

CHRISTOPHER HIDALGO

Up and Running with Audit Management Pro



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.

Unauthorized release of this information is prohibited.
Original material is copyright © 2022 Tandem.



2



Christopher Hidalgo

ITIL-F, Audit and Security
Consultant



3

This walkthrough is for...

HERE'S THE PLAN

- Users who have Audit Management Pro but are unsure where to start
- Users who have other Audit Management versions but are considering Pro
- Internal auditors who are curious how CoNetrix auditors use Tandem



4

Agenda

HERE'S THE PLAN

- Audit Pro 101: A Refresher
- FFIEC Resources for Work Programs
- Creating an AIO Work Program
- Audit Pro 201: Bringing it all together
- Tips for Tandem workflow
- Recap



5



Audit Pro 101: A Refresher

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

6

What is Audit Management Pro?

AUDIT PRO 101: A REFRESHER

- A tool to create and organize your internal audit projects and conduct audits of your information security program and controls
- A consistent method of reporting the state of internal controls, their weaknesses, and solutions
- Trend analysis of your audit project cycle
- Provides tools for creating custom audits with the response tools available in Audit Management Standard



7

Definitions

AUDIT PRO 101: A REFRESHER



Work Program

A container of control verifications that will be used to test the effectiveness of your controls.

Control Verification

A control verification is a method used to document testing of a control's effectiveness.

AKA

- Control Statements
- Control Objectives

Control Evidence

Interview questions, testing procedures, physical examination or document review requirements.

8

Quick Start Steps

AUDIT PRO 101: A REFRESHER

1

Introductory
Video

2

Assign User
Access

3

Review
Global
Levels and
Ratings

4

Create Work
Programs

[Support Dashboard](#) > [Knowledge Base](#)



9

Audit Management Pro Knowledge Base

AUDIT PRO 101: A REFRESHER

Support

- Support Dashboard
- Contact Support
- Knowledge Base**
- Videos
- Software Updates
- Resources

- User Agreement
- Privacy Policy
- Due Diligence

Audit Management Pro Knowledge Base

< Back to All Categories

Search

Quick Start Tandem Audit Management Pro
Welcome to Tandem Audit Management Pro! Follow the steps in this article to begin conducting audits.

[Audit Management Pro Access Roles](#)
This article describes the access roles available in the Audit Management Pro product, along with the access role capabilities.

[Audit Management Pro Notifications](#)
This article describes the notifications and emails sent by Audit Management Pro.

[Audit Management Pro Product Integrations](#)
This article details the products that integrate with Audit Management Pro, including Business Continuity Plan, Risk Assessment, and Vendor Management.

[What is Tandem Audit Management Pro?](#)
The Tandem Audit Management Pro product allows financial institutions to create control verifications and organize these testing procedures into work programs.



10



FFIEC Resources for Work Programs

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

11

FFIEC Booklets and Work Programs

FFIEC RESOURCES FOR WORK PROGRAMS



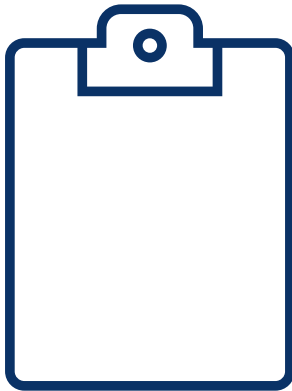
- IT Booklets
 - Provide Action Summaries with specific examination items
 - Appendix A includes full examination procedures
- IT Work Programs
 - Built from the Appendix A sections as a standalone document
 - Might still need to context of the booklet to build a custom work program



12

The Cybersecurity Assessment Tool

FFIEC RESOURCES FOR WORK PROGRAMS



- Domains
 - Coverage spans the FFIEC booklets
 - Already broken up into distinct sections for Work Programs
- Declarative Statements
 - Baseline statements work as a comprehensive evaluation of your information security program
 - Prescriptive list of controls and functions can be repurposed for control evidence and request list items
 - Helpful for providing attestation to your Cybersecurity Maturity answers



13

The Cybersecurity Assessment Tool

FFIEC RESOURCES FOR WORK PROGRAMS

Domain 1: Cyber Risk Management and Oversight	
Work Program	Assessment Factor: Governance
OVERSIGHT	<p>Y, Y(C), N</p> <p>Baseline</p> <p>Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3)</p> <p>Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6)</p> <p>Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5)</p> <p>The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20)</p> <p>Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, page J-12)</p>

Control Verifications



14

Creating an AIO Work Program

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

15

Architecture, Infrastructure, and Operations Booklet

CREATING AN AIO WORK PROGRAM



- IT Booklet Approach
 - Booklet sections provide logical Work Program subject areas
 - Action Summaries are descriptive in what should be examined
 - More work breaking down into a full work program but provides explanations for additional Control Verifications and Control Evidence
- IT Work Program Approach
 - Follows the same booklet sections for subject areas
 - Less work to break down into Work Programs, Control Verifications, and Control Evidence
 - May be too general or “rolls up” too many items into one section

16

AIO Booklet: Action Summaries

CREATING AN AIO WORK PROGRAM

Work Program

FFIEC IT Examination Handbook Architecture, Infrastructure, and Operations

II ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS GOVERNANCE

Control Verification

II.A Board and Senior Management Responsibilities

Action Summary

The board is responsible for overseeing, and senior management is responsible for implementing and maintaining, a safe and sound operating environment that supports the entity's goals and objectives and complies with applicable laws and regulations. Management should establish responsibility and accountability for the administration of the day-to-day functions of the IT environment.

Examiners should review for the following:

Control Evidence

- Board regularly receives reports on AIO functions and activities from management.
- Discussions regarding AIO with the board are captured in meeting minutes.
- Tracking mechanisms and processes are in place to monitor issues related to AIO to their resolution.



17

AIO Booklet: Appendix A

CREATING AN AIO WORK PROGRAM

Work Program

Objective 2: Management promotes and provides effective governance of AIO functions through defined responsibilities, accountability, and adequate resources to support these functions. (II, "Architecture, Infrastructure, and Operations Governance")

Control Verifications

1. Determine whether management implemented a process to continuously manage technology to support operational needs and mitigate AIO-related risks. Determine whether the entity's risk management processes include the following governance mechanisms:

Control Evidence

- a. Delineation of board and senior management responsibilities.
- b. Strategic planning.
- c. ERM.
- d. Delineation of other roles and responsibilities.
- e. Policies, standards, and procedures.
- f. Internal audit, independent reviews, and certifications.
- g. Communications.
- h. Board and senior management reporting.

2. Determine whether oversight includes the following:

- a. Board and senior management consideration of the entity's business objectives, including functions performed by affiliates and third-party service providers.
- b. Management identification and evaluation of AIO-related risks, definition of short- and long-term objectives, and creation of policies and procedures to mitigate those risks.
- c. Management consideration of security and resilience in the design of new products and services.

3. Determine whether board oversight includes the following:



18

AIO Work Program Map: Prototype

CREATING AN AIO WORK PROGRAM

A	B	C	D	E	F	G
Work Program Title	CV Title	CV description	CE name	CE Type	CE description	Request List Items
		The board is responsible for overseeing, and senior management is responsible for implementing and maintaining, a safe and sound operating environment that supports the entity's goals and objectives and complies with applicable laws and regulations. Management should establish responsibility and accountability for the administration of the day-to-day functions of the IT environment.	Board regularly receives reports on AIO functions and activities from	Examination		Report to the Board
			Discussions regarding AIO with the board are captured in meeting minutes	Examination		Board Meeting Minutes
			Tracking mechanisms and processes are in place to monitor issues related to AIO to their resolution.	Examination		Change Management Policies
						Sample of Change Management
AIO Governance	Management has documented and maintained policies, standards, and procedures related to AIO.	Management should document and maintain policies, standards, and procedures related to AIO. Smaller or less complex entities may have one policy and related procedures that encompass AIO, while larger or more complex entities may have multiple policies, standards, and procedures covering various aspects of AIO or various divisions or departments.				
		The board and senior management should engage internal audit or other independent personnel or third parties to review AIO functions and activities and validate effectiveness of controls. Effective AIO auditing assists the board and senior management with oversight, helps verify compliance with applicable laws and regulations, and helps ensure adherence to contractual agreements and entity policies, standards, and procedures to mitigate risks	Independence of AIO-related audits or other reviews.			
			Appropriate scope and detail of AIO-related audits or other reviews.			
			Applicable reporting of the AIO-related audit results to the board.			
			Evaluation of third-party service providers' AIO-related audit or reviewer reports.			
			Qualifications of auditors reviewing AIO functions and activities.			
	The board and senior management engages internal audit or other independent personnel or third parties to review AIO functions and activities and validate effectiveness of controls.					



19

Example Statements

CREATING AN AIO WORK PROGRAM

Interview	Testing	Examination
Can you describe...	Confirm that...	Assess [that, the]...
Describe...	Review a sample of...	Determine [how, that, whether]...
Explain...	Review results of...	Ensure...
How does [personnel, team, organization] do...		Obtain a list of...
What's the [procedure, process, workflow]		Review evidence that...
		Review procedures for...
		Verify that...



20



Audit Pro 201: Bringing it all together

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

21

Work Program Steps

AUDIT PRO 201: BRINGING IT ALL TOGETHER

1

Download Bulk Import Templates

2

Bulk Import Control Evidence and Request List Items

3

Bulk Import and Edit Control Verifications

4

Create Work Programs and assign Control Verifications



22

Control Evidence and Request List Items

AUDIT PRO 201: BRINGING IT ALL TOGETHER

Audit Management

Global

Control Evidence

Audit Management > Global > Control Evidence

Work Program Keywords Tag

Interview Testing Examination

Displaying 1 - 15 of 15

Question
Does the organization verify the remote environment is safe before allowing users to connect from the remote location?
How frequently does management perform audits of IT-related activities?
How often are keypad combinations changed?
Inquire of management as to how notifications are delayed in case of law enforcement requests.
Inquire of management as to whether a process exists for notifying an individual or an individual's next of kin of a breach.
Inquire of management as to whether a process exists for notifying individuals within the required time period.
Inquire of management as to whether a process exists for notifying media outlets for breaches of more than 500 individuals' PHI.
Inquire of management as to whether a process exists to ensure that all required notifications were made or that the impermissible use or disclosure did not constitute a breach.
Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach.
Inquire of management as to whether there have been any breaches of unsecured PHI and verify that the Secretary was notified.
Inquire of management as to whether there have been any breaches of unsecured PHI for a business associate and verify that the covered entity was notified.
Inquire of management to determine if there is a standard template or form letter for breach notification.
Is confidential paperwork left where non-validated parties can access it?
Is there a written agreement with the backup location?
Which vendors have direct connections to the bank's network?

Displaying 1 - 15 of 15

KEYS CONFERENCE

23

Audit Management

Global

Control Evidence

Work Program Keywords Tag

Interview Testing Examination

Displaying 1 - 15 of 15

Question
Does the organization verify the remote environment is safe before allowing users to connect from the remote location?
How frequently does management perform audits of IT-related activities?
How often are keypad combinations changed?
Inquire of management as to how notifications are delayed in case of law enforcement requests.
Inquire of management as to whether a process exists for notifying an individual or an individual's next of kin of a breach.
Inquire of management as to whether a process exists for notifying individuals within the required time period.
Inquire of management as to whether a process exists for notifying media outlets for breaches of more than 500 individuals' PHI.
Inquire of management as to whether a process exists to ensure that all required notifications were made or that the impermissible use or disclosure did not constitute a breach.
Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach.
Inquire of management as to whether there have been any breaches of unsecured PHI and verify that the Secretary was notified.
Inquire of management as to whether there have been any breaches of unsecured PHI for a business associate and verify that the covered entity was notified.
Inquire of management to determine if there is a standard template or form letter for breach notification.

24

Control Verifications

AUDIT PRO 201: BRINGING IT ALL TOGETHER

Audit Management

Global > AIG Governance > + Open

Create Control Verification *Audit Management > Global > Control Verifications*

Title
Management has established responsibility and accountability for the administration of the day-to-day functions of the IT environment.

Description
The board is responsible for overseeing, and senior management is responsible for implementing and maintaining, a safe and sound operating environment that supports the entity's goals and objectives and complies with applicable laws and regulations. Management should establish responsibility and accountability for the administration of the day-to-day functions of the IT environment.

Tags
+ Tag

Explanation
+ Explanation

Type	Evidence
<input checked="" type="checkbox"/> Examination	Board regularly receives reports on AIG functions and activities from management.
<input checked="" type="checkbox"/> Examination	Discussions regarding AIG with the board are captured in meeting minutes.
<input checked="" type="checkbox"/> Examination	Tracking mechanisms and processes are in place to monitor issues related to AIG to their resolution.

Request List Items
+ Request List Items

- Report to the Board
- Change Management Policies and Procedures

Guidance
+ Request List Items

Save & Close Save Cancel



25

Work Programs

AUDIT PRO 201: BRINGING IT ALL TOGETHER

Audit Management

Global > AIG Governance > + Open

Edit Work Program *Audit Management > Global > Work Programs*

Title
AIG Governance

Description

Tags
+ Tag

Guidance Category
- Select One

Category
+ Category + Existing Category

Control Verification	Reference
<input checked="" type="checkbox"/> Management has documented and maintained policies, standards, and procedures related to AIG.	<input type="text"/>
<input checked="" type="checkbox"/> Management has established responsibility and accountability for the administration of the day-to-day functions of the IT environment.	<input type="text"/>
<input checked="" type="checkbox"/> The board and senior management engages internal audit or other independent personnel or third parties to review AIG functions and activities and validate effectiveness of controls.	<input type="text"/>

Attachments
+ Attachments

Select a file or drag a file here to upload

Save & Close Save Cancel



26



Tips for Tandem workflow

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

27

Notifications

TIPS FOR TANDEM WORKFLOW

The screenshot displays the 'Request List Items' page in the Audit Management application. The breadcrumb trail is 'Audit Management > +Open (Auditor Audit) > Request List Items'. The interface includes a sidebar with navigation options like Dashboard, Control Verifications, Findings, and Reports. The main content area shows a table of request items with columns for Title, Contact, Status, Sent Email Request, Work Program, and Last Modified Date.

ID	Title	Contact	Status	Sent Email Request	Work Program	Last Modified Date
<input type="checkbox"/>	Annual Security Testing Plan	Alyssa Pugh	Response Completed		IT GLBA 501(b)	09/08/2021
<input type="checkbox"/>	Backup Location Agreement	Sara Rosewood	Incomplete		IT GLBA 501(b)	02/15/2022
<input type="checkbox"/>	Employee Security Awareness Training Course Content	-Select One-	Incomplete		Telework	
<input type="checkbox"/>	Employee Security Awareness Training Policy	-Select One-	Incomplete		Telework	
<input type="checkbox"/>	Identification of technologies, vendors, and personnel (complete attached form)	-Select One-	Incomplete		IT GLBA 501(b)	
<input type="checkbox"/>	IDS/IPS Email Notification Logs	-Select One-	Incomplete		IT GLBA 501(b)	
<input type="checkbox"/>	Information Security Risk Assessment	-Select One-	Incomplete		IT GLBA 501(b)	
<input type="checkbox"/>	IT Policies	-Select One-	Incomplete		IT GLBA 501(b)	
<input type="checkbox"/>	Malicious Software Protection Policy	-Select One-	Incomplete		Telework	
<input type="checkbox"/>	Remote Access Policy	-Select One-	Incomplete		Telework	
<input type="checkbox"/>	SARs	-Select One-	Incomplete		IT GLBA 501(b)	



28

Filters

TIPS FOR TANDEM WORKFLOW

Control Verifications **Audit Management > +Open (Auditor Audit) > Control Verifications**

Work Program/Category Status Tag Contact Apply

+ Control Verification

Displaying 1 - 13 of 13 < Previous | Next >

Work Program	Category	Title	Contact	Status
<input type="checkbox"/>	IT GLBA 501(b)	A formal process for approving and testing all network connections and changes		Pass
<input type="checkbox"/>	IT GLBA 501(b)	Deploy anti-virus software on all systems commonly affected by malicious software		Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Determine if a comprehensive written agreement is in effect with the recovery location.	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Determine if a formal plan for annual security testing exists (e.g. penetration testing, social engineering, etc)?	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Determine if shared bins are adequately secured and available to all applicable personnel.	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Determine if written agreements have been provided for each vendor.	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Verify that the bank's policies, procedures, and processes include a comprehensive program for identifying customers who open an account after October 1, 2003.	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Data and Physical Security	Determine password parameters (length, numeric/alphanumeric, composition, etc.).	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Development and Acquisitions	Evaluate procedures for acquiring significant new software.	Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Development and Acquisitions	Review general RDC controls (as they apply to all variations of RDC such as branch capture, merchant capture, ATM capture, etc.).	Incomplete
<input type="checkbox"/>	Telework	Anti-malware protection is installed, updated, and active for devices used to remotely connect to the organization network.		Incomplete
<input type="checkbox"/>	Telework	Employee security awareness training includes topics related to remote access.		Incomplete
<input type="checkbox"/>	Telework	Patches are current on devices used to remotely connect to the organization network.		Incomplete

Displaying 1 - 13 of 13 < Previous | Next >



29

Import Changes

TIPS FOR TANDEM WORKFLOW

Control Evidence

Work Program/Category Status Tag Contact Apply

Interview Testing Examination

Completed Last Updated

Questionnaire 0 / 4 N/A Import Changes

Displaying 1 - 4 of 4 < Previous | Next >

Work Program	Category	Question	Contact	Status
<input type="checkbox"/>	IT GLBA 501(b)	How often are keypad combinations changed?		Incomplete
<input type="checkbox"/>	IT GLBA 501(b)	Business Continuity Planning	Is there a written agreement with the backup location?	Incomplete
<input type="checkbox"/>	Telework	Does the organization verify the remote environment is safe before allowing users to connect from the remote location?		Incomplete
<input type="checkbox"/>	Telework	Does the organization verify the remote environment is safe before allowing users to connect from the remote location?		Incomplete



30

Findings and Previous Findings

TIPS FOR TANDEM WORKFLOW

Audit Management > +Open (Auditor Audit) > Control Verifications

Edit Control Verification

Title
+ Tag

Description
Determine if a formal plan for annual security testing exists (e.g., penetration testing, social engineering, etc)?
If a plan exists, evaluate its sufficiency.

Guidance
+ Guidance

Contact
- Select One -

Request List Items

Title	Contact	Status
Annual Security Testing Plan	Alyssa Pugh	Response Completed

Response

Attachments
+ Select a file or drop a file here to upload

Buttons: Save, Save & Close, Cancel, Delete



31

Finding and Response Summary

TIPS FOR TANDEM WORKFLOW

Audit Management > +Open (Auditee Audit) > Findings

Findings

Buttons: Status, Primary Contact, Tag, Apply

Buttons: + Finding, Bulk Import, Notify Primary Contacts

Displaying 1 - 14 of 14

Reference	Finding	Risk	Cost	Target Date	Completed Date
104-Apr21	The Windows security audit policy is not configured to log all key events on critical servers.	High	Low	03/24/2022	
112-Apr21	Printer management interfaces are not password protected.	High	Low		
101-Apr21	Critical security patches have not been installed on most bank systems.	High	Medium		
103-Apr21	Anti-malware definitions do not appear to be current on all systems.	Medium	Low		
110-Apr21	The bank's Information Security Risk Assessment needs to be expanded.	Medium	Low		
114-Apr21	Domain passwords appear to be stored in the weaker (LM) password hashes.	Medium	Low		
106-Apr21	The use of removable media is not restricted on bank computers.	Medium	Medium		
108-Apr21	A formal Business Impact Analysis (BIA) is not conducted as part of the bank's Information Systems Disaster Planning Policy.	Medium	Medium		
109-Apr21	Vulnerable software was discovered on the bank's network.	Medium	Medium		
105-Apr21	No backup domain controller is in place.	Medium	High		
111-Apr21	Unlicensed software appears to be installed on one bank system.	Low	Low		
113-Apr21	Unnecessary protocols may be traversing the bank's network.	Low	Low		
102-Apr21	Router and firewall configurations could be strengthened to improve security.	Low	Medium		
107-Apr21	Individual users appear to be running as local administrators.	Low	Medium		

Displaying 1 - 14 of 14



32

Finding and Response Summary

TIPS FOR TANDEM WORKFLOW

2 Finding and Response Summary Matrix

Risk	Reference	Finding	Target	Response	Completed	Verified	Residual Risk	Approved
High	104-Apr21	The Windows security audit policy is not configured to log all key events on critical servers.	03/24/2022	No			○ TBD	
High	112-Apr21	Printer management interfaces are not password protected.		No			○ TBD	
High	101-Apr21	Critical security patches have not been installed on most bank systems.		No			○ TBD	
Medium	103-Apr21	Anti-malware definitions do not appear to be current on all systems.		No			○ TBD	
Medium	110-Apr21	The bank's Information Security Risk Assessment needs to be expanded.		No			○ TBD	
Medium	114-Apr21	Domain passwords appear to be stored in the weaker (LM) password hashes.		No			○ TBD	
Medium	106-Apr21	The use of removable media is not restricted on bank computers.		No			○ TBD	



33

Recap

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

- Audit Pro 101: A Refresher
- FFIEC Resources for Work Programs
- Creating an AIO Work Program
- Audit Pro 201: Bringing it all together
- Tips for Tandem workflow



34



35

A dark blue background with a light blue circle containing a white clipboard icon. The KEYS CONFERENCE logo is in the top right. Text reads: DON'T FORGET! Fill out the survey to get your sticker!

36



KEYS
CONFERENCE

THANKS FOR JOINING!

Up and Running with Audit Management Pro

Christopher Hidalgo
ITIL-F, Audit and Security Consultant

37

Upcoming Sessions

TANDEM

Creating an Effective Incident Response Plan

Lindsey McReynolds, Tandem

RISK & COMPLIANCE

CoNetrix Security Auditors: A Panel Discussion

Mark Faske, Bret Mills, Mark Riff, & Ty Purcell, CoNetrix Security

CYBERSECURITY

Understanding the Value of Your SIEM and SOC

Mike Richline, CoNetrix Technology



38