

OFFICE OF
INSPECTOR GENERAL

Audit Report

Examination of Business Continuity
at Farm Credit System Institutions
A-16-02

Auditor-in-Charge
Tammy Rapp

Issued June 1, 2016



FARM CREDIT ADMINISTRATION



June 1, 2016

The Honorable Kenneth A. Spearman, Board Chairman
The Honorable Dallas P. Tonsager, Board Member
The Honorable Jeffery S. Hall, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Board Chairman Spearman and FCA Board Members Tonsager and Hall:

The Office of Inspector General completed an audit of the Examination of Business Continuity at Farm Credit System (FCS or System) Institutions. The objective of this audit was to evaluate the Farm Credit Administration's (FCA or Agency) process in determining which business continuity procedures were performed and whether there were any gaps during the Agency's examination process of FCS institutions identified by the Office of Examination (OE) as high risk.

FCA issued guidance in the form of directives and an *Examination Manual* that provides elements an examiner should consider during examination and monitoring of System institutions. As a result of our audit recommendations, OE modified a few references in the *Examination Manual* that needed updates.

In our review of the examination of business continuity procedures performed at System institutions, we observed documentation supporting the procedures performed and conclusions. In most cases, if a procedure was not performed, there was justification provided in the workpapers. In a few cases, the workpapers did not identify justification for skipping a procedure during the examination cycle. The reasons for not performing a procedure were a result of the risk based approach, resource availability, and priorities.

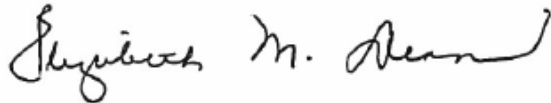
OE developed workpaper templates to be used during the examination of business continuity that describe the items an examiner should consider. Our audit identified the workpaper templates as an effective method for documenting the work performed and observations made during examinations of business continuity when they were used. However, the templates were not consistently included in the workpaper documentation.

As a result of our audit recommendations, OE took the following actions that will improve the examination of business continuity at FCS institutions:

1. Updated references in the *Examination Manual*.
2. Reminded examiners to document their justifications for examining or skipping the business continuity topic at System institutions.
3. Encouraged examiners to utilize workpaper templates when completing the business continuity examination procedures, especially those examiners with little or no experience in this area.

We appreciate the courtesies and professionalism extended by the FCA personnel to the Office of Inspector General staff. If you have any questions about this audit, Tammy Rapp, Auditor-in-Charge, and I would be pleased to meet with you at your convenience.

Respectfully,

A handwritten signature in black ink that reads "Elizabeth M. Dean". The signature is written in a cursive style with a large initial "E" and a long, sweeping underline.

Elizabeth M. Dean
Inspector General

Enclosure

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....1

INTRODUCTION & BACKGROUND.....2

AUDIT RESULTS.....4

Guidance Issued to Examiners..... 4

Business Continuity Procedures Performed by Examiners..... 7

Actions Taken 8

OBJECTIVE, SCOPE, AND METHODOLOGY.....10

ACRONYMS11



EXECUTIVE SUMMARY

EXAMINATION OF BUSINESS CONTINUITY AT FCS INSTITUTIONS

A-16-02

OBJECTIVE:

The objective of our audit was to evaluate FCA's process in determining which business continuity procedures were performed and whether there were any gaps during the Agency's examination process of FCS institutions.

ACTIONS TAKEN:

As a result of our audit recommendations, OE took the following actions to improve the examination of business continuity at FCS institutions:

1. Reminded examiners to document their justifications for examining or skipping the business continuity topic at System institutions.
2. Encouraged examiners to utilize workpaper templates when completing the business continuity examination procedures, especially those examiners with little or no experience in this area.

The Farm Credit Administration's (FCA or Agency) mission as a financial regulator is to ensure a safe, sound, and dependable source of credit and related services for agriculture and rural America. Section 5.19 of the Farm Credit Act of 1971, as amended, provides the FCA with the authority to examine Farm Credit System (FCS or System) institutions. FCA's Board adopted a policy to use a "risk-based" approach for the oversight and examination of System institutions.

FCA's goal is to have a flexible regulatory environment that facilitates electronic commerce and the use of information technology. However, institutions must establish good business practices that ensure safety and soundness. FCA Regulation, 12 CFR 609.930 requires FCS institutions to have policies and procedures that address "business resumption after disruption." Business continuity planning refers to the activities necessary to continue, resume, and recover an organization's business processes when operations are interrupted unexpectedly.

FCA issued guidance in the form of directives and an *Examination Manual* that provides elements an examiner should consider during examination and monitoring of System institutions. The *Examination Manual* contains specific guidance related to the examination of business continuity of System institutions. As a result of our audit recommendations, OE modified a few references in the *Examination Manual* that needed updates.

We reviewed the examination of business continuity procedures performed for 12 System institutions that were identified by OE as having the majority of transactional risk within the System.

- The examination workpaper documentation for 9 of the System institutions revealed business continuity procedures were either performed, or justification was documented for skipping any procedures during the current examination cycle.
- In our review of documentation for 3 of the System institutions, we determined there was a lack of documented justification for not performing certain business continuity procedures during the examination cycle. OE stated the procedures were not performed as a result of the risk based approach, resource availability, and priorities. OE agreed the *Risk Assessment Comments and Scoping Rationale* should reflect why the BCP topical area was being evaluated. Any supplemental guidance or information at the procedural level is optional for the examiner to complete.

OE developed workpaper templates to be used during the examination of business continuity that describe the items an examiner should consider. Our audit identified the workpaper templates as an effective method for documenting the work performed and observations made during examinations of business continuity. However, the templates were not consistently included in the workpaper documentation.

INTRODUCTION & BACKGROUND

The purpose of the Farm Credit Act of 1971, as amended, is, “To further provide for the farmer-owned cooperative system of making credit available to farmers and ranchers and their cooperatives, for rural residences, and to associations and other entities upon which farming operations are dependent, to provide for an adequate and flexible flow of money into rural areas, and to modernize and consolidate existing farm credit law to meet current and future rural credit needs, and for other purposes.”¹

The Farm Credit Administration (FCA or Agency) is an independent agency in the Executive Branch of the U.S. Government. The FCA is responsible for regulating and examining the Farm Credit System (FCS or System).

FCA’s mission as a financial regulator is to ensure a safe, sound, and dependable source of credit and related services for agriculture and rural America. Section 5.19 of the Farm Credit Act of 1971, as amended, provides the FCA with the authority to examine System institutions. FCA’s Board adopted a policy to use a “risk-based” approach to the oversight and examination of System institutions.²

FCA’s goal is to have a flexible regulatory environment that facilitates electronic commerce and the use of information technology (IT). However, FCS institutions must establish good business practices that ensure safety and soundness. FCA Regulation 12 CFR 609.930 requires policies and procedures that address “business resumption after disruption.” Business continuity planning refers to the activities necessary to continue, resume, and recover an organization’s business processes when operations are interrupted unexpectedly.

FCA issued Informational Memoranda to the System related to the importance of planning for catastrophic events and threats to information systems.

An Informational Memorandum on *Guidance on Preparing Your Institution for a Catastrophic Event* was sent to System institutions on June 22, 2006. This memorandum informed System Institutions about guidance that was issued by the Federal Financial Institutions Examination Council (FFIEC) related to lessons learned from Hurricane Katrina.

An Informational Memorandum on *Threats to Information Management Systems* was sent to System institutions on August 30, 1999. The purpose of this memorandum was to heighten the awareness of the increasing threat from “cyber-terrorism” and threats to information management systems. This memorandum specifically reminds System institutions of the importance of developing and testing disaster recovery and contingency plans.

FCA’s Office of Examination (OE) has primary responsibility for conducting examinations of System institutions to ensure the System operates in a safe and sound manner.

¹ Farm Credit Act of 1971, Pub. L. 92-181, 85 Stat. 583 (1971)

² FCA Policy Statement 53

In 2006, OE completed a national examination activity on IT. As part of this national examination activity, examiners evaluated the adequacy of business continuity planning at 28 System institutions. The results of this activity were sent to System institutions on December 19, 2006. The results memorandum included examples of good business continuity practices as well as areas for improvement. OE found that System institutions were taking business continuity planning seriously and had many controls in place to prevent or minimize the impact of potential adverse events. Specifically, they found that most institutions had good recovery plans for IT systems, as well as back-up and offsite storage facilities. However, examiners identified opportunities for improvement in the areas of risk assessment, training, testing, and audit coverage.

Guidance Issued to Examiners

FCA issued guidance in the form of directives and an *Examination Manual* that provides elements an examiner should consider during examination and monitoring of System institutions. The *Examination Manual* contains specific guidance related to the examination of business continuity of System institutions. As a result of our audit recommendations, OE took the following actions:

- modified a few references in the *Examination Manual*
- reminded examiners to document their justifications for examining or skipping the business continuity topic at System institutions
- encouraged examiners to utilize workpaper templates when completing the business continuity examination procedures, especially those examiners with little or no experience in this area

OE Examination Process Directives

OE issued three directives that outline the examination process and expectations as summarized below.

Institutional Examination Planning, #31, 3/18/2014

“This directive establishes expectations on planning examination and related activities throughout the institution’s examination cycle. The purpose of planning is to identify the objectives you want to accomplish in an examination and allocate examination resources to accomplish those objectives effectively and efficiently. The key underlying principals are: (1) all examination and related activities must be adequately planned, and (2) planning activities and Scoping Tools must be tailored to the institution in a risk-based manner.”

The *Scoping Tool* “facilitates OE’s risk-based and ongoing examination practices by helping Examiners-in-Charge (EIC) balance institution and examination risks when planning scope, depth, timing, and resources. The Scoping Tool must be approved prior to committing resources and be continually assessed and reevaluated throughout the examination process to balance examination risks and costs.”

The *Scoping Tool* contains a list of standard procedures for each topic. Since the examination is risk based, not every topic or procedure is required to be performed during an examination cycle. The EIC is responsible for determining which procedures will be performed based on the EIC’s risk assessment and resources available for the institution.

The *Scoping Tool* contains a section for EICs to document their *Risk Assessment Comments and Scoping Rationale* for each topic. The purpose of this section is to provide others with the reasons why an area was reviewed or skipped.

Examination Quality and Controls, #16, 6/25/2013

“This directive outlines expectations for examination quality and controls over work products and processes associated with the examination of System banks, associations, service corporations and other entities.” The directive documents the examination cycle workflow including the various levels of review.

“OE uses the Enterprise Documentation and Guidance (EDGe) application, and specifically the Examination Workprogram (EWP) for examination workpaper documentation...The primary objective of documentation and cross-referencing is to ensure the Reports of Examination (ROEs) and Activity Letters are substantiated by adequate, accurate, and relevant evidence.”

Monitoring, #22, 5/15/2013

This directive primarily outlines expectations for monitoring activities, “which are the activities associated with the ongoing oversight of System banks, associations, and service corporations. The objectives of monitoring are to timely identify and stay informed of emerging risks and issues in institutions in order to promote efficient and effective risk-based examination activities.”

If a higher level of risk is identified during monitoring activities, the examiner should adjust the procedures selected for examination in the *Scoping Tool* and document the results of those procedures in the EWP. “Examiners need to apply sound judgment, based on risks and resources, when determining the depth and breadth of both monitoring and examination work.”

Examination Manual

The *Examination Manual* contains guidance on elements an examiner should consider during examination and monitoring of System institutions. The *Examination Manual* is also available to System institutions on FCA’s public website.

As part of the risk based examination for an institution, examiners are provided the flexibility to determine the scope and select which procedures will be performed. The examiners use their knowledge of the institution and professional judgment to determine which procedures will be performed. Differences in scope and depth of examination between institutions or examination cycles may occur as a result of risk based examinations.

Although the frequency and scope of examination activities varies based on risk, each institution receives a summary of examination activities and a report on its overall conditions at least every 18 months. Oversight and examination activities include planning, monitoring, examination, reporting, and corrective actions. FCA issues a Statutory Compliance Date report every 18 months to each institution that summarizes the ongoing oversight and examination results of their examination cycle.

OE developed standard procedures for each topic that may be performed on an examination. However, since the examinations are risk based, not all procedures are performed. Additionally, the EIC may choose to supplement with custom procedures for an examination. As provided for in the EDGe guidance, “OE has two types of workpapers on the EDGe. The first type, monitoring workpapers, will be used on an ongoing basis during an EICs monitoring and are not associated with a specific

examination procedure. The second type, examination workpapers, are used to assist examiners in completing procedures. Not all procedures will have a workpaper. If there is a workpaper associated with a procedure, it is typically not required to be used (unless directed by OE management or the EIC for that examination).”

“Business continuity refers to the activities necessary to continue, resume, and recover an organization’s business processes when operations are interrupted unexpectedly... The focus of this examination topic and related procedures is on an enterprise-wide business continuity program. A sound program considers the business operations, personnel, technology, and resources that are critical for continuing the entire organization, not just the information technology (IT) department. As such, it is important for an institution’s business continuity program to include risk assessment, planning, training, testing, and maintenance processes.”³

A strong business continuity program will, “...ensure the organization can:

- Minimize disruptions of service to the institution and its customers,
- Ensure timely resumption of operations, and
- Limit financial loss.”⁴

The *Examination Manual* contains standard procedures for business continuity that may be performed on an examination.⁵ A summary of the standard procedures is described below:

1. Policies & Procedures
“Evaluate the adequacy of business continuity policies and procedures.”
2. Risk Assessment & Business Impact
“Review the institution’s business continuity risk assessment to determine whether management appropriately identified potential threats, related consequences, and the resulting impact to the institution.”
3. Business Continuity Plan
“Review the institution’s business continuity plan (BCP) to verify that the plan contains the components necessary to continue, resume, and recover the institution’s business processes when operations are interrupted unexpectedly.”
4. Disaster Recovery Plan
“Review the institution’s disaster recovery plan to determine if the institution is prepared to restore IT systems to support the institution’s recovery goals.”
5. Staff Training Program
“Determine if the institution provides adequate staff training to address a business disruption or disaster event.”
6. Testing Program
“Evaluate the adequacy of the institution’s annual BCP testing process.”

³ *FCA Examination Manual 31.6*

⁴ *FCA Examination Manual 31.6*

⁵ *FCA Examination Manual 31.6*

7. Audit

“Determine if the institution conducts an effective audit (scope, reporting, and followup) of the business continuity program.”

For each procedure, guidance and supplemental information is provided for the examiner. For example, OE included references to guidance and booklets issued by the FFIEC to assist examiners when reviewing business continuity planning. Additionally, OE presented examination guidance for business continuity at a Risk Management Conference in May 2014. This presentation is also linked in the *Examination Manual*. There are also links to National Institute of Standards and Technology (NIST) *Special Publication 800-34* and FCA Informational Memoranda related to business continuity.

During our audit, we identified a few references in the *Examination Manual* that should be updated. OE was responsive to suggestions we made to update the examination guidance and made the following changes promptly:

- a broken link was identified in the *Examination Manual* and corrected
- an outdated special publication from NIST was identified and corrected with a link to the current version
- FFIEC booklets referenced in OE's guidance were added to the *Examination Manual*
 - *Business Continuity Planning Process*
 - *Strengthening the Resilience of Outsourced Technology Services*

Business Continuity Procedures Performed by Examiners

We reviewed the examination of business continuity procedures performed for 12 System institutions that were identified by OE as having the majority of transactional risk within the System. The most recent examination of key technology service providers and systems banks were reviewed with a Statutory Compliance Date prior to January 1, 2016. We reviewed ROE and Activity Letters for conclusions related to the examination of business continuity. We reviewed the *Scoping Tool* to identify which business continuity procedures were selected. In the *EWP*, we reviewed the documentation supporting the business continuity procedures performed, results of the procedures reviewed, and conclusions.

The examination workpaper documentation for 9 of the 12 System institutions revealed business continuity procedures were either performed, or justification was documented for skipping any procedures during the current examination cycle. We observed documentation describing the procedures performed and conclusions made for each procedure. If a procedure was not performed, the documentation contained justifications for skipped procedures. The reason for not performing a procedure was often justified due to a review performed during the previous examination cycle that had no material concerns or timing of relocations of institution or disaster recovery site.

In our review of documentation for 3 of the System institutions, we determined there was a lack of documented justification for not performing certain business continuity procedures during the examination cycle. OE stated the procedures were not performed as a result of the risk based approach, resource availability, and priorities. Any supplemental guidance or information at the procedural level is optional for the examiner

to complete. *Institutional Examination Planning, #31*, provides guidance on documenting Risk Assessment Comments and Scoping Rationale. The directive states, “Examiners should use monitoring activities and knowledge of the institution to conduct the risk assessment and estimate staff days. Document this thought process and justify resulting decisions in the Risk Assessment Comments and Scoping Rationale section so others can understand the examination plan and decisions made. For example, EICs could document why the topic will or will not be examined...” As a result of our audit recommendations, the OE Operations Risk Program Manager communicated a reminder to examiners to document their justifications for the business continuity topic to be performed or skipped in the *Risk Assessment Comments and Scoping Rationale*.

Workpaper Templates

The *Examination Manual* contains links to 4 workpaper templates for business continuity:

1. *Risk Assessment and Business Impact*
2. *Business Continuity Plan*
3. *Disaster Recovery Plan*
4. *Testing Program*.

The workpaper templates cover the items an examiner should consider when performing the respective procedure. These templates contain questions that can be responded to with yes, no, or not applicable, as well as additional space to make comments. According to OE’s Operations Risk Program Manager, workpaper templates are optional and not required to be included in the examination workpapers.

Our audit identified workpaper templates as an effective method when they are used for documenting the work performed and observations made during examinations of business continuity. However, the templates were not consistently included in the workpaper documentation. Although there is a workpaper template for *Risk Assessment and Business Impact*, it was not included in any of the System institutions where this procedure was reviewed. The *Business Continuity Plan* workpaper template was included in 3 of the Systems reviewed. The *Disaster Recovery Plan* workpaper template was included in 2 of the Systems reviewed. The *Testing Program* workpaper template was included in 5 of the Systems reviewed. According to OE, the examination work for the 12 institutions examined was completed by IT Risk Specialists who have many years of experience and expertise in examining this area.

As a result of our audit recommendations, OE encouraged examiners to utilize these workpaper templates when completing the business continuity examination procedures, especially those examiners with little or no experience in this area.

Actions Taken:

1. OIG Recommendation: OE agreed to provide EICs with reminders to document their justifications for the BCP topic to be performed or skipped in the *Risk Assessment Comments and Scoping Rationale*.

Management Response: The current EDGe guidance provides a location within the Scoping Tool (*Risk Assessment & Scoping Rational* section) for

documenting why or why not the BCP topic will be examined. This is performed within each of the 29 topics in our scoping tool. The supplemental guidance at each of the 228 examination procedures is optional and available to provide additional direction to examiners performing these procedures. The Operations Risk Program Manager will send out a communication to examiners reinforcing the importance of documenting the rationale for examining BCP at the topic level within the risk assessment.

OE provided documentation reminding examiners to document justifications for the business continuity topic to be performed or skipped in the Risk Assessment Comments and Scoping Rationale using the following communication methods:

- 1. email communication to examiners*
- 2. posted reminder on OE SharePoint Announcements site*

OIG Reply: *OIG received documentation taking appropriate action and considers this item resolved.*

2. OIG Recommendation: *OE agreed to consider when to require the use of workpaper templates for documenting work performed and observations when performing respective business continuity procedures.*

Management Response: *OE would expect that lesser experienced and tenured examiners would utilize the BCP workpaper templates. Our current EDGe guidance provides for the optional use of these workpaper templates. The examination work for the 12 institutions examined by OIG was completed by our IT Risk Specialists who have many years of experience and expertise in examining this area. The Operations Risk Program Manager will send out a communication to examination supervisors to reinforce the use of the BCP workpaper templates for lesser experienced examiners.*

OE provided documentation that encouraged examiners to utilize workpaper templates when completing the business continuity examination procedures, especially those examiners with little or no experience in this area, using the following communication methods:

- 1. email communication to examiners*
- 2. posted reminder on OE SharePoint Announcements site*
- 3. updated EDGe guidance*

OIG Reply: *OIG received documentation taking appropriate action and considers this item resolved.*

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to evaluate FCA's process in determining which business continuity procedures were performed and whether there were any gaps during the Agency's examination process of FCS institutions identified by OE as high risk.

The scope of this audit focused on the business continuity procedures performed by FCA examiners at the 12 System institutions identified by OE in their fiscal 2016 Operations Risk Program Operating Plan as having the majority of transactional risk within the System. The most recent examination of key technology service providers and systems banks were reviewed with a Statutory Compliance Date prior to January 1, 2016.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objective, we performed the following procedures:

- Identified and reviewed related laws and regulations
- Identified related guidance issued to FCS institutions
- Identified related policies and procedures issued to examiners
- Identified which business continuity procedures were performed for the most recent examination
- Reviewed ROE and Activity Letters for any conclusions related to the examination of business continuity
- Reviewed the *Scoping Tool* to identify which business continuity procedures were selected
- Reviewed the *EWP*, including documentation supporting the business continuity procedures performed, results of the procedures reviewed, and conclusions
- Determined if there was a gap in procedures performed for business continuity
- Conducted interviews of key personnel with responsibility for related examination procedures

We reviewed internal controls identified as significant to the audit objectives and did not identify any material control weaknesses.

The risk of fraud and abuse was considered during the audit. Nothing came to our attention during the audit to indicate fraud or abuse was occurring.

We assessed the risk of the reliability of data used to achieve our audit objective and determined it was sufficiently reliable for purposes of our report.

This audit was performed at the FCA headquarters in McLean, Virginia, from January through May 2016. At the conclusion of this audit, we provided management with a draft report of our observations and held an exit conference on May 17, 2016.

ACRONYMS

BCP	business continuity plan
EDGE	Enterprise Documentation and Guidance
EIC	Examiner-in-Charge
EWP	Examination Workprogram
FCA or Agency	Farm Credit Administration
FCS or System	Farm Credit System
FFIEC	Federal Financial Institutions Examination Council
IT	information technology
OE	Office of Examination
ROE	Report of Examination

R E P O R T

Fraud | Waste | Abuse | Mismanagement



FARM CREDIT ADMINISTRATION OFFICE OF INSPECTOR GENERAL

Phone: Toll Free (800) 437-7322; (703) 883-4316

Fax: (703) 883-4059

E-mail: fca-ig-hotline@rcn.com

Mail: Farm Credit Administration
Office of Inspector General
1501 Farm Credit Drive
McLean, VA 22102-5090