

RISK & COMPLIANCE

Robert Wells & Samantha Torrez-Hidalgo

What to Expect When You're Expecting (An Auditor)



1



Robert Wells

Audit and Security Consultant, CoNetrix
Security+, SSCP



Samantha Torrez-Hidalgo

Software Specialist, Tandem
CXSF



4

Agenda

Here's the Plan

- The Elephant in the Room
- What to Expect
- How to Prepare
- What to Gather (from Tandem)
- Bringing it all Together



6

Can an auditor be helpful?



7




The Elephant in the Room

What to Expect When You're Expecting (An Auditor)


8

The Elephant in the Room


Audits Are Stressful!




Who Has Time?!?



Compliance: Regulation & Guidance



Job Performance



9

Define Yourself

The purpose of the audit is to assess the effectiveness of your Information Security Controls.



10

Audits are an opportunity to...

Reframe Your Approach

1

Identify Vulnerabilities

2

Identify Areas Requiring Additional Resources

3

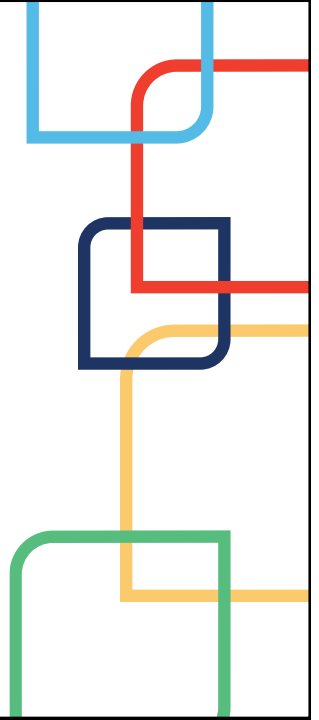
Use Your Auditors Knowledge & Expertise



11

What to Expect (from the Auditor)

What to Expect When You're Expecting (An Auditor)

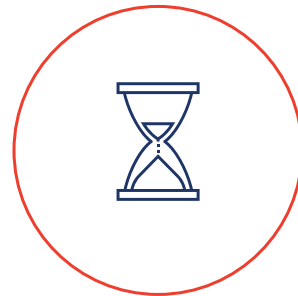


12

What to Expect from the Auditor



Request List Items



Your Time
& Focus



13

ISO Scheduler Resource

<https://tandem.app/schedule>

The collage features several key documents:

- ISO Annual Schedule Instructions:** A document explaining how to use the scheduler, including sections on components to schedule (Risk Assessments, Policies, Business Continuity Plan, Incident Response, Assurance & Training, Report to the Board, Security Awareness Training) and a table for reviewing and updating documentation.
- ISO Annual Schedule Instructions (continued):** Documents detailing steps for identifying frequency and time needed, identifying goals, and providing tips for building a successful ISO program.
- ISO Annual Schedule Calendar:** A monthly calendar from January to December, listing specific activities for each month. For example, January includes Security Awareness Training, and February includes Business Continuity Plan. The calendar also lists monthly activities and quarterly goals.
- 4 Tips To Building a Successful ISO:** A document with sections on 'Expect the unexpected', 'Use your tools', and 'Take your information security program to the next level'.

Preparing for Your Auditor

What to Expect (from the Auditor)



Know the Scope of the Audit



Organize and Delegate



Get the Ball Rolling!



What to Gather (from Tandem)

What to Expect When You're Expecting (An Auditor)



16

Using Tandem's Resources

What to Gather (from Tandem)

1

Knowledge Base

Previous Deliverables

2

3

Finding & Response Summary

Work Papers & Attachments

4

5

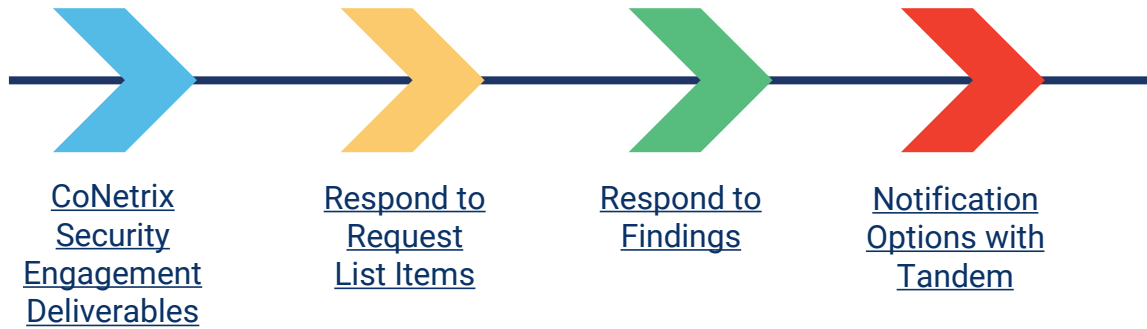
Access Roles



17

Knowledge Base

What to Gather (from Tandem)



18

Access Previous Deliverables

What to Gather (from Tandem)



Penetration Test Report



IT Audit and Vulnerability Assessment Report



Other Documentation



19

Why These Deliverables?

What to Gather (from Tandem)

1

Formally
Address
Vulnerabilities

2

Necessary
for Examiner
Visits

3

Helpful
for Future
Audits



20

Finding and Response Summary

What to Gather (from Tandem)



Problem



Recommendation



Response

21

Finding and Response Summary

What to Gather (from Tandem)

Audit Management

Global 2024 (Auditee) IT/GLBA Audit × + Open

Dashboard
Controls
Findings
Files
Reports
Download Documents

Download Documents

Finding and Response Summary

Excel includes multiple sheets.

- Include Attachments ⓘ
- Include Finding Notes

22

The Importance of Access Roles

What to Gather (from Tandem)

- Security
- Assistance
- Options

23

Which Access Roles to Use

What to Gather (from Tandem)



Admin
(Global
& Individual)



Auditor
(Global
& Individual)



Request List Edit
All
(Global
& Individual)



Findings Edit All
(Global &
Individual)



Findings
View All
(Individual)



24

Delegating to Other Tandem Product Admins



BCP
Admin



Policies
Admin



Risk Assessment
Admin



Vendor
Management
Admin



25

Who are My Product Admins?

What to Gather (from Tandem)

User Access Details

← All Reports

Report Presets: Employees With Notification Emails Disabled | Employees Without Multi-Factor Authentication Enabled

	First Name	Last Name	Access Roles
	Adam	Stevens	Tasks User, Training User, Audit Management Findings Edit All (Individual), Audit Management Finding User, Audit Management Request List Items Access, Business Continuity Plan Edit Responsible, Cybersecurity Edit Responsible, Incident Management Incident Tracking Reporter, Vendor Management Admin
	David	Staggs	Tasks User, Training User, Audit Management Finding User, Audit Management Request List Items Access, Business Continuity Plan Edit Responsible, Cybersecurity Edit Responsible, Incident Management Incident Tracking Reporter, Internet Banking Security Admin, Policies Admin, Risk Assessment Admin, Vendor Management Admin
	Justin	Thompson	Tasks User, Training User, Audit Management Findings Edit All (Individual), Audit Management Finding User, Audit Management Request List Items Access, Business Continuity Plan Edit Responsible, Compliance Management Admin, Cybersecurity Edit Responsible, Policies Admin, Vendor Management Admin
	Lily	Malone	Employee Manager Admin, File Manager Admin, Tasks User, Training User, Business Continuity Plan Edit Responsible, Compliance Management Admin, Cybersecurity Admin, Policies Admin, Vendor Management Admin

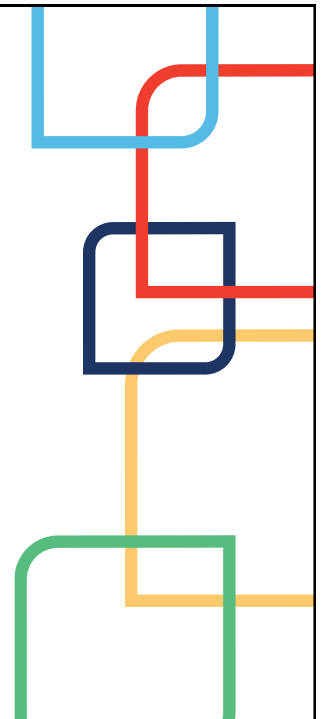
Navigate to:
Admin >
Reports >
User Access
Details



26

Bringing It All Together

What to Expect When You're Expecting (An Auditor)



27

Bringing it Back

What To Expect When You're Expecting (An Auditor)

**Know
Your
Scope**

**Organize
&
Delegate**

**Tandem
Has
Your
Back!**

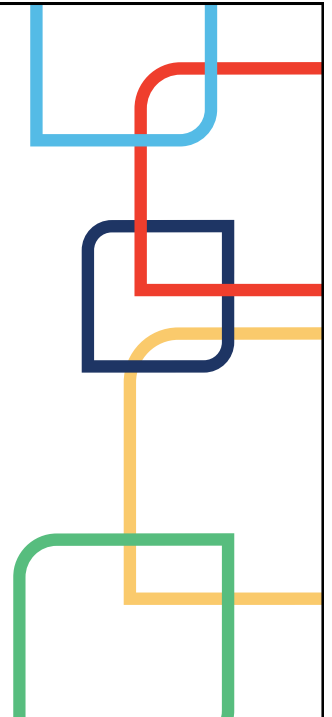
**IT
Audits
Are All
About
Controls**

**Get the
Ball
Rolling**



28

Questions?



29

THANKS FOR JOINING!

What to Expect When You're Expecting (An Auditor)

Robert Wells

Security +, SSCP,
Audit Consultant

CoNetrix Security

Samantha
Torrez-Hidalgo

CXSF, Software Specialist
Tandem

storrez@tandem.app
linkedin.com/in/samanthatorrez

