CHRISTOPHER HIDALGO

Up and Running with Audit Management Pro

KEYS CONFERENCE

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.

KEYS CONFERENCE

2

Christopher Hidalgo

ITIL-F, Audit and Security Consultant

KEYS CONFERENCE

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

KEYS CONFERENCE

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

KEYS CONFERENCE

5

KEYS CONFERENCE

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

KEYS CONFERENCE

7

Definitions

KEYS CONFERENCE

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	2	3	4
Introductory Video	Assign User Access	Review Global Levels and Ratings	Create Work Programs

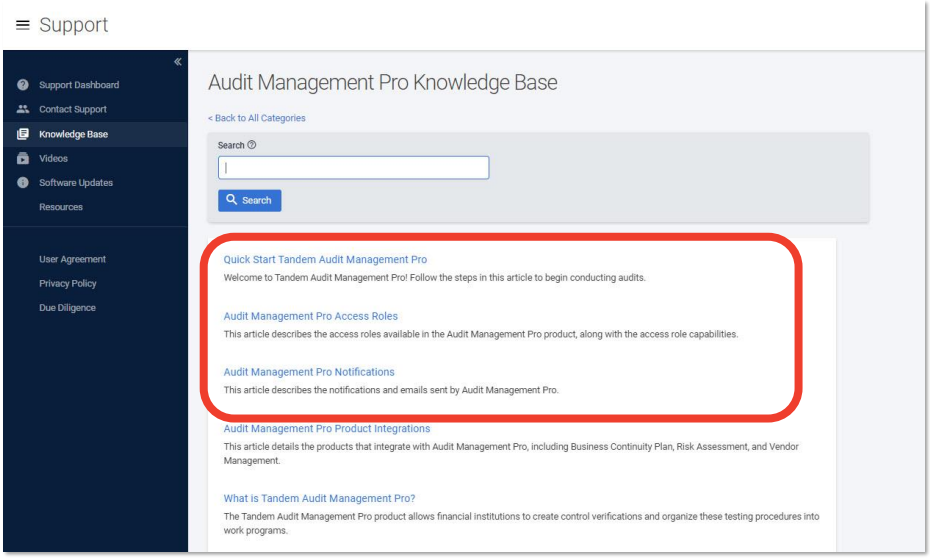
Support Dashboard > Knowledge Base

KEYS CONFERENCE

9

Audit Management Pro Knowledge Base

AUDIT PRO 101: A REFRESHER



KEYS CONFERENCE

10

KEYS CONFERENCE

FFIEC Resources for Work Programs

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

11

FFIEC Booklets and Work Programs

FFIEC RESOURCES FOR WORK PROGRAMS

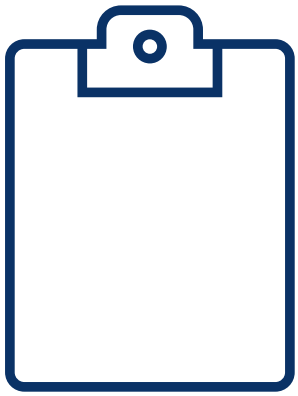
- IT Booklets
  - Provide Action Summaries with specific examination items
  - Appendix A includes full examination procedures
- IT Work Programs
  - Built from the Appendix A sections as a standalone document
  - Might still need to context of the booklet to build a custom work program

KEYS CONFERENCE

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

KEYS CONFERENCE

13

The Cybersecurity Assessment Tool

FFIEC RESOURCES FOR WORK PROGRAMS

Domain 1: Cyber Risk Management and Oversight

Work Program

Assessment Factor: Governance

OVERSIGHT

	Y, Y(C), N	
	Baseline	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)*
		Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 6)*
		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)*
		The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)*
		Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *(FFIEC Business Continuity Planning Booklet, page J-12)*

Control Verifications

KEYS CONFERENCE

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.

Control Evidence

Examiners should review for the following:

- 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.

KEYS CONFERENCE

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.

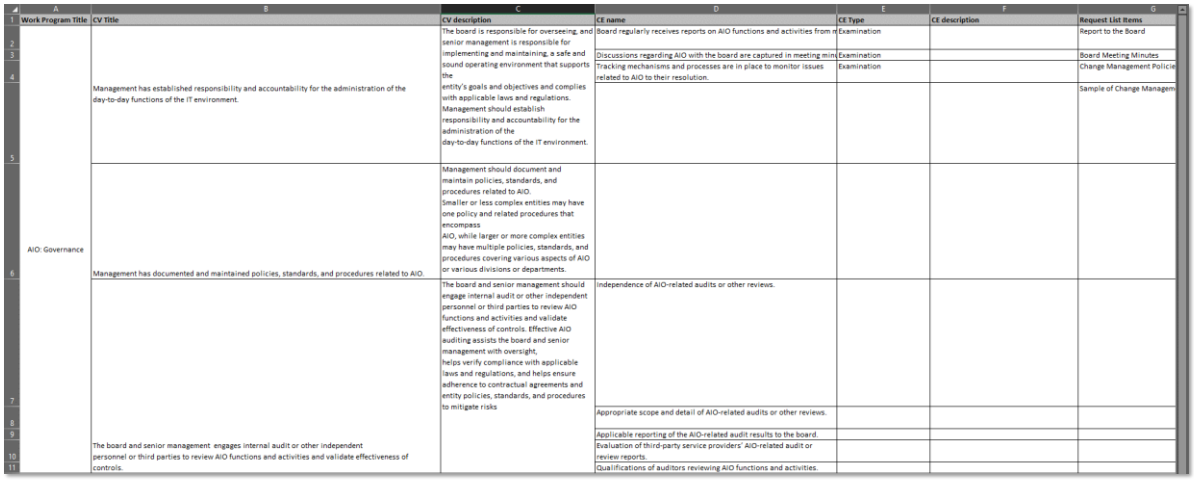
3. Determine whether board oversight includes the following:

KEYS CONFERENCE

18

AIO Work Program Map: Prototype

CREATING AN AIO WORK PROGRAM



	A	B	C	D	E	F	G
1	Work Program Title	CV Title	CV description	CE name	CE Type	CE description	Request List Items
2	AIO: Governance	Management has established responsibility and accountability for the administration of the day-to-day functions of the IT environment.	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 m	Examination		Report to the Board
3				Discussions regarding AIO with the board are captured in meeting min	Examination		Board Meeting Minutes
4				Tracking mechanisms and processes are in place to monitor issues related to AIO to their resolution.	Examination		Change Management Policie
5							Sample of Change Managem
6		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.				
7		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.	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.			
8				Appropriate scope and detail of AIO-related audits or other reviews.			
9				Applicable reporting of the AIO-related audit results to the board.			
10				Evaluation of third-party service providers' AIO-related audit or review reports.			
11				Qualifications of auditors reviewing AIO functions and activities.			

KEYS CONFERENCE

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…

KEYS CONFERENCE

20

KEYS CONFERENCE

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

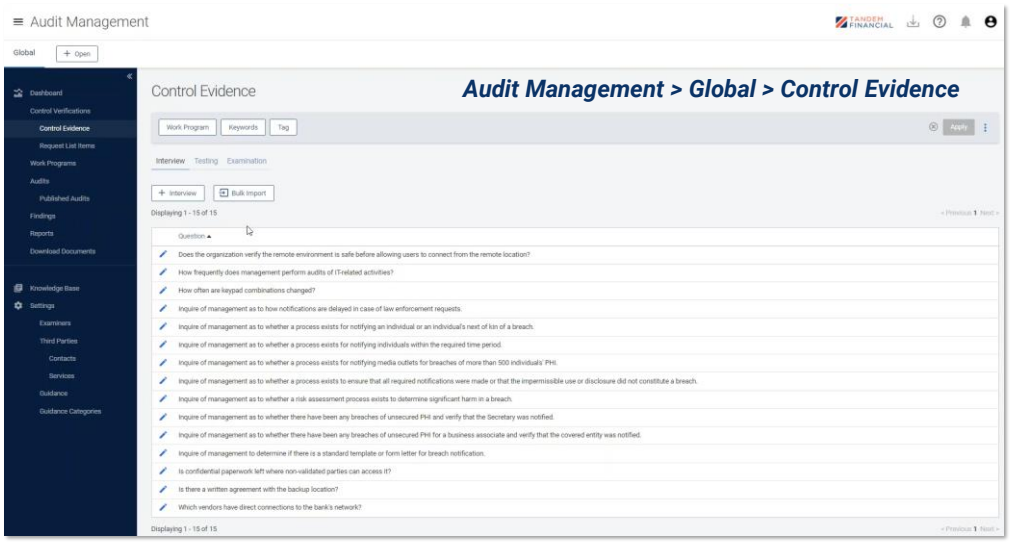
1	2	3	4
Download Bulk Import Templates	Bulk Import Control Evidence and Request List Items	Bulk Import and Edit Control Verifications	Create Work Programs and assign Control Verifications

KEYS CONFERENCE

22

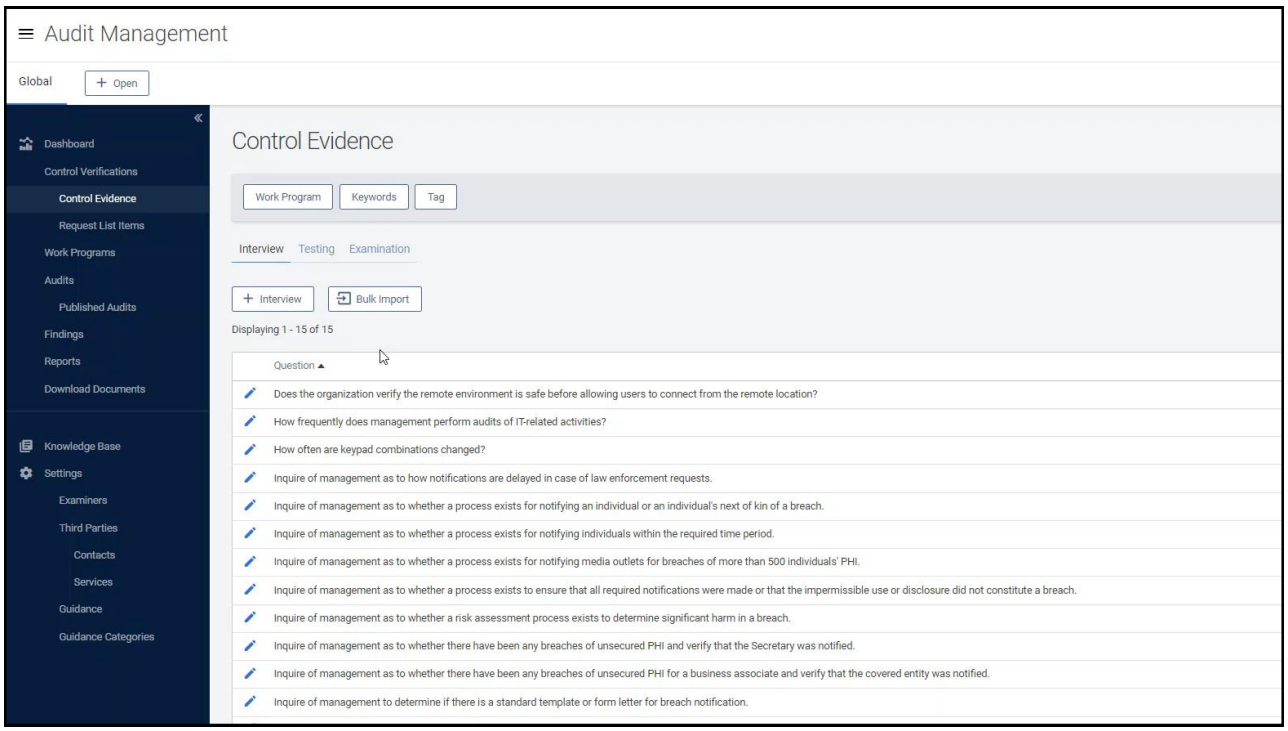
Control Evidence and Request List Items

AUDIT PRO 201: BRINGING IT ALL TOGETHER



KEYS CONFERENCE

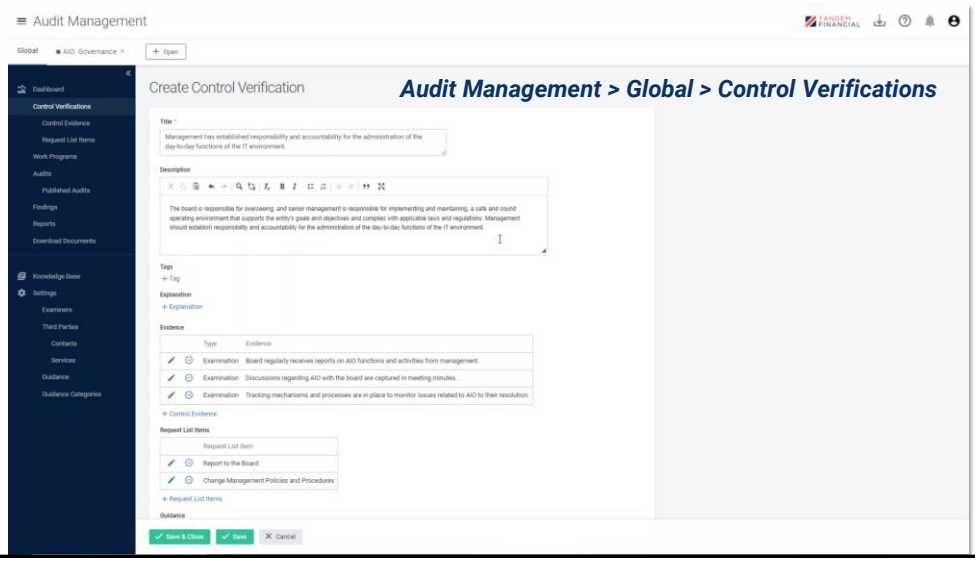
23



24

Control Verifications

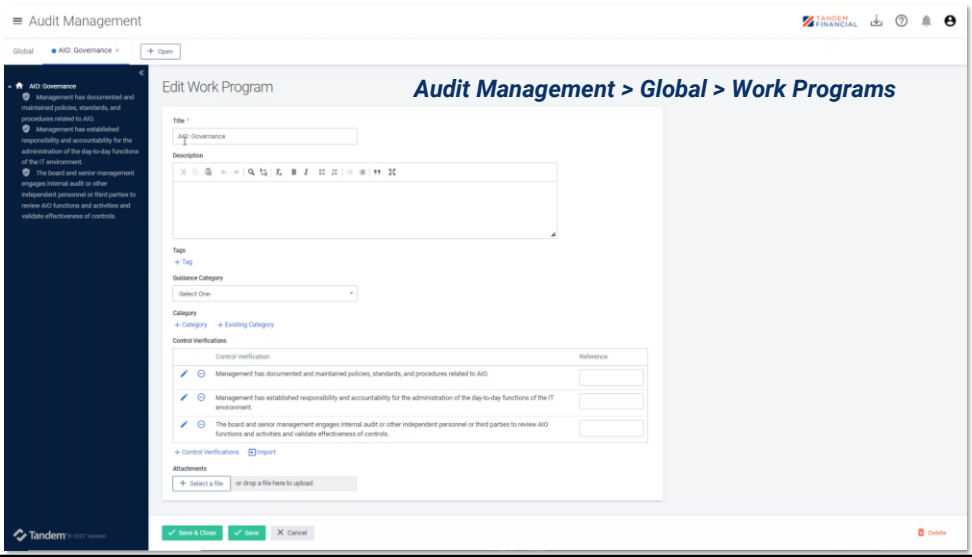
AUDIT PRO 201: BRINGING IT ALL TOGETHER



25

Work Programs

AUDIT PRO 201: BRINGING IT ALL TOGETHER



26

KEYS CONFERENCE

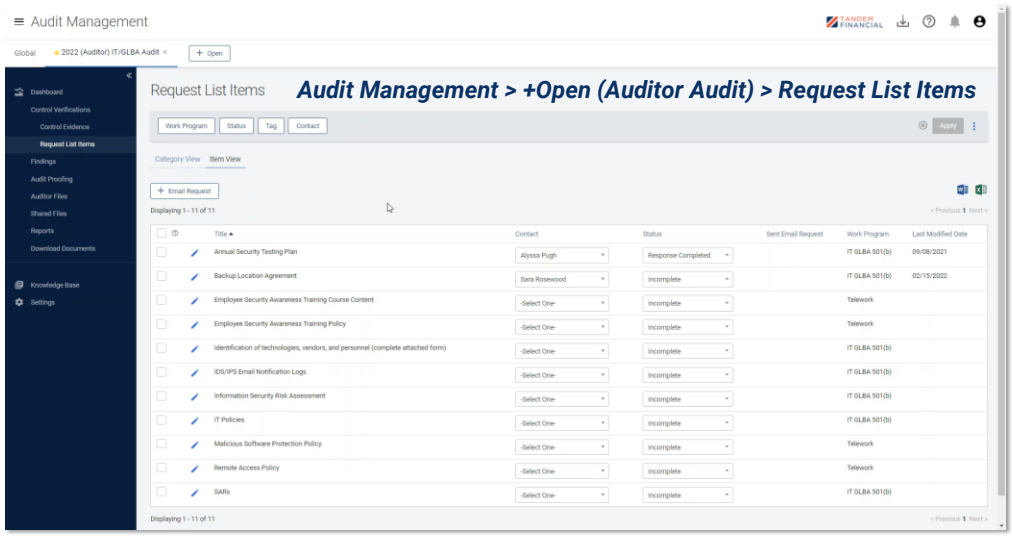
Tips for Tandem workflow

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

27

Notifications

TIPS FOR TANDEM WORKFLOW

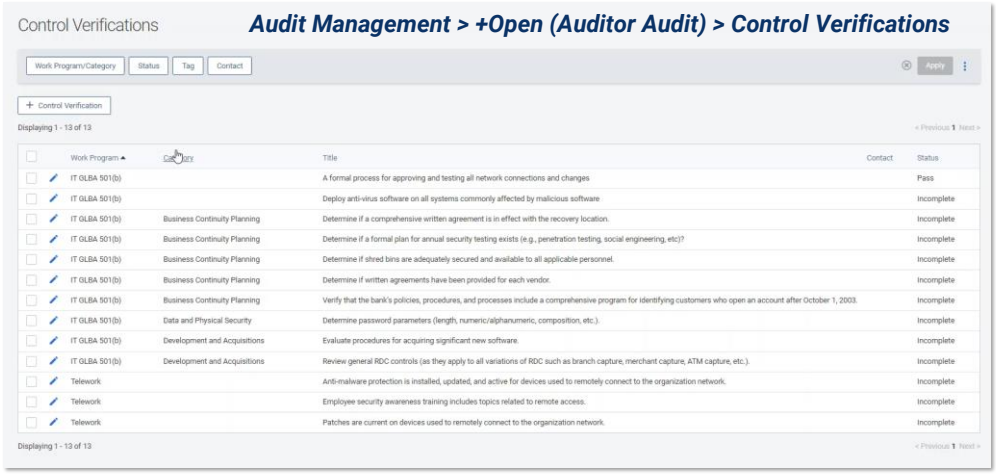


KEYS CONFERENCE

28

Filters

TIPS FOR TANDEM WORKFLOW

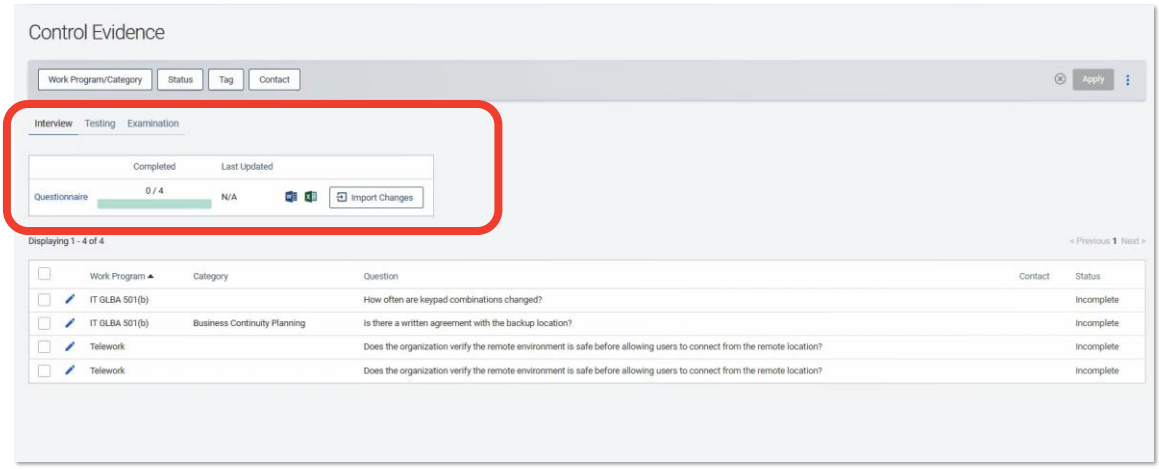


KEYS CONFERENCE

29

Import Changes

TIPS FOR TANDEM WORKFLOW

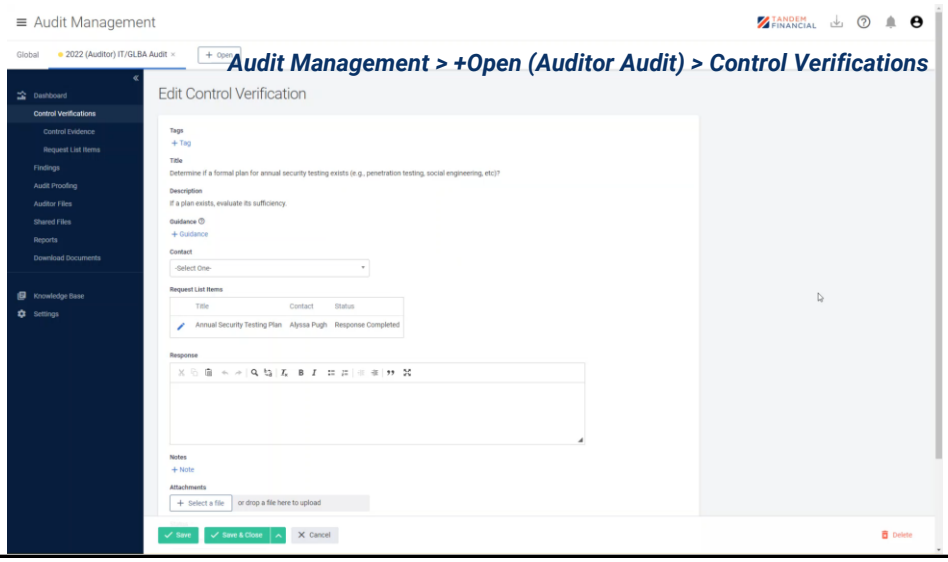


KEYS CONFERENCE

30

Findings and Previous Findings

TIPS FOR TANDEM WORKFLOW

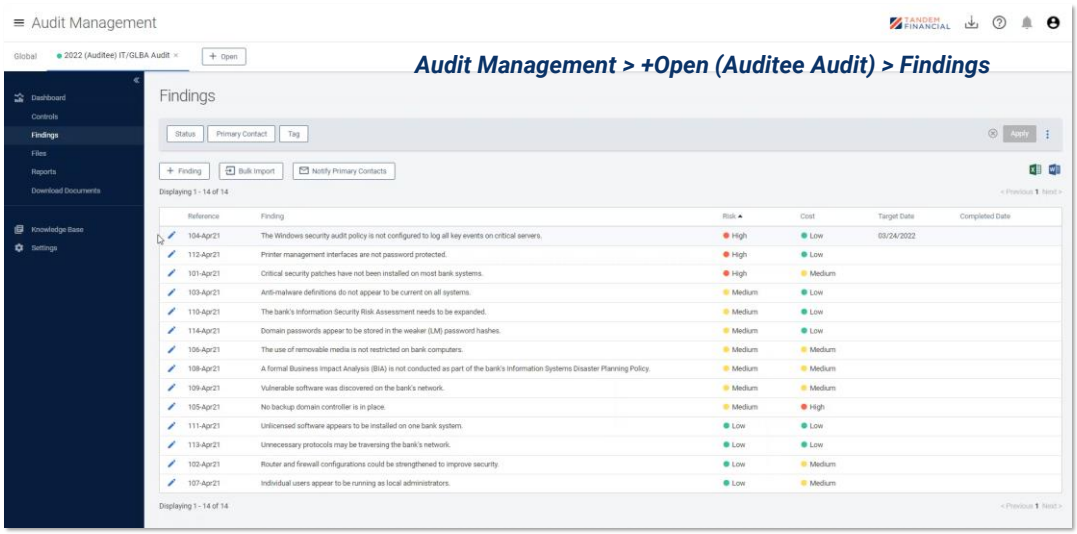


KEYS CONFERENCE

31

Finding and Response Summary

TIPS FOR TANDEM WORKFLOW



KEYS CONFERENCE

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	

KEYS CONFERENCE

33

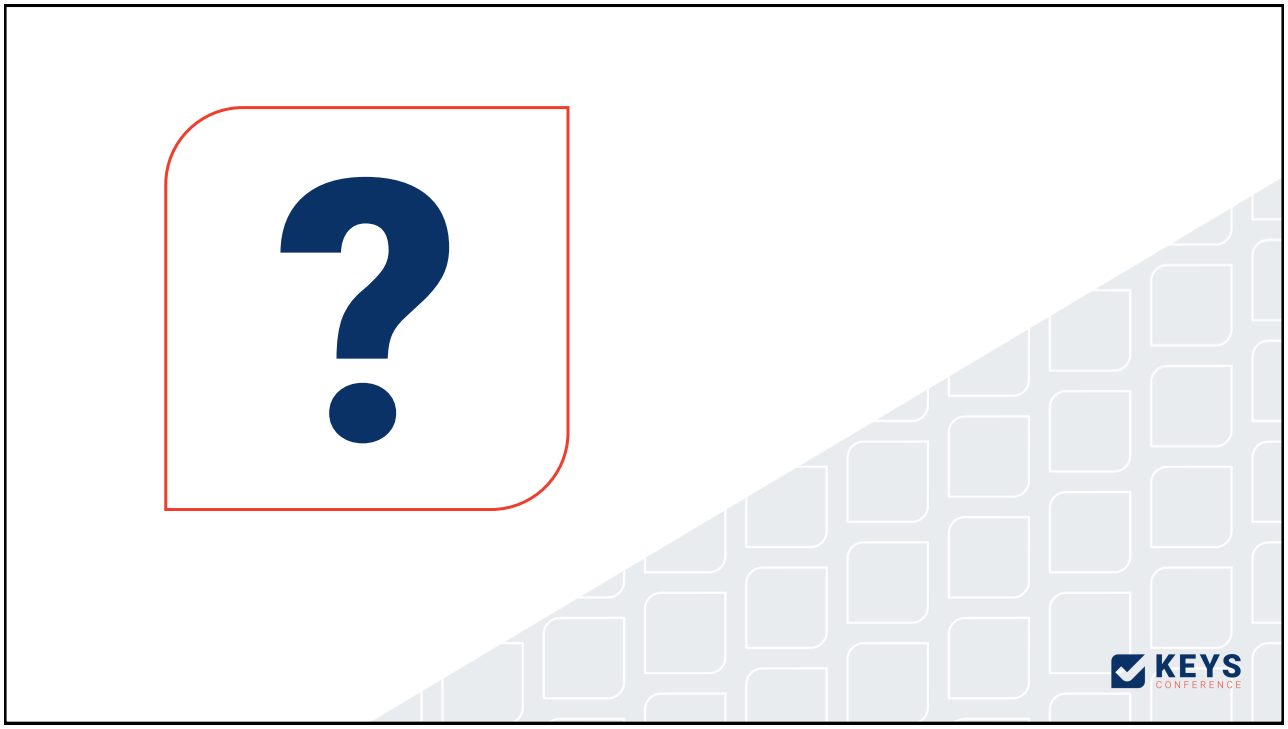
Recap

UP AND RUNNING WITH AUDIT MANAGEMENT PRO

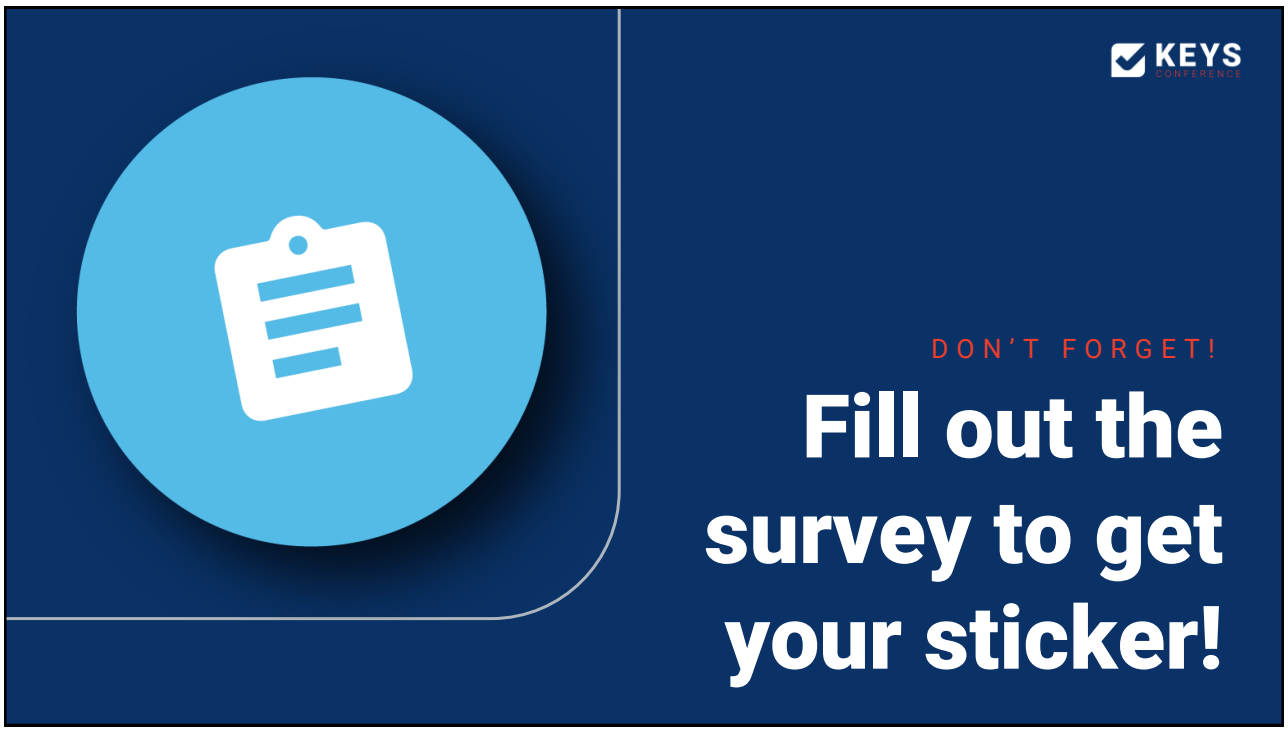
- Audit Pro 101: A Refresher
- FFIEC Resources for Work Programs
- Creating an AIO Work Program
- Audit Pro 201: Bringing it all together
- Tips for Tandem workflow

KEYS CONFERENCE

34


KEYS
CONFERENCE

35


KEYS
CONFERENCE
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

KEYS CONFERENCE

38