These polies and procedures should be updated at pre-defined intervals, at least annually, and communicated to staff. Management may also want to consider the governance structure of the

[4] The IIA International Professional Practices Framework (IPPF) Supplemental Guidance, Assessing the Risk Management Process, March 2019

ERM Committee such that dedicated resources are included to allow for consistent focus on policy, procedures, and the dissemination of this information.

Observation 2: Absence of an ERM Charter

The current composition of the ERM Governance Framework consists of an executive sponsor (CFO), a senior advisor (SVP Organizational Assessment Division), the risk committee (the Senior Leadership Team - SVPs/Officers), and Independent Review (Internal Auditor). In the absence of an ERM Charter, roles and responsibilities of participants in the ERM Governance structure were unclear. There should be a charter for the ERM Committee that establishes and defines roles and responsibilities and should be inclusive of critical functions (Information Technology, Human Resources, Procurement, Finance, Ethics and Compliance etc.). Although the risk committee is comprised of SVPs and Officers instances were identified where members were either unaware of their inclusion in the Committee or were unaware of their roles or both. For example, contrary to the ERM Framework, one ERM risk committee participant described their role as a volunteer. In the absence of an ERM charter frequent changes at the SLT level have contributed to a lack of awareness and buy in which has created an unevenness regarding participant engagement.

In addition, there appears to be limited dedicated capacity and resources, typical in the nonprofit environment, making it difficult to allocate resources to ERM initiatives due to other mission oriented competing priorities. The lack of dedicated ERM resources increases the risk that the organization will not be able to mature past the current state towards further enhancements to increased efficiencies and effectiveness. Availability of resources plays a part in how successful and sustainable an ERM program develops.

Recommendation 2: Development of ERM Charter

The ERM Framework and ERM charter should complement each other. The development of an ERM charter would facilitate the establishment of dedicated ERM governance. This should include at a minimum all critical assurance providers (Finance, IT, HR, OGC, Procurement, Ethics and Compliance, and FPAC). Participants should have clearly defined roles and responsibilities that are documented and well communicated.

The availability of resources plays a part in how successful and sustainable an ERM program develops. Management should plan on dedicating more resources to ERM in order to access risk management expertise for the necessary skills to further develop and implement ERM.

Observation 3: Enterprise Risk Not Imbedded in Strategic Planning Process

The consideration of enterprise level risks that could impact strategic goals and/or objectives facilitates the identification of critical risks that can hinder the achievement of strategic objectives and the organization's ability to deliver on its mission. Internal Audit noted consideration of enterprise level risks are not included in the organization's strategic planning process. As a result, it is not possible to tie and relate potential threats and opportunities to the organization's goals/and or objectives from an enterprise level. Relating strategic goals/objectives with potential risks or opportunities greatly facilitates the development of divisional goals and the establishment of divisional risk logs/registers which in this environment are collectively the conduct of risk assessments.

In addition, when developing divisional goals with consideration to enterprise risk, specific thresholds need to be set for risk criteria (risk tolerance). Risk assessments are also not consistently conducted at the department level outside of Internal Audit's annual risk assessment. In the instances that risk assessments are conducted by departments, the frequency is inconsistent, the process is not standardized, and the risk assessment may not be documented. In most cases, for risks that are identified in the risk assessments, risk logs are not maintained, risk responses are not developed and documented, and key risk indicators are not consistently developed.

If enterprise risks are not considered at the strategic planning stage, then there could potentially be the risk of not formally identifying or addressing the risk at the enterprise level and departmental/divisional level. Staff may not be able to conceptualize how to react to divisional risks, which could potentially be enterprise risks, without being provided with the nature of the strategic objective risk and if they are unaware of how these risks might impact their goals and objectives. Currently, each department/division determines risks in silos from a departmental/divisional level, adopting individual risk tolerance levels (metrics) that may not align with the Strategic goals/objectives.

Recommendation 3: Explore the Feasibility of Integrating Enterprise Level Risk at the Strategic Planning Stage

Recognizing that this would also need to be championed by the Board, Management should explore the feasibility of integrating enterprise level risk at the Strategic Planning stage. Enterprise level risk should be discussed and integrated into the organization's strategic planning process. Risk identified at the enterprise level that would have an impact on accomplishing the organization's goals/objectives should be communicated downwards in order for departments/divisions to have a context for considering potential risks which may become enterprise risks. Risk assessment should occur at least annually along with pre-determined risk tolerance thresholds for identified enterprise level risks. This would further facilitate the conduct of risk assessments and encourage staff in identifying and addressing enterprise risks should they occur or change.

Observation 4: Include Risk Criteria (Risk Tolerance) in ERM Framework

While the ERM Framework identifies risk categories (e.g. financial, operational/human capital, legal & compliance, information technology, political and reputational) in the taxonomy along with their corresponding risks, the framework does not provide for risk criteria (risk thresholds and metrics), an essential component of ERM. Risk criteria enable the effective evaluation and prioritization of the [5]risk assessment and mitigation process. The omission hinders effective risk assessment, mitigation and monitoring. It results in inconsistency and insufficiency in the decision-making process.

In addition, Internal Audit identified that staff have mixed views about risk criteria and are divided as to whether NeighborWorks America has defined a set of risk criteria applicable to the entirety of the organization. Most do not have a clear understanding of how risk criteria are used to identify risk or the process to review the risk criteria. There is also a lack of consensus as to when and how

[5] Risk criteria are an adopted set of standards, measures, or expectations in enterprise risk management used to determine the significance of a risk assessed.

the risk criteria are communicated. Most do not agree that the language used surrounding risk is consistent across the organization.

The absence of clearly defined risk criteria can lead to inadequate risk identification and assessment. Additionally, inconsistent risk language across the organization makes accurately analyzing the risk more difficult, which can result in less effective decision making.

Established protocols suggest that organizations should clearly define risk criteria and communicate them to staff. Staff should have a good understanding of how risk criteria are used to identify risk and the process to update the risk criteria. In addition, there should be a common risk language that promotes a consistent view of risk and makes it easier to compare risk across the organization, analyze the risks, and make decisions.

Recommendation 4: Enhance Current Framework with Risk Criteria (Risk Tolerance Levels)

Management should, in the short term, develop and document risk criteria in order to maintain a consistent common language. This should include:

- Risk thresholds (e.g. the acceptance of moderate financial risk with annual budget variance of 10%, accept high risk for partnering with new community organizations to expand outreach, zero tolerance for harassment, discrimination or intimidation, low risk for client confidentiality, secure data storage etc.
- Risk metrics (Financial, Operational, Reputational, Strategic, Compliance, Technology, Programmatic & Governance)
- Other metric definitions
    - High: Accepts significant risk in order to achieve strategic objectives
    - Moderate: Maintain a balance between risk and reward with mitigating controls
    - Low: Places priority on stabilizing and being cautious in order to minimize risk
    - Zero: No tolerance for the risk and requires immediate mitigation

Management should integrate risk criteria into existing ERM processes and procedures including regularly reviewing and refining risk criteria to ensure effectiveness.

Observation 5: Definition and Communication of Risk Appetite in the ERM Framework

The ERM Framework does not define the organization's risk appetite, another essential component for effective risk management and strategic decision making. Risk appetite represents the amount and type of risk the organization is willing to accept or tolerate to achieve its objectives.

The survey results also indicated that staff are generally made aware of the Board's risk appetite in specific circumstances. If the risk appetite/tolerance levels are unclear, then the risk responses may not be in alignment with the strategic objectives and risk tolerance levels the organization is willing to accept or tolerate.

An organization's risk appetite/tolerance levels should be addressed by senior management and the board. It is documented and communicated with the ERM committee to facilitate risk taking and decision making.

Recommendation 5: Establish a Risk Appetite Statement as part of the ERM Charter

Establish a Risk Appetite Statement defining:

- Overall risk tolerance
- Risk categories and thresholds
- Acceptable risk levels
- Communicate risk appetite to stakeholders and risk owners

Management should regularly review and refine risk appetite to ensure effectiveness.

Observation 6: Reporting and Escalation of Identified Enterprise Level Risk

The ERM Framework identifies when a concern should be raised through ERM and outlines the early alert process for escalating specific risk issues. While Internal Audit identified that there was a general awareness of the requirements for reporting enterprise level risk exposure, it was subsequently determined that:

- The level of understanding of these requirements varies - most of the staff were neutral or only somewhat aware of the reporting requirements.
- It is unclear whether enterprise risks identified in division risk assessments are consistently escalated to the ERM Committee. When risks are escalated, the timeline for escalation ranges from within 24 hours to within two weeks.
- Understanding of how an enterprise level risk should be escalated and reported to the ERM Committee via early alert system appears inconsistent. Despite the early alert process being outlined in the ERM Framework, most staff do not use the early alert system to escalate risk. Instead identified enterprise risks are reported to SVPs or the Officers.
- There is no reporting of ERM activities to the BOD or Audit Committee charged with oversight over risk management activities.

Staff should be aware of how to identify and report enterprise level risk. Once identified, relevant risk information is captured and communicated in a timely manner across the organization, enabling staff and management to carry out their responsibilities. Staff should feel empowered to report the risk via the early alert system.

The ERM Framework outlines the early alert system, and it is an agenda item for the Quarterly Business Reviews. However, it is unclear how much training is provided on using the early alert system or how much time is devoted to training staff on identifying, reporting, and escalating enterprise risks.

When enterprise risks are not reported through the early alert system, it increases the likelihood of the risk not being not being escalated timely or not captured at all.

Recommendation 6: Stakeholder Buy-In through Training and Awareness

We recommend that the Corporation educate stakeholders on the importance of ERM through training and communication sessions. Provide additional training on the early alert system including risks associated with not using the early alert system and when to use this medium. In addition, management should work to increase awareness of alternate reporting mediums such as the anonymous reporting system, the newly created function of the VP Ethics and Compliance and detailing how and when these alternate mediums can be used in either reporting or escalating enterprise risk events. Management should work towards developing a common language of risk in the definition and use of terms by providing a Glossary to the framework.

In addition, ERM activities should be reported to the BOD or Audit Committee.

Conclusion

The audit review of Enterprise Risk Management noted the current process as adequate but there is room for further improvement. Successful aspects of the process include most staff are familiar with the ERM framework, most SVPs agree that the Officers at NeighborWorks America are supportive of Enterprise Risk Management, and quite importantly the overall culture appears to be conducive to open discussion and the consideration of risk in the operational areas. As indicated earlier on it should be noted that while it is not necessary to reach optimum maturity, implementation of these recommendations will bring the organization closer to a maturity level that provides an effective risk management framework considering the size, nature, and complexity of the organization.

Our interactions with the CFO and the SVP OAD were collaborative and productive. We would like to take this opportunity to extend our thanks to CSI and the survey/interview participants for their cooperation and assistance during this review.