Internal Audit Department
NeighborWorks® America

Audit Review of

The

FLUXX

Grant Application

Project Number: NW.FLD.FLX.2017

Audit Review of FLUXX

Table of Contents

March 19, 2018

To: NeighborWorks America Audit Committee

Subject: **Audit Review of FLUXX**

Enclosed is our draft audit report for the FLUXX review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: J. Bryson
T. Chabolla
R. Bond
R. Simmons

Function Responsibility and Internal Control Assessment
Audit Review of FLUXX

Business Function Responsibility	**Report Date**	**Period Covered**
IT&S	March 19, 2018	July 1, 2017 to December 31, 2017
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations	**Generally Effective**[1]	
Reliability of Financial Reporting	**Not Applicable**	
Compliance with Applicable Laws and Regulations	**Not Applicable**	

This report was reissued February 15, 2024 in accordance with a recommendation by the Government Accountability Office (GAO-23-105944, June 14, 2023).

[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
Observation 1 The review of the processes and procedures for handling system changes indicated that there is no systemic reporting and related reconciliation processes in place to ensure that only authorized changes have been made. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 1** Management is recommended to implement systemic reporting to identify when changes are made to the FLUXX system. In addition, reconcile the changes per the systemic report to supporting authorizations to ensure that only approved changes have been made.	**Yes**	Fluxx currently doesn't have the capability to monitor admin activities. We have already communicated the importance of having this capability in Fluxx during our meeting with Fluxx Management team on Feb. 16, 2018 and multiple times before. Fluxx said they have added this request to their product change request queue and it will be considered in 2019. Until the functionality is available, we have	9/30/2019	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
				been following strict admin access request procedure. Please refer to the document attached "Grants Portal Admin Access Request Procedure" for a detailed procedure.		
Observation 2 The review of the processes and procedures on system permissions indicated that entitlement review is not currently performed for all FLUXX users and administrator accounts. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 2** Management is recommended to implement a process for a periodic (e.g. semi-annual) review of the FLUXX system permissions to ensure appropriateness of accounts and roles defined.	**Yes**	Grants Portal system launched at the end of July and it has been live for 7+ months. We have established multiple monitoring procedures and admin access is strictly restricted to very few users. A procedural document is already in place to monitor user access management. This	7/30/2018	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
				document was submitted to the auditors during the auditing process. We have updated this document to review system permission for users on a semi-annual basis. We have done the auditing for user access permissions on 7/25/2018 and the audit summary report is attached. Please refer to "Grants Portal User Access Permissions Audit Summary"		

Executive Summary of Observations, Recommendations and Management Responses (continued)

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
Observation 3 Review of the FLUXX user access indicated that Fluxx was granted full access to the NeighborWorks' grants system via Fluxx Admin account, which include setting or maintaining user accounts, making changes to the FLUXX application, and functions to initiate and approve grant applications. **Risk Rating**: (b) (5)	**Yes**	**Recommendation 3** NeighborWorks should determine the appropriateness of the vendor's persistent access to the financial data. Where persistent access is needed, procedures should be put in place to monitor activities performed by the vendor. Implement a time limited access to 3rd parties based on specific job assigned and limit access (e.g. capabilities to process financial transactions) to critical information/ application with only the functions needed to complete the job.	**Yes**	We have disabled Fluxx's admin accounts so they do not have persistent access to the Grants Portal system now. IT&S reactivates their account on a need basis.	4/30/2018	Internal Audit Accepts Management's Response

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: FLUXX		
# Of Responses	**Response**	**Recommendation #**
3	Agreement with the recommendation(s)	3
	Disagreement with the recommendation(s)	

Background

NeighborWorks America's management migrated a new Grant application (FLUXX) from the legacy system GrantWorks. FLUXX is hosted and maintained by a third party vendor. Even though hosted, NeighborWorks is still responsible for establishing and maintaining security assurance around cloud-based information technology assets from unauthorized access, use or disposition and the integrity of data or transactions that reside within.

SBC under the supervision of the Chief Audit Executive (CAE) conducted a post implementation review of the FLUXX grant management application. SBC's responsibility was to conduct these internal audit procedures over this migrated grants application and report finding/ recommendations to NeighborWorks.

Objective

The objective of this review was to obtain reasonable assurance that FLUXX as a grant making application process meets critical program objectives in terms of functionality and transactional performance. The review would examine input and output transactional data, application controls, delegation of authority and external interfaces with other relevant applications.

Scope

The scope of this audit included an evaluation of the adequacy and effectiveness of the processes and controls associated with the FLUXX application. The audit period is July 1, 2017 to December 31, 2017.

Our audit focused specifically on the following areas:

- Data migration from GrantWorks (the legacy application) to FLUXX.
- Adoption of Corporations IT Project Governance standard operating procedures (SOP).
- FLUXX integrations/interfaces, system controls, identity and user access authentication, access rights, segregation of duties in respect of grant approvals, compliance with the corporations delegation of authority; grantee and grantor requirements including adherence to applicable policies/procedures.
- FLUXX master and transactional data.

Methodology

We obtained an overall understanding of the Fluxx application, performed risk assessments, evaluated controls, evaluated the operating effectiveness of those controls, and reviewed documentation related to the migration process, IT project governance and oversight, grants application controls including system permissions, and FLUXX interface with NetSuite application.

The following specific procedures (i.e. inquiry, inspection of documents, and observation) performed were included but not limited to:

- Determining that data migration from the legacy application was properly executed in terms of process steps, grant management requirements, record retention and data integrity.
- Determining that Corporations IT Project Governance standard operating procedures (SOP) were adopted.
- Assessing the sufficiency and adequacy of integrations/interfaces, system controls, identity and user access authentication, access rights, segregation of duties in respect of grant approvals
- Determining that grant data and relevant processes are in compliance with the corporation's delegation of authority; grantee and grantor requirements including adherence to applicable policies/procedures.
- Reviewing master and transactional data.

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

Observations and Recommendations

Observation 1

Change Management:

The business rules within the FLUXX application define the sign-offs and reviews required to approve a grant application request. When changes are needed to be made to components of the application including business rules, NeighborWorks performs testing of changes. However, the review of the processes and procedures for handling system changes indicated that there is either the lack or non-compliance with a formal systemic reporting and related reconciliation processes in place to ensure that only authorized changes have been made.

As a result, there is an increased risk that inappropriate or unauthorized changes to business rules, data, or other critical areas to FLUXX application that may not be detected and addressed in a timely manner. If the business rules are not functioning properly, systemic functions may not ensure that all of the required reviews and approvals have been obtained on a grant request.

Recommendation 1

It is recommended that management implement a formal systemic reporting to identify when changes are made to the FLUXX system. The current Change Request Process known as CAB which is a change management system already in place could be used to facilitate this recommendation. The flux change Manager should pre-approve and initiate requests by submitting a CAB ticket to the Service Desk for final review and approval of IT Change Advisory Board prior to any work commencement. In addition, reconcile the changes per the systemic report to supporting authorizations to ensure that only approved changes have been made.

Observation 2

System Permission:
NeighborWorks has developed a process for user accounts registration, modification, and termination. Review and approvals are performed to ensure authorized individuals are granted access to data and application. Segregation of roles such as application processing, review, and approval have been defined in FLUXX system

However, the review of the processes and procedures on system permissions indicated that entitlement review is not currently performed for all FLUXX user and administrator accounts. Absence of above control increases the risk that unauthorized system permissions or capabilities may not be identified and corrected in a timely manner.

Recommendation 2

NeighborWorks Management is recommended to implement a process for a periodic (e.g. semi-annual) review of FLUXX system permissions to ensure appropriateness of accounts and roles defined. This should be documented as part of the Access-Rights corporate policy document.

Observation 3

Vendor Access:

Review of the FLUXX user access indicated that external individuals/third party users were granted full access to NeighborWorks' grants system which include setting or maintaining user accounts, making changes to the FLUXX application, and functions to initiate and approve grant applications. The vendor currently has persistent access to the FLUXX application. While manual mitigating controls are in place, vendors should not be able to have this level of permissions to the application unmonitored.

As a result, there is a risk exposure that inappropriate actions or errors could be performed using these super permissions without monitoring controls in place.

Recommendation 3

Management should determine the appropriateness of the vendor's persistent access to the financial data. Where persistent access is needed, procedures should be put in place to monitor activities performed by implementing time limitations to access by the vendor.

It is recommended that management implement a time limited access to 3rd parties based on specific job assigned and limit access (e.g. capabilities to process financial transactions) to critical information/application with only the functions needed to complete the job.

Conclusion

The FLUXX application system is a critical tool because it facilitates the delivery of grants to the community which is a core function of the Corporation. All the recommendations here can be incorporated into an Access-Rights corporate policy document for cloud based vendors. We hope that the recommendations raised here would be adopted accordingly in order to provide the necessary framework for monitoring the FLUXX application in order to maintain security, integrity and accessibility to corporate transactional data. We would like to take this opportunity to thank the staff of Information Technology and Services for their cooperation throughout this review.

Grants Portal Admin Access Request Procedure
Grants Portal Admin Account

There are two active Grants Portal admin accounts. These two accounts are needed to support the continuation of the business in case one account owner is not available.
The accounts are used to grant admin access to a team member who is responsible for the deployment.
To ensure the separation of duties, these accounts are not used for any deployment and serve as the gatekeeper accounts.

Request Temporary Admin Access to Grants Portal

A ticket should be submitted to request an admin access to the Grants Portal production environment.

The admin access can be requested for new deployments, troubleshooting of issues or small non-functional changes, e.g., text changes.

A change authorization request must be submitted for all new grant application deployments, workflow changes, and bug fixes**.** Change Authorization Board(CAB) reviews the request and approves it. Not all request requires CAB request. For example small text changes doesn't require CAB approval.

If a CAB request is required, the CAB request should be approved before creating a ticket.

A team member responsible for the deployment will open a ticket to request admin access to the production environment. The ticket should be assigned to IT&S Director and Lead Software Engineer.

The ticket must have the information listed below:

- Purpose of the deployment or troubleshooting
- Functionality to deploy or issue to troubleshoot
- Deployment/troubleshooting timeframe
- If CAB is approved, specify

After completion of the deployment, the team member will remove the admin access from him/herself, make a screenshot with the date and time and attach the screenshot to the ticket.

The team member will also send email from the ticketing system to IT&S Director and Lead Software Engineer to let them know that the deployment has been completed.

The IT&S Director and Lead Software Engineer will review and close the ticket.

General Fluxx Safety Features

FLUXX Session Timeout is currently set for (b) (5) minutes. If there are no activities, application will automatically log the user out.

FLUXX account will be locked after (b) (5) tries.

Grants Portal User Access Permissions Audit Summary
(07/25/2018)

The report of individual user access privileges was created and reviewed to ensure the least amount of privilege necessary was granted and that segregation of duties exists so no single user can circumvent a critical process in the system.

The users with multiple roles were especially carefully reviewed to make sure that the security privileges granted to the users support segregation of duties.

The issues listed below were identified:

1. **Test IDs available in production environment**

   8 active test ids and 29 inactive ids were found in the production environment, including 1 active vendor developer's id.

   All test ids were removed from the production environment.

   List of active Test IDs:

Full Name	Email	Login	Program
Test Tester	(b) (5)	(b) (5)	All
Test User			All
rom user2			
Fluxx Support			All
Grantee AO Test			All
OAD Emp Test			All
President User			
Finance OAD			

List of Non-active Test Ids:

Full Name	Email	Login
Hanna Tester	(b) (5)	
test user1		
Data Sync		
App Tester2	(b) (5)	
NWOTest ApplicationAdmin		
Michael Doe	(b) (5)	
K James		
Agate IA		
Agate NIAR Director		
Agate NWAdmin		
Agate AppAdmin		
Agate AO		
Peter Smith		
New User		
Tom Smith		
Frank Smith		
Eric Smith		
TFirst TLast		
CDE FGH		
John Smith		
System Admin		
Angela Test		
Angela Test	(b) (5)	
Mary InitialReviewer		
Test MailTest		
ResOpp Tester		
test user80		
App Tester		
Test LeadReviewer	(b) (5)	

2. The active external reviewer ids were identified and the reviewer names were sent to the business teams for confirmation of access:
    a. CORE business team confirmed that 2 external reviewers are currently reviewing CORE applications and the accounts should remain active.
    b. Project Reinvest business team and National Initiative business team confirmed that no reviews are currently going on and the ids can be deactivated.

108 external reviewer ids were deactivated.