



Memorandum from the Office of the Inspector General

September 13, 2018

Andrea S. Brackett, WT 5D-K
Diane T. Wear, WT 4B-K

**REQUEST FOR MANAGEMENT DECISION – AUDIT 2017-15451 –
KEY SARBANES-OXLEY FINANCIAL SPREADSHEETS**

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report.

If you have any questions or wish to discuss our findings, please contact Michael R. Newport, Senior Auditor, at (865) 633-7335 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
WT 2C-K

MRN:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MP 3B-C
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Philip D. Propes, MP 2C-C
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
OIG File No. 2017-15451



Office of the Inspector General

Audit Report

To the Director, Cybersecurity,
and to the Vice President and
Controller, Corporate
Accounting

KEY SARBANES-OXLEY FINANCIAL SPREADSHEETS

Audit Team
Michael R. Newport
Melissa L. Conforti

Audit 2017-15451
September 13, 2018

ABBREVIATIONS

IT	Information Technology
ITGC	Information Technology General Control
SOX	Sarbanes-Oxley
SPP	Standard Program and Process
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
BACKGROUND.....	1
OBJECTIVE, SCOPE, AND METHODOLOGY	2
FINDINGS	2
MANAGEMENT OF SHARED PASSWORDS NOT DOCUMENTED	2
SHARED ACCOUNT WITH ACCESS TO CRITICAL SPREADSHEETS.....	3
INEFFECTIVE INVENTORY CONTROLS OVER CRITICAL SPREADSHEETS	3
SOX CONTROL NARRATIVES DID NOT ALWAYS REFERENCE APPLICABLE SPREADSHEETS	4
UNENFORCED NAMING CONVENTION USAGE	4
CRITICAL SPREADSHEET POLICY COULD BE STRENGTHENED	4
RECOMMENDATIONS	5

APPENDICES

- A. OBJECTIVE, SCOPE, AND METHODOLOGY
- B. MEMORANDUM DATED SEPTEMBER 7, 2018, FROM DIANE T. WEAR
AND ANDREA S. BRACKETT TO DAVID P. WHEELER



Audit 2017-15451 – Key Sarbanes-Oxley Financial Spreadsheets

EXECUTIVE SUMMARY

Why the OIG Did This Audit

Information systems, including spreadsheets, are an integral part of the Tennessee Valley Authority's (TVA) financial reporting process. As part of the Sarbanes-Oxley (SOX) compliance initiatives, TVA has classified spreadsheets used in the financial reporting process as critical and TVA's SOX Control Environment group, which is responsible for assessing SOX controls within TVA, has assessed each with a risk ranking of high, moderate, or low based on its purpose, complexity, and potential dollar impact to TVA's financial statements based on TVA policy. TVA has implemented information technology general controls (ITGC)ⁱ to these critical spreadsheets based on their risk ranking. As part of our annual audit plan, we conducted an audit of these critical spreadsheet controls.

Our audit objective was to determine if the controls for key SOX financial spreadsheets were sufficiently defined, appropriately designed, and operating effectively. The scope for this audit was ITGCs for the SOX critical spreadsheets within TVA. Tests of completeness and accuracy of the spreadsheet calculations were not included in the scope of this audit.

What the OIG Found

We identified several issues that could provide a stronger control environment for critical spreadsheets. Specifically, we found:

1. Shared passwords used to modify critical spreadsheets are not appropriately managed.
2. One spreadsheet was accessible using a shared account with no known business need.
3. TVA's SOX Control Environment group's inventory controls over critical spreadsheets are ineffective.
4. Critical spreadsheets are not documented consistently in SOX control narratives maintained by TVA's SOX Control Environment group.
5. Naming convention controls are not being enforced which limits TVA's ability to quickly assess if critical spreadsheets are properly stored for access control and backup purposes.

ⁱ An ITGC is a control other than an application control that relates to the environment within which computer-based application systems are developed, maintained and operated, and that is therefore applicable to all applications.



Audit 2017-15451 – Key Sarbanes-Oxley Financial Spreadsheets

EXECUTIVE SUMMARY

6. TVA's SOX Control Environment group's spreadsheet policy could be strengthened by adding controls for user training, baselining, templates, and testing.

What the OIG Recommends

We recommend the Vice President and Controller, Corporate Accounting, take the following actions:

1. Define a process for managing critical spreadsheet passwords that is consistent with TVA's Standard Program and Process (SPP) 12.003, *IT Account Management*.
2. Coordinate with the Director of Information Technology Planning and Operations to determine (a) the number of critical spreadsheets accessible by shared accounts either directly or via groups and (b) if that access is appropriate.
3. Coordinate with the critical spreadsheet owners to ensure the inventory information is complete, consistently formatted, and properly classified.
4. Revise the SOX control narratives to reference the applicable critical spreadsheet(s).
5. Enforce compliance with the specified naming convention for critical spreadsheets.
6. Add the following controls to the critical spreadsheet policy:
 - a. A training program for critical spreadsheet owners and reviewers.
 - b. Baseline each spreadsheet to develop a basis for understanding future changes.
 - c. Create templates for future critical spreadsheets where possible.
 - d. Add functional testing controls where determined appropriate.



Audit 2017-15451 – Key Sarbanes-Oxley Financial Spreadsheets

EXECUTIVE SUMMARY

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our audit findings and recommendations. In addition, TVA management stated (1) certain aspects of TVA-SPP-12.003 are not technically feasible in the current environment, and (2) management is evaluating other alternatives to help TVA quickly assess if critical spreadsheets are properly stored for access control and backup purposes. TVA management also noted an issue with the title of TVA-SPP-12.003 we referenced, which has been corrected. See Appendix B for TVA management's complete response.

BACKGROUND

Information systems, including spreadsheets, are an integral part of the Tennessee Valley Authority's (TVA) financial reporting process. The spreadsheets are integral because they (1) are used to compile information and perform calculations as the first steps in developing journal entries material to TVA's financial statements and (2) impact internal financial decision making. As part of the Sarbanes-Oxley (SOX) compliance initiatives, spreadsheets used in the financial reporting process have been classified as critical and provided with a risk ranking of high, moderate, or low based on its purpose, complexity, and annual financial impact to TVA's financial statements.

Overall risk of each spreadsheet is determined as a function of both the annual financial impact and the complexity as defined by TVA management. Criteria for financial impacts and complexity are shown in Table 1.

Overall Risk	Annual Financial Impact	Complexity Characteristics
High	>\$50,000,000	<ul style="list-style-type: none"> • Support complex calculations or models • Multiple supporting spreadsheets • Basis for journal entries into the general ledger or financial statement disclosure
Moderate	\$10,000,000-\$50,000,000	<ul style="list-style-type: none"> • Spreadsheets that perform calculations using formulas • Potentially multiple source systems • Translates information for journal entries or financial statement disclosures
Low	<\$10,000,000	<ul style="list-style-type: none"> • Spreadsheets used for electronic logging or information tracking • Single source systems • Simple calculations

Table 1

As shown in Table 2, TVA has implemented seven information technology general controls (ITGC) over the critical spreadsheets based on their risk ranking.

Control	Low Risk	Moderate Risk	High Risk
Access Control	X	X	X
Backups	X	X	X
Documentation	X	X	X
Standard Naming Convention	X	X	X
Independent Review and Approval		X	X
Input Reconciliation		X	X
Logic Inspection		X	X

Table 2

As of December 19, 2017, TVA had identified 260 spreadsheets as critical. The number of spreadsheets and their associated risk ranking are shown in Table 3 on the following page.

Risk Ranking	Number of Spreadsheets	Percentage of Spreadsheets
Low	92	35%
Moderate	104	40%
High	63	24%
None	1	<1%
Total	260	100%

Table 3

As part of our annual audit plan, we conducted an audit of controls over these critical spreadsheets due to their potential financial impact.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if the controls for key SOX financial spreadsheets were sufficiently defined, appropriately designed, and operating effectively. The scope for this audit was ITGCs¹ for the SOX critical spreadsheets within TVA. Tests of completeness and accuracy of the spreadsheet calculations were not included in the scope of this audit. A complete discussion of our objective, scope, and methodology is included in Appendix A.

FINDINGS

We identified several issues that could provide a stronger control environment for critical spreadsheets. Specifically, we found (1) the management of shared passwords was not documented, (2) a shared account with no known business need had access to a critical spreadsheet, (3) ineffective inventory controls over critical spreadsheets, (4) SOX control narratives did not always reference applicable spreadsheets, (5) an unenforced naming convention control, and (6) controls not currently in place which, if implemented, could lower TVA's risk.

MANAGEMENT OF SHARED PASSWORDS NOT DOCUMENTED

Critical spreadsheets are required to have a password set within the application. The password, which is separate from a user's network access account, is used to ensure a user authenticates to a spreadsheet prior to modifying it. We found these passwords are frequently shared among personnel needing to modify the spreadsheets due to a limitation of the application. However, a documented process for managing these passwords has not been developed.

TVA's Standard Program and Process (SPP) 12.003, *IT Account Management*, requires all shared accounts to have a documented process for managing shared accounts and/or passwords. A documented process for users to follow regarding password management reduces the risk of (1) inappropriate access to the critical

¹ An ITGC is a control other than an application control that relates to the environment within which computer-based application systems are developed, maintained and operated, and that is therefore applicable to all applications.

spreadsheets as employees change positions or groups and (2) unavailability of the spreadsheets if passwords are misplaced and the spreadsheets cannot be accessed when needed.

SHARED ACCOUNT WITH ACCESS TO CRITICAL SPREADSHEETS

We performed access control testing on a sample of 18 critical spreadsheets. We determined, through information obtained from TVA's Information Technology (IT) Planning and Operations, 17 of the 18 spreadsheets generally had appropriate network account access controls applied. However, we found a shared account with network access to review a critical spreadsheet with no known business need. Accordingly, the shared account's access appears to be unnecessary. According to TVA's IT Planning and Operations personnel, the account was part of a group with access to the same critical spreadsheet. We did not attempt to determine if the account had accessed the spreadsheet.

INEFFECTIVE INVENTORY CONTROLS OVER CRITICAL SPREADSHEETS

TVA's SOX Control Environment group owns the critical spreadsheet inventory. TVA's critical spreadsheet user groups are responsible for ensuring the SOX Control Environment group is aware of all critical spreadsheets and related information. Effective inventory controls include (1) defining the criteria items needed to be inventoried and (2) creating and maintaining the inventory. We found several inaccuracies that result in an ineffective inventory which increases the risk of expected controls not being applied appropriately or consistently. Specifically, we noted the following:

- Twelve spreadsheets were incorrectly classified based on the recorded financial impact that impacts their overall risk ranking and could lead to unnecessary controls or too few controls being applied. Four spreadsheets were classified too high and eight were classified too low.
- More than 30 percent of the inventory records had missing information that could lead to misclassifying spreadsheets or difficulty appropriately tracking the spreadsheets. Specifically:
 - 82 of 260 were missing SOX process numbers.
 - 84 of 260 were missing SOX process names.
 - 1 of 260 was not ranked for complexity, frequency, financial impact, or overall risk.

- Inconsistent formatting of fields in the Excel document that lists all critical spreadsheets. The inconsistent formatting creates difficulty with properly identifying and classifying spreadsheets. Specifically, we found:
 - Eighty-five spreadsheets were recorded with alphanumeric financial impacts (e.g., dollar ranges or verbiage instead of specific and rounded dollar amounts).
 - Spreadsheet owner and reviewer names recorded using different formats, such as legal names, nicknames, and misspelled names.
 - Twelve spreadsheets showed incomplete server information in file paths including mapped drives instead of specific server locations.

SOX CONTROL NARRATIVES DID NOT ALWAYS REFERENCE APPLICABLE SPREADSHEETS

TVA's Financial Services group has defined financial processes in 47 SOX control narratives. We found all key spreadsheets reference the applicable SOX control narrative. However, we found only 11 of 47 of the SOX control narratives reference the applicable spreadsheet(s). The remaining 36 SOX control narratives did not identify some or all applicable critical spreadsheets.

TVA-SPP-13.251, *SOX Critical Spreadsheets* does not currently require the SOX control narratives to reference the applicable spreadsheet(s). This could result in potential impacts to TVA's financial statements by failing to identify critical spreadsheets and applying controls required by TVA-SPP-13.251.

UNENFORCED NAMING CONVENTION USAGE

TVA-SPP-13.251, *SOX Critical Spreadsheets*, provides guidance for the naming of critical spreadsheets including the spreadsheet number and the accounting period in which it was created/used. We reviewed the file names in the critical spreadsheet inventory as of December 19, 2017, and found 20 of the 260 followed the provided guidance while the remaining 240 did not follow the guidance. The spreadsheets that do not follow the naming convention control impact TVA management's ability to quickly assess if critical spreadsheets are properly stored for access control and backup purposes.

CRITICAL SPREADSHEET POLICY COULD BE STRENGTHENED

TVA-SPP-13.251, *SOX Critical Spreadsheets*, includes ITGCs, such as access control and backups. However, the policy does not include other recommended controls regarding training, baselining, critical spreadsheet templates, and testing requirements. Training controls would reduce risk by educating users on required information, how spreadsheets are used, and when a critical spreadsheet is considered critical. Baseline controls would better ensure expected functionality when modifications are made. Critical spreadsheet template controls help to reduce the risk of inaccuracies. Testing requirements further reduce risk by testing the functionality and providing quality control to

each spreadsheet. Not including these controls increases the risk of inaccurate financial reporting.

RECOMMENDATIONS

We recommend the Vice President and Controller, Corporate Accounting, take the following actions:

1. Define a process for managing critical spreadsheet passwords that is consistent with TVA-SPP-12.003, *IT Account Management*.
2. Coordinate with the Director of IT Planning and Operations to determine (a) the number of critical spreadsheets accessible by shared accounts either directly or via groups and (b) if that access is appropriate.
3. Coordinate with the critical spreadsheet owners to ensure the inventory information is complete, consistently formatted, and properly classified.
4. Revise the SOX control narratives to reference the applicable critical spreadsheet(s).
5. Enforce compliance with the specified naming convention for critical spreadsheets.
6. Consider adding the following controls to the critical spreadsheet policy:
 - a. A training program for critical spreadsheet owners and reviewers.
 - b. Baseline each spreadsheet to develop a basis for understanding future changes.
 - c. Create templates for future critical spreadsheets where possible.
 - d. Add functional testing controls where determined appropriate.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our audit findings and recommendations. In addition, TVA management stated (1) certain aspects of TVA-SPP-12.003 are not technically feasible in the current environment, and (2) management is evaluating other alternatives to help TVA quickly assess if critical spreadsheets are properly stored for access control and backup purposes. TVA management also noted an issue with the title of TVA-SPP-12.003 we referenced, which has been corrected. See Appendix B for TVA management's complete response.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if the controls for key Sarbanes-Oxley (SOX) financial spreadsheets were sufficiently defined, appropriately designed, and operating effectively. The scope for this audit was information technology general controls for the SOX critical spreadsheets within the Tennessee Valley Authority (TVA). Tests of completeness and accuracy of the spreadsheet calculations were not included in the scope of this audit. To achieve our objective we:

- Interviewed TVA personnel within TVA's SOX Control Environment group, TVA's Information Technology, and spreadsheet user groups throughout TVA to obtain an understanding of processes and procedures related to critical spreadsheets.
- Obtained and reviewed TVA Standard Programs and Processes (SPP) as TVA specific criteria including:
 - TVA-SPP-13.251, *SOX Critical Spreadsheets*
 - TVA-SPP-12.003, *IT Account Management*
- Identified and reviewed the following best practices:
 - Deloitte & Touche, LLP, *End User Computing–Solving the Problem*, 2013
 - National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014
- Obtained and reviewed applicable TVA SPPs, against applicable best practices including:
 - TVA-SPP-12.203, *Remote Access*
 - TVA-SPP-12.704, *Security Configuration Benchmark Standards*
 - TVA-SPP-12.017, *Security Awareness and Training*
 - TVA-SPP-12.002, *TVA Information Management Policy*
 - TVA-SPP-12.000, *Information Technology*
 - TVA-SPP-12.013, *Information System Contingency Planning*
 - TVA-SPP-12.005, *Enterprise Cybersecurity Monitoring Program*
 - TVA-SPP-14.430, *Security Clearances*
 - TVA-SPP-12.004, *TVA Cybersecurity Patch and Vulnerability Management Program*
 - TVA-SPP-12.001, *Acceptable Use of Information Resources*
 - TVA-SPP-13.025, *Sarbanes-Oxley Program*
 - TVA-SPP-12.900, *IT Change Management*
 - TVA-SPP-12.100, *NERC Critical Infrastructure Protection – Cyber Security*
- Obtained and analyzed inventories of spreadsheets as of December 19, 2017, to determine completeness.

- Judgmentally selected 18 of 260 spreadsheets for access control testing based on how the spreadsheets were recorded in the critical spreadsheet inventory as compared to the SOX control narratives. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Compared the critical spreadsheet inventory to the SOX control narratives to determine completeness of the inventory.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

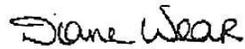
September 7, 2018

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2017-15451 – KEY
SARBANES-OXLEY FINANCIAL SPREADSHEETS

Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Michael Newport, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Vincent Beichler.



Diane Wear
Vice President & Controller
Financial Services
WT 4B-K



Andrea Brackett
Director, TVA Cybersecurity
Financial Services
WT 5D-K

cc (Attachment):

Vincent Beichler, WT 4D-K
James Berrong, MR 3M-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
Jeremy Fisher, MR 6D-C
Dwain Lanier, MR 6D-C

Jill Matthews, ET 4C-K
Kevin Mead, WT 4D-K
Philip Propes, MP 2B-C
John Thomas III, MR 6D-C
OIG File No. 2017-1545

AUDIT 2017-15451
Key Sarbanes-Oxley Financial Spreadsheets
Response to Request for Comments

ATTACHMENT A
Page 1 of 2

Page	Draft Report Section	Comments
5	Recommendations	TVA-SPP-12.003 is titled <i>IT Account Management</i> .

Recommendation		Management Comments
1	Define a process for managing critical spreadsheet passwords that is consistent with TVA-SPP-12.003, <i>IT Account Management</i> .	Management agrees with developing a process that is generally consistent with TVA-SPP-12.003. However, certain aspects of this SPP are not technically feasible in the current environment.
2	Coordinate with the Director of IT Planning and Operations to determine (a) the number of critical spreadsheets accessible by shared accounts either directly or via groups and (b) if that access is appropriate.	Management agrees.
3	Coordinate with the critical spreadsheet owners to ensure the inventory information is complete, consistently formatted, and properly classified.	Management agrees.
4	Revise the SOX control narratives to reference the applicable critical spreadsheet(s).	Management agrees.
5	Enforce compliance with the specified naming convention for critical spreadsheets.	Management agrees that version control is an important element of end user computing controls. However, management is evaluating other alternatives to help TVA quickly assess if critical spreadsheets are properly stored for access control and backup purposes.

AUDIT 2017-15451
Key Sarbanes-Oxley Financial Spreadsheets
Response to Request for Comments

ATTACHMENT A
Page 2 of 2

	Recommendation	Management Comments
6	Consider adding the following controls to the critical spreadsheet policy: a. A training program for critical spreadsheet owners and reviewers. b. Baseline each spreadsheet to develop a basis for understanding future changes. c. Create templates for future critical spreadsheets where possible. d. Add functional testing controls where determined appropriate.	Management agrees.