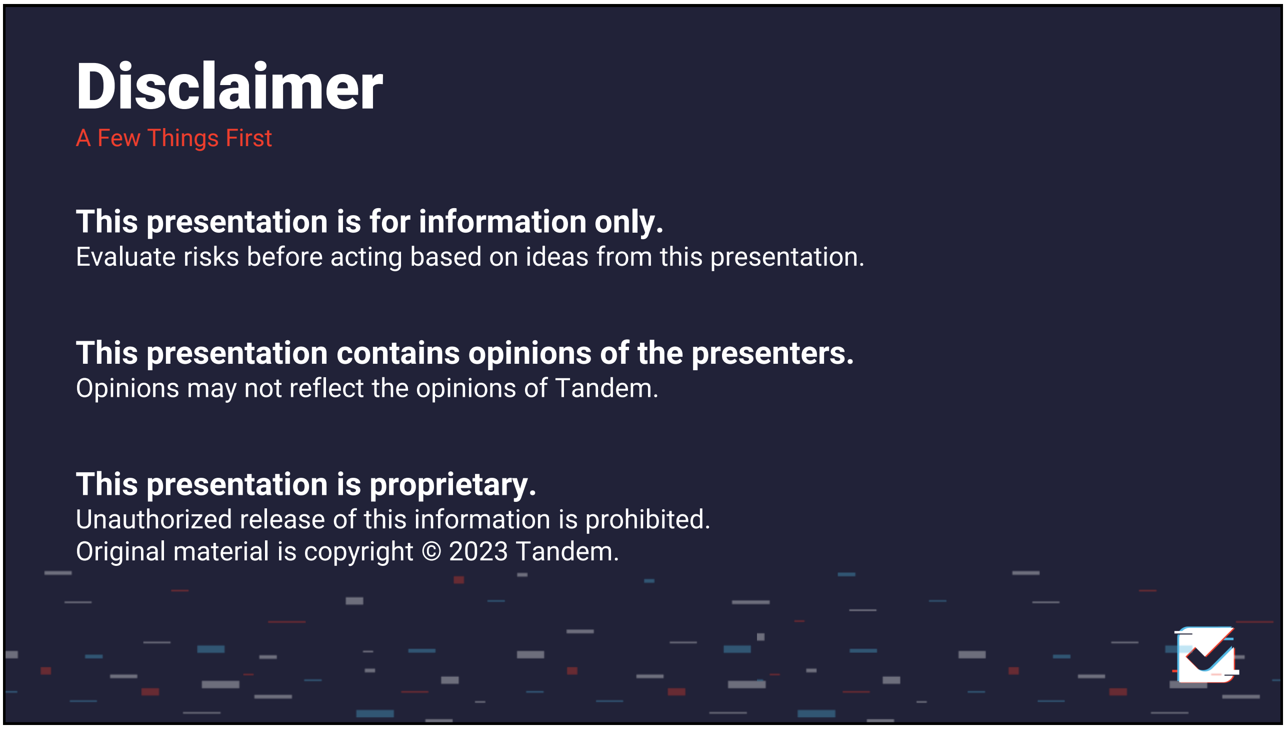
LEVEL UP

Andrew Hettick

What I Learned in My First Year as an ISO

Cybersecurity

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 © 2023 Tandem.

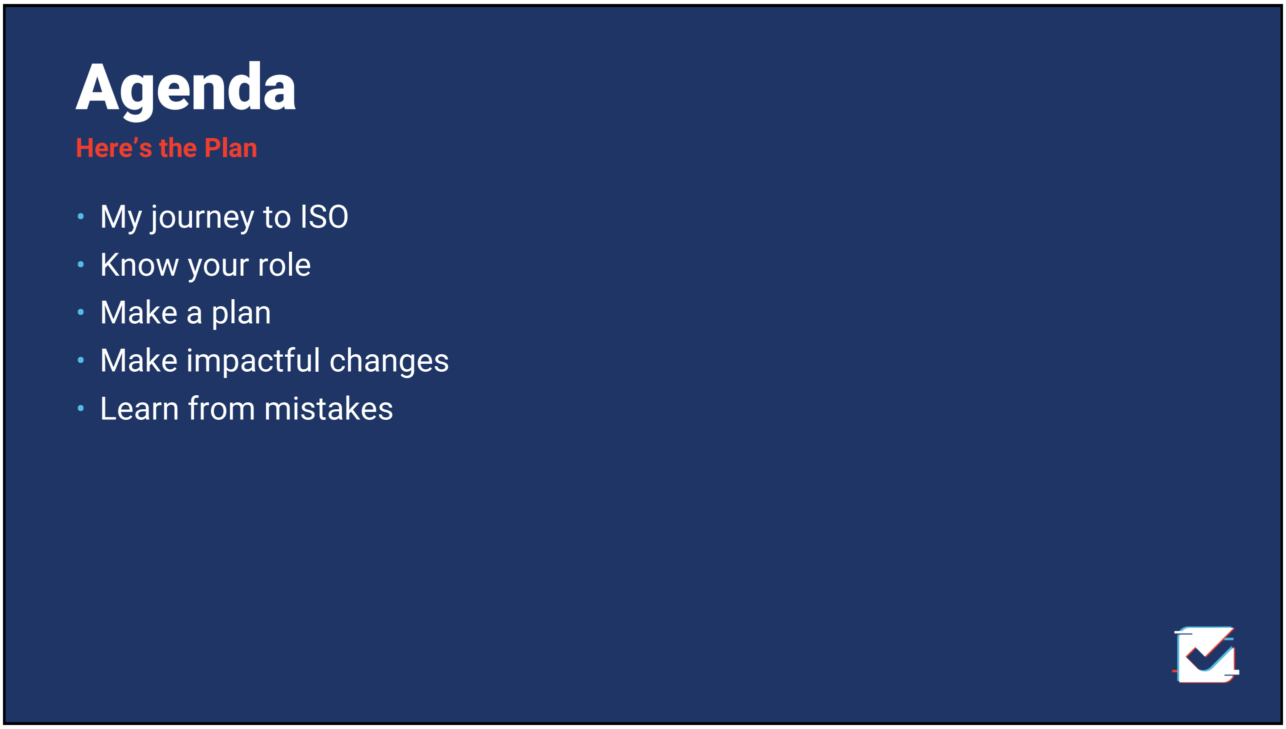
2

Andrew Hettick

CISA, CISSP, SSCP

Information Security Officer

3

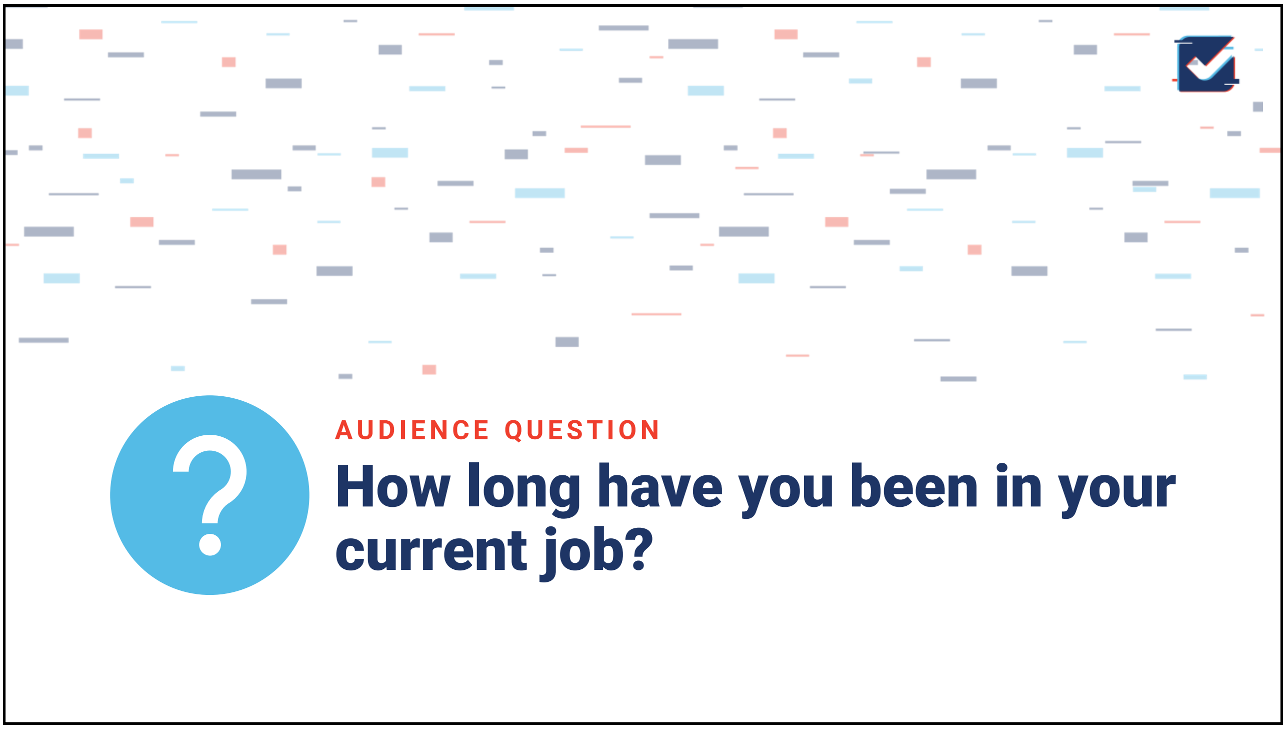


Agenda

Here's the Plan

- My journey to ISO
- Know your role
- Make a plan
- Make impactful changes
- Learn from mistakes

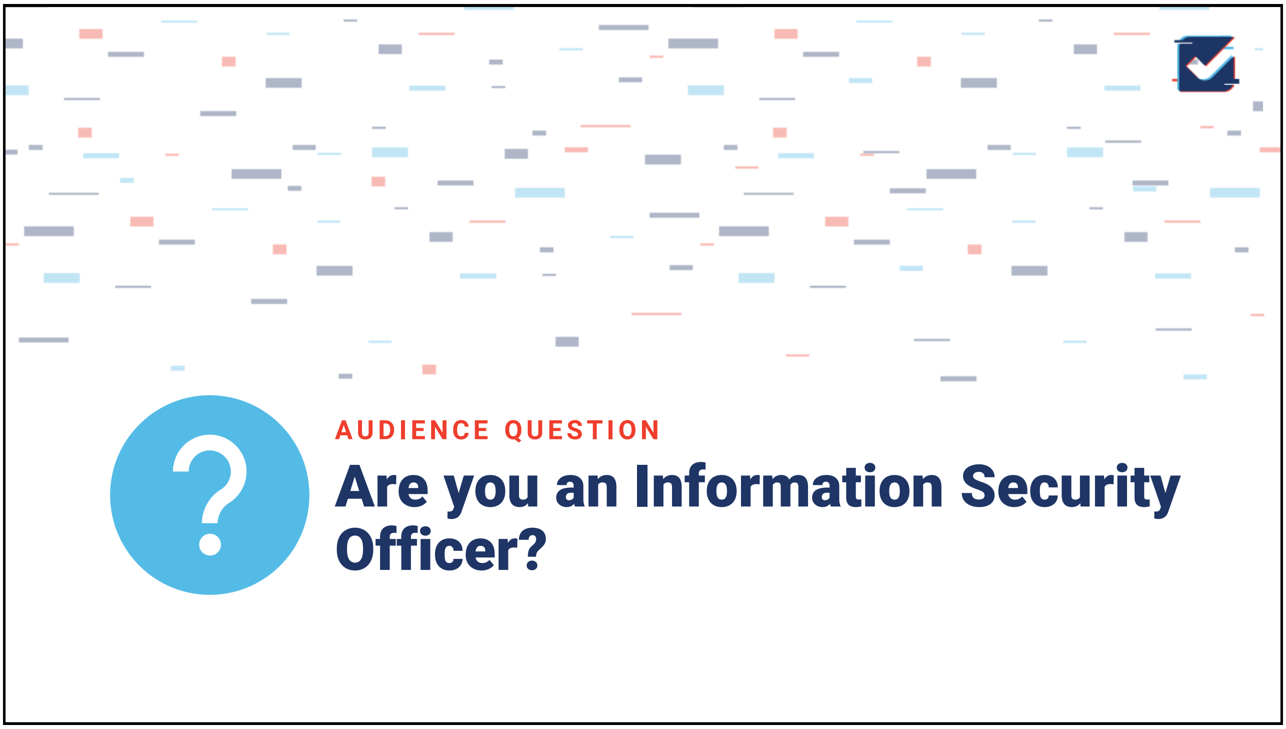
4



AUDIENCE QUESTION

How long have you been in your current job?

5



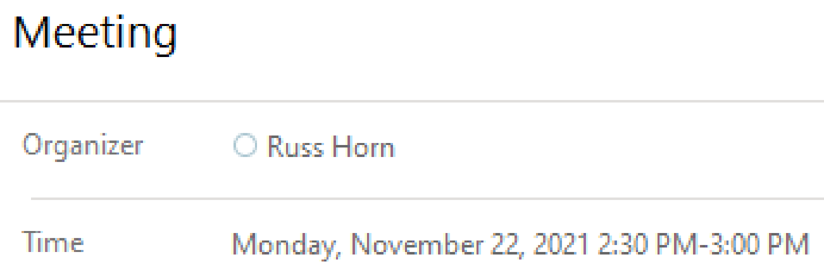
AUDIENCE QUESTION

Are you an Information Security Officer?

6

My Journey to ISO

- Started as an IT Auditor for CoNetrix Security
- Russ sets up a meeting with me



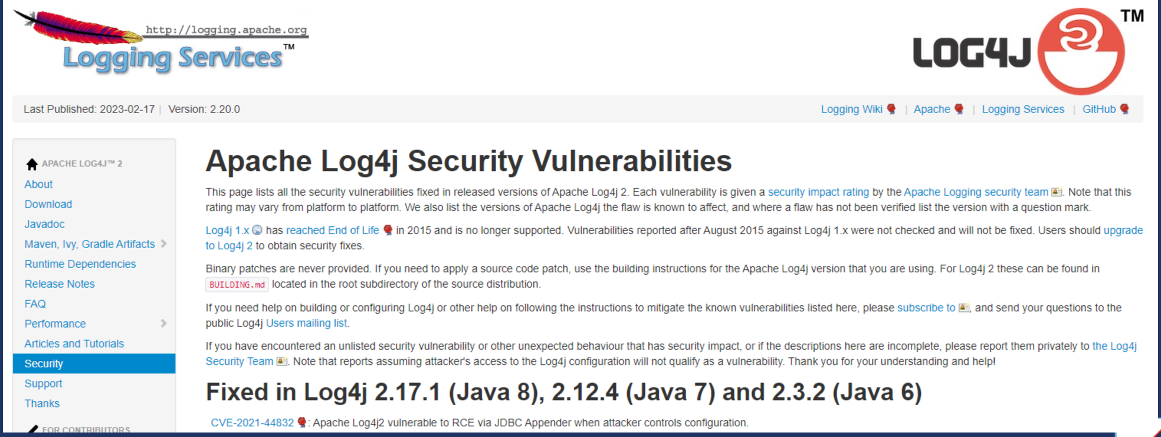
Meeting

Organizer	○ Russ Horn
Time	Monday, November 22, 2021 2:30 PM-3:00 PM

8

My (Unofficial) First Day as an ISO

Apache Log4j Vulnerability



Last Published: 2023-02-17 | Version: 2.20.0

Apache Log4j Security Vulnerabilities

This page lists all the security vulnerabilities fixed in released versions of Apache Log4j 2. Each vulnerability is given a security impact rating by the Apache Logging security team. Note that this rating may vary from platform to platform. We also list the versions of Apache Log4j the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Log4j 1.x has reached End of Life in 2015 and is no longer supported. Vulnerabilities reported after August 2015 against Log4j 1.x were not checked and will not be fixed. Users should upgrade to Log4j 2 to obtain security fixes.

Binary patches are never provided. If you need to apply a source code patch, use the building instructions for the Apache Log4j version that you are using. For Log4j 2 these can be found in `BUILDING.md` located in the root subdirectory of the source distribution.

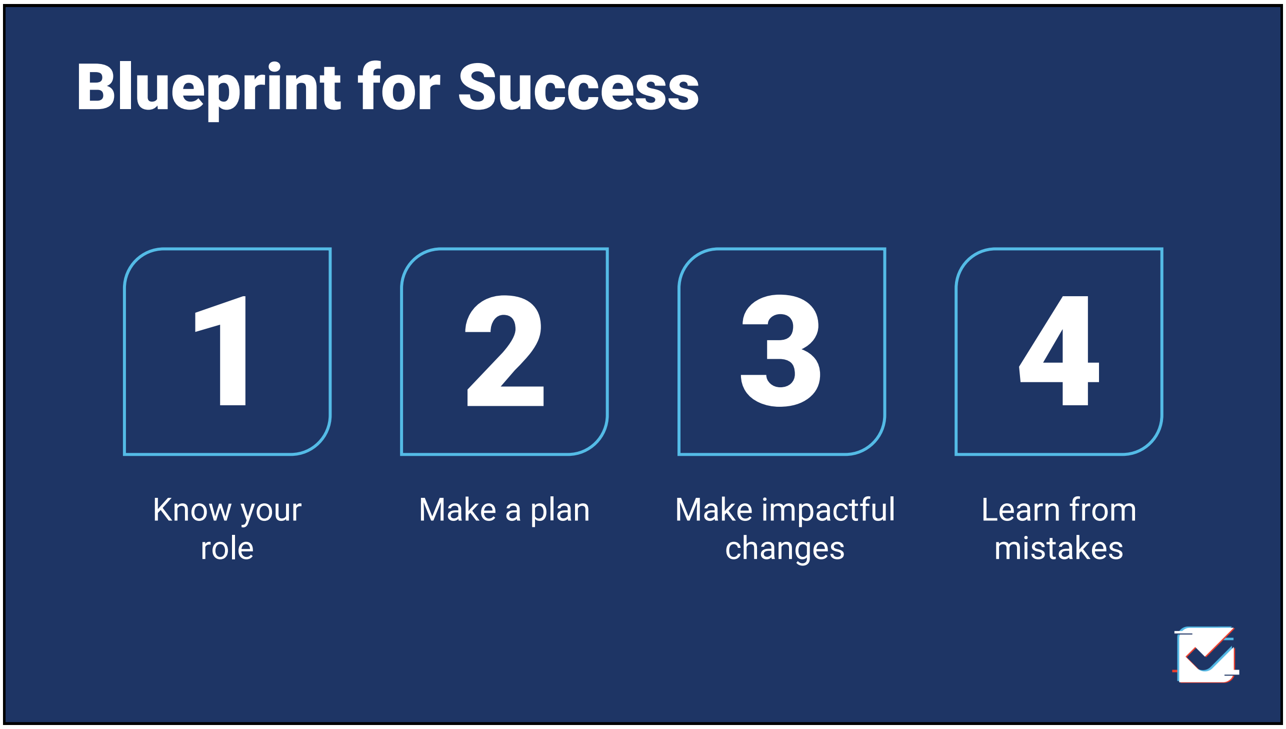
If you need help on building or configuring Log4j or other help on following the instructions to mitigate the known vulnerabilities listed here, please subscribe to, and send your questions to the public Log4j Users mailing list.

If you have encountered an unlisted security vulnerability or other unexpected behaviour that has security impact, or if the descriptions here are incomplete, please report them privately to the Log4j Security Team. Note that reports assuming attacker's access to the Log4j configuration will not qualify as a vulnerability. Thank you for your understanding and help!

Fixed in Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6)

CVE-2021-44832: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration.

9



Blueprint for Success

1 Know your role

2 Make a plan

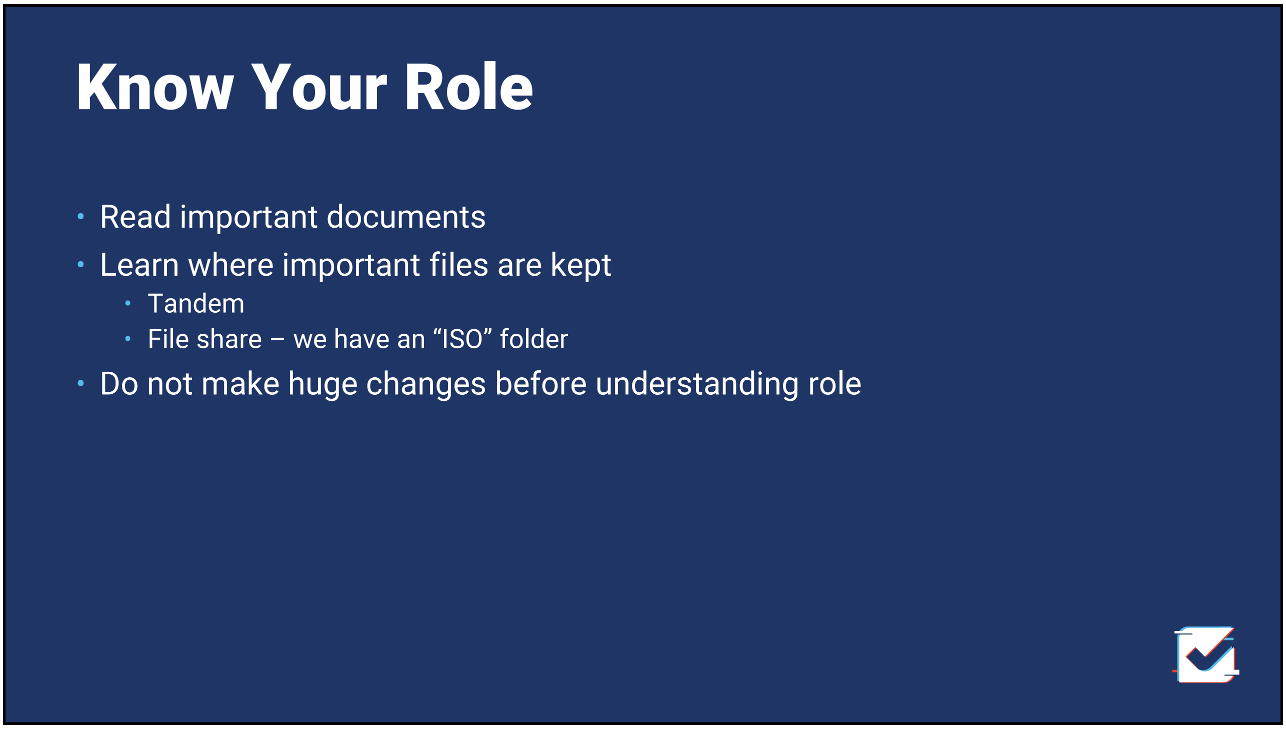
3 Make impactful changes

4 Learn from mistakes

10

Know Your Role

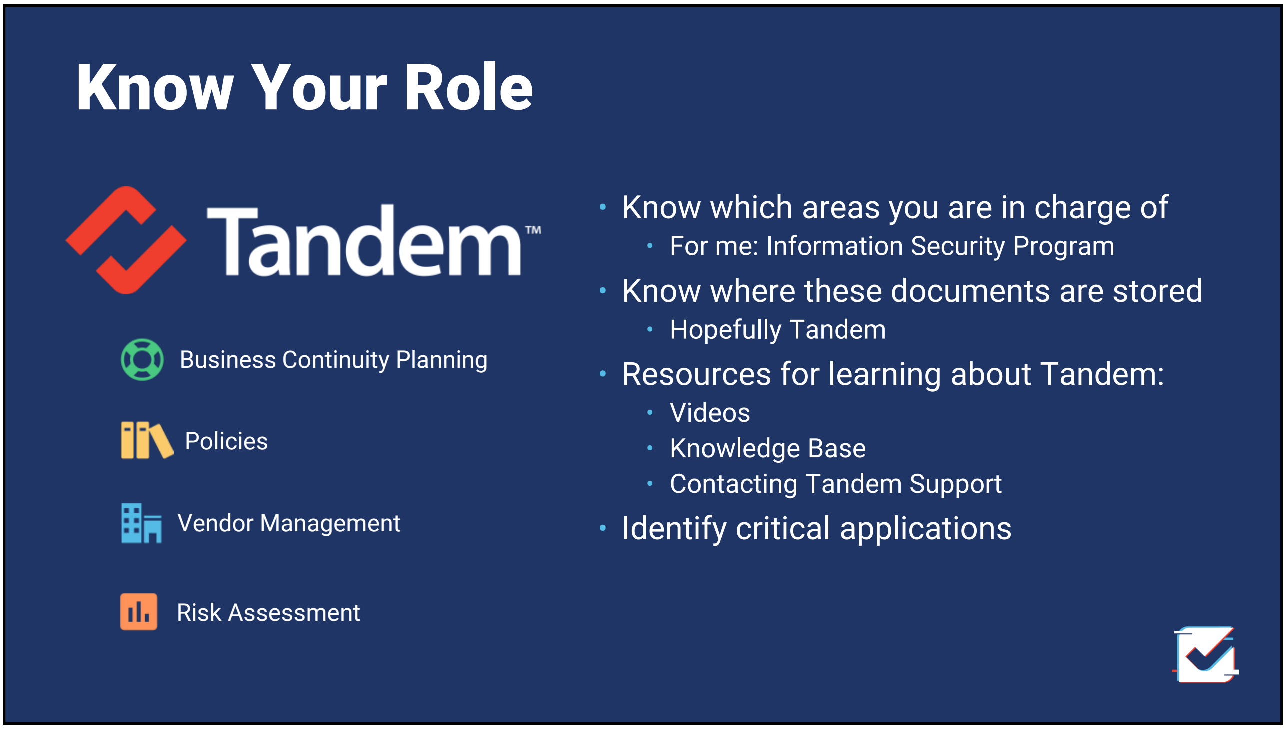
11



Know Your Role

- Read important documents
- Learn where important files are kept
  - Tandem
  - File share – we have an “ISO” folder
- Do not make huge changes before understanding role

12



Know Your Role

- Business Continuity Planning
- Policies
- Vendor Management
- Risk Assessment

- Know which areas you are in charge of
  - For me: Information Security Program
- Know where these documents are stored
  - Hopefully Tandem
- Resources for learning about Tandem:
  - Videos
  - Knowledge Base
  - Contacting Tandem Support
- Identify critical applications

13

Know Your Role

Identify Critical Applications

- Know which applications hold sensitive data
  - Tandem
  - Core
  - Wire/ACH
  - Internet banking
  - Mortgage software
- Understand access to these applications
- How is access removed/managed?
- Learn security settings in place

14

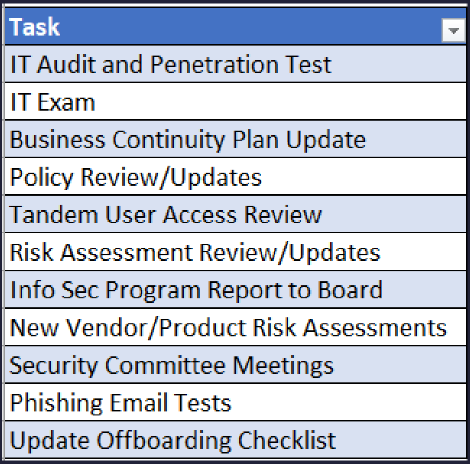
Make a Plan

15

Make a Plan

Make a Plan

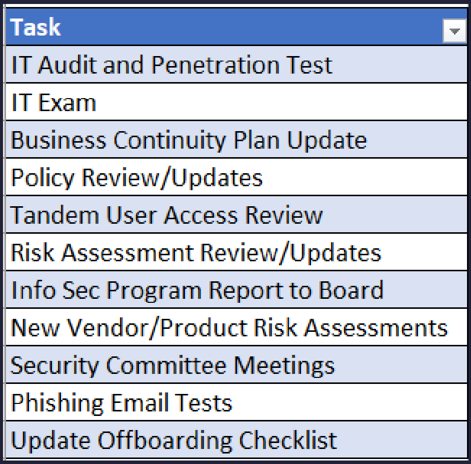
- List everything you do in your role



Task
IT Audit and Penetration Test
IT Exam
Business Continuity Plan Update
Policy Review/Updates
Tandem User Access Review
Risk Assessment Review/Updates
Info Sec Program Report to Board
New Vendor/Product Risk Assessments
Security Committee Meetings
Phishing Email Tests
Update Offboarding Checklist

Make a Plan

- List everything you do in your role
- Determine frequency for each item

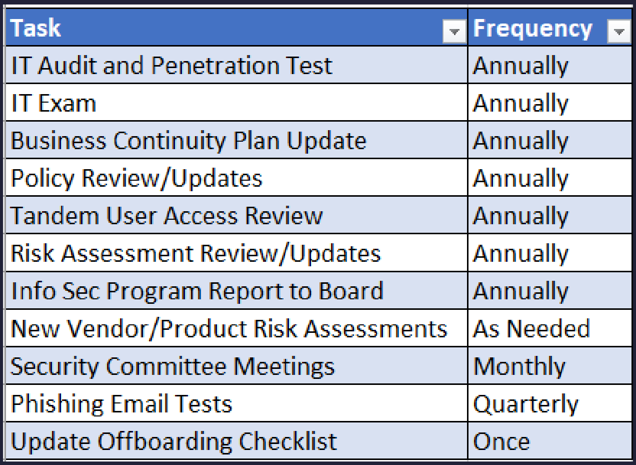


Task
IT Audit and Penetration Test
IT Exam
Business Continuity Plan Update
Policy Review/Updates
Tandem User Access Review
Risk Assessment Review/Updates
Info Sec Program Report to Board
New Vendor/Product Risk Assessments
Security Committee Meetings
Phishing Email Tests
Update Offboarding Checklist

18

Make a Plan

- List everything you do in your role
- Determine frequency for each item

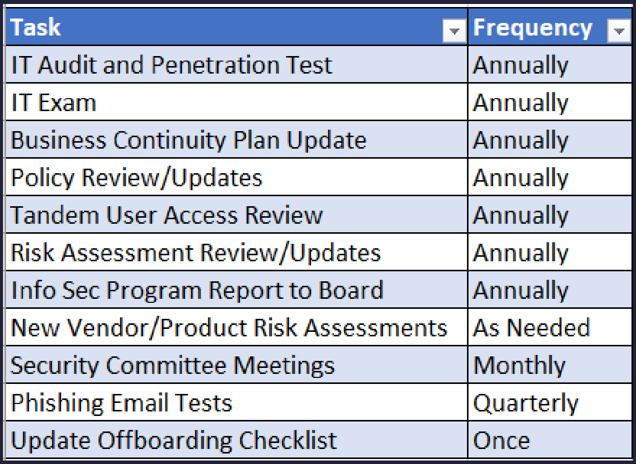


Task	Frequency
IT Audit and Penetration Test	Annually
IT Exam	Annually
Business Continuity Plan Update	Annually
Policy Review/Updates	Annually
Tandem User Access Review	Annually
Risk Assessment Review/Updates	Annually
Info Sec Program Report to Board	Annually
New Vendor/Product Risk Assessments	As Needed
Security Committee Meetings	Monthly
Phishing Email Tests	Quarterly
Update Offboarding Checklist	Once

19

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first

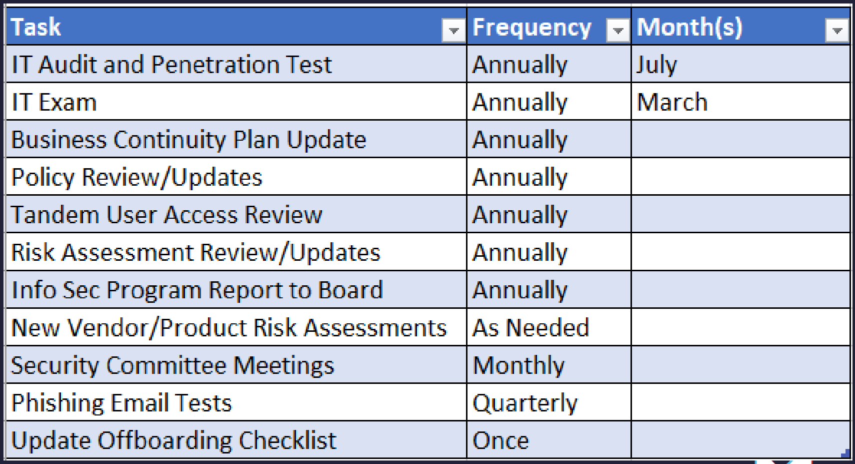


Task	Frequency
IT Audit and Penetration Test	Annually
IT Exam	Annually
Business Continuity Plan Update	Annually
Policy Review/Updates	Annually
Tandem User Access Review	Annually
Risk Assessment Review/Updates	Annually
Info Sec Program Report to Board	Annually
New Vendor/Product Risk Assessments	As Needed
Security Committee Meetings	Monthly
Phishing Email Tests	Quarterly
Update Offboarding Checklist	Once

20

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first

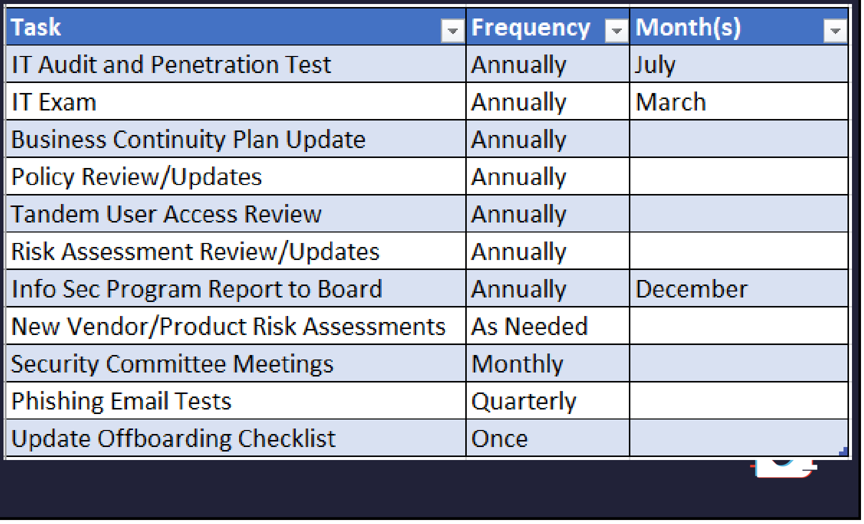


Task	Frequency	Month(s)
IT Audit and Penetration Test	Annually	July
IT Exam	Annually	March
Business Continuity Plan Update	Annually	
Policy Review/Updates	Annually	
Tandem User Access Review	Annually	
Risk Assessment Review/Updates	Annually	
Info Sec Program Report to Board	Annually	
New Vendor/Product Risk Assessments	As Needed	
Security Committee Meetings	Monthly	
Phishing Email Tests	Quarterly	
Update Offboarding Checklist	Once	

21

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first

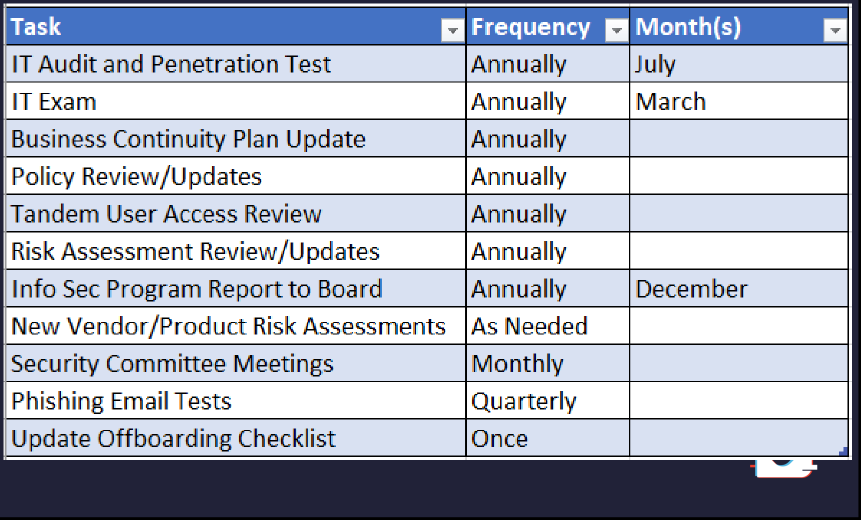


Task	Frequency	Month(s)
IT Audit and Penetration Test	Annually	July
IT Exam	Annually	March
Business Continuity Plan Update	Annually	
Policy Review/Updates	Annually	
Tandem User Access Review	Annually	
Risk Assessment Review/Updates	Annually	
Info Sec Program Report to Board	Annually	December
New Vendor/Product Risk Assessments	As Needed	
Security Committee Meetings	Monthly	
Phishing Email Tests	Quarterly	
Update Offboarding Checklist	Once	

22

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first
- Plan flexible projects around these

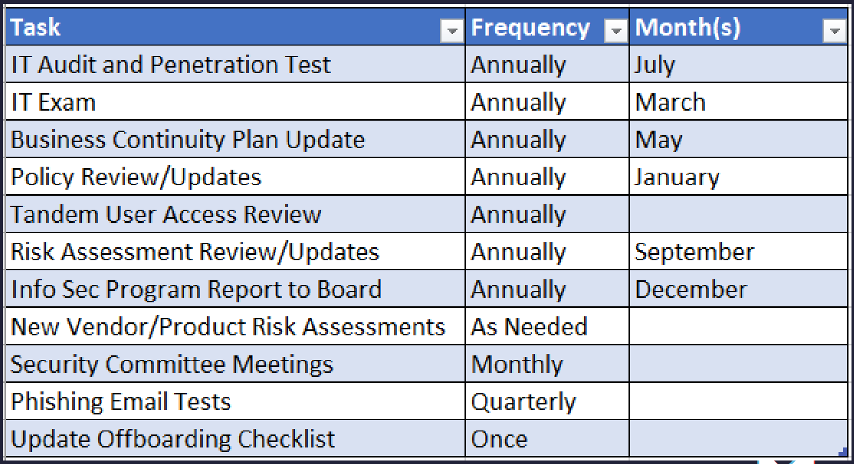


Task	Frequency	Month(s)
IT Audit and Penetration Test	Annually	July
IT Exam	Annually	March
Business Continuity Plan Update	Annually	
Policy Review/Updates	Annually	
Tandem User Access Review	Annually	
Risk Assessment Review/Updates	Annually	
Info Sec Program Report to Board	Annually	December
New Vendor/Product Risk Assessments	As Needed	
Security Committee Meetings	Monthly	
Phishing Email Tests	Quarterly	
Update Offboarding Checklist	Once	

23

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first
- Plan flexible projects around these

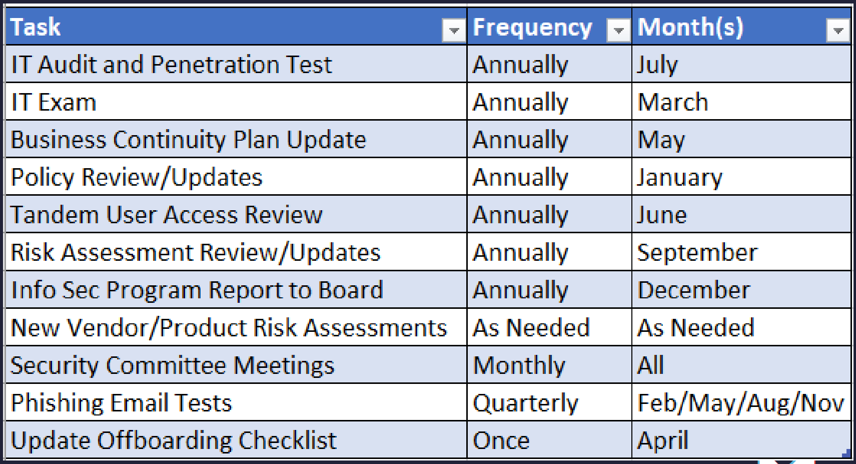


Task	Frequency	Month(s)
IT Audit and Penetration Test	Annually	July
IT Exam	Annually	March
Business Continuity Plan Update	Annually	May
Policy Review/Updates	Annually	January
Tandem User Access Review	Annually	
Risk Assessment Review/Updates	Annually	September
Info Sec Program Report to Board	Annually	December
New Vendor/Product Risk Assessments	As Needed	
Security Committee Meetings	Monthly	
Phishing Email Tests	Quarterly	
Update Offboarding Checklist	Once	

24

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first
- Plan flexible projects around these

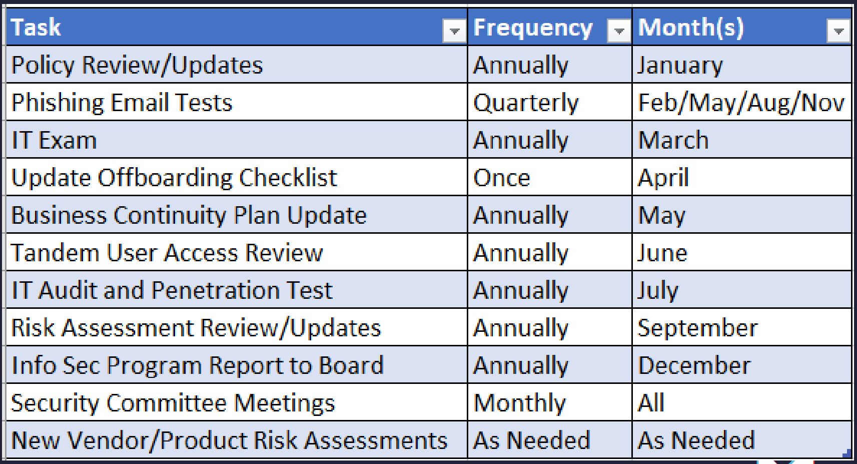


Task	Frequency	Month(s)
IT Audit and Penetration Test	Annually	July
IT Exam	Annually	March
Business Continuity Plan Update	Annually	May
Policy Review/Updates	Annually	January
Tandem User Access Review	Annually	June
Risk Assessment Review/Updates	Annually	September
Info Sec Program Report to Board	Annually	December
New Vendor/Product Risk Assessments	As Needed	As Needed
Security Committee Meetings	Monthly	All
Phishing Email Tests	Quarterly	Feb/May/Aug/Nov
Update Offboarding Checklist	Once	April

25

Make a Plan

- List everything you do in your role
- Determine frequency for each item
- Schedule biggest areas first
- Plan flexible projects around these



Task	Frequency	Month(s)
Policy Review/Updates	Annually	January
Phishing Email Tests	Quarterly	Feb/May/Aug/Nov
IT Exam	Annually	March
Update Offboarding Checklist	Once	April
Business Continuity Plan Update	Annually	May
Tandem User Access Review	Annually	June
IT Audit and Penetration Test	Annually	July
Risk Assessment Review/Updates	Annually	September
Info Sec Program Report to Board	Annually	December
Security Committee Meetings	Monthly	All
New Vendor/Product Risk Assessments	As Needed	As Needed

26

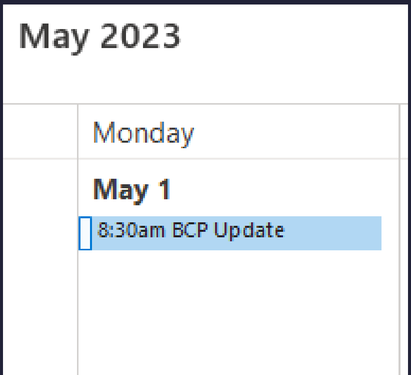
Make a Plan

LEVEL UP

Set Reminders for Tasks

Outlook

Calendar Reminder



May 2023

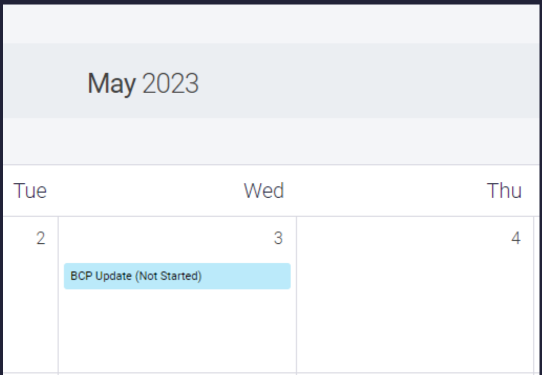
Monday

May 1

8:30am BCP Update

Tandem

Calendar -> Tasks



May 2023

Tue	Wed	Thu
2	3 BCP Update (Not Started)	4

27

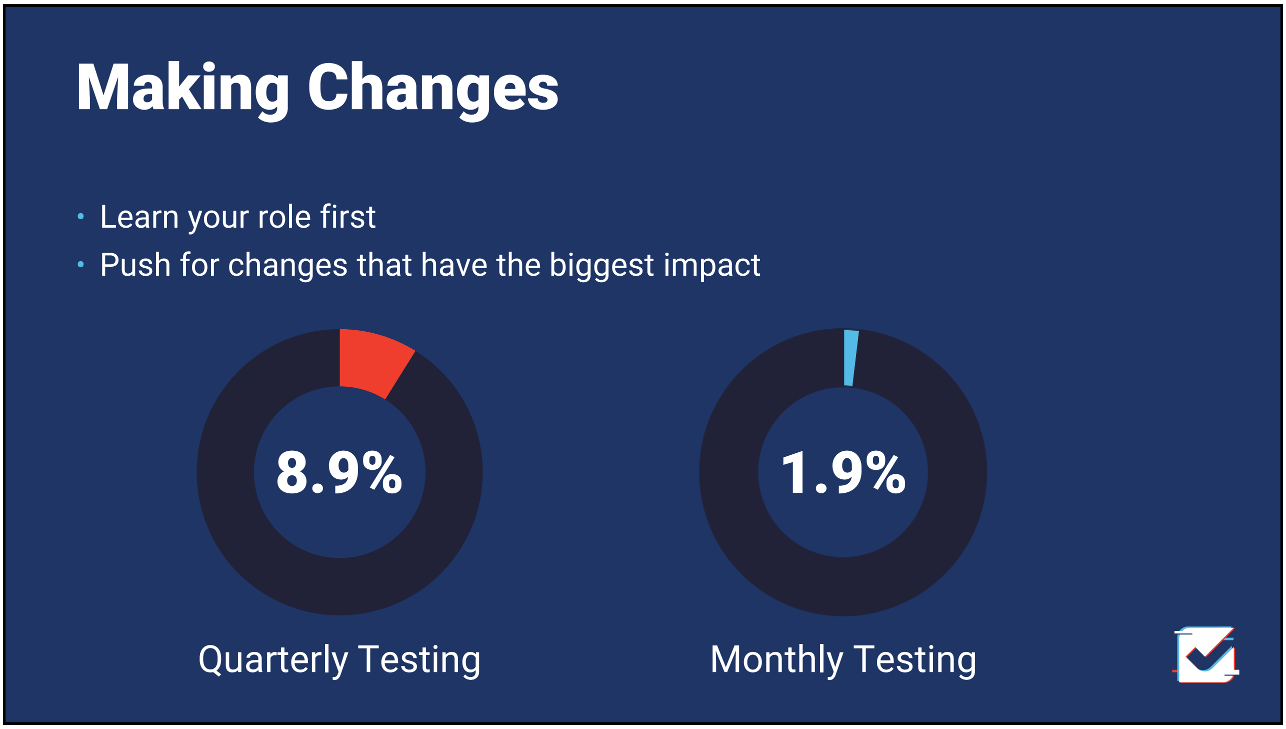
Making Changes

28

AUDIENCE QUESTION

Does anyone want to share an "easy" change that ended up being much more complex?

29



Making Changes

- Learn your role first
- Push for changes that have the biggest impact

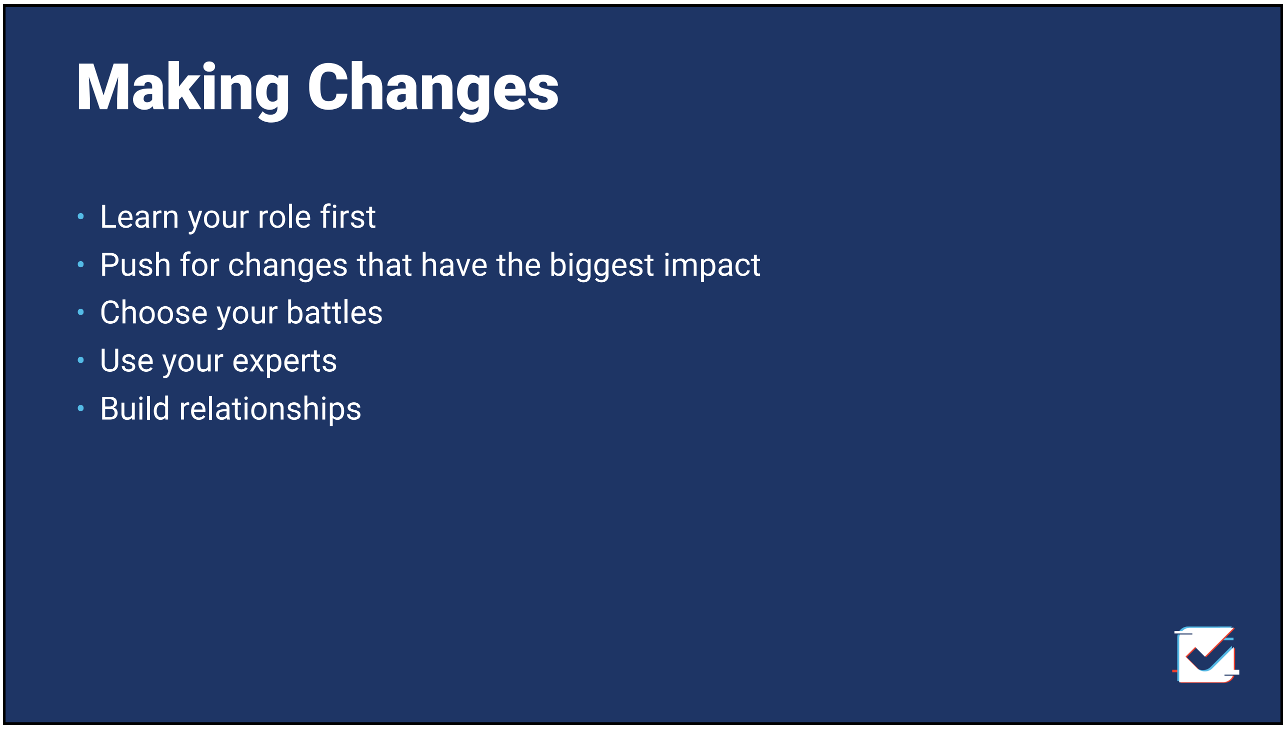
8.9%

Quarterly Testing

1.9%

Monthly Testing

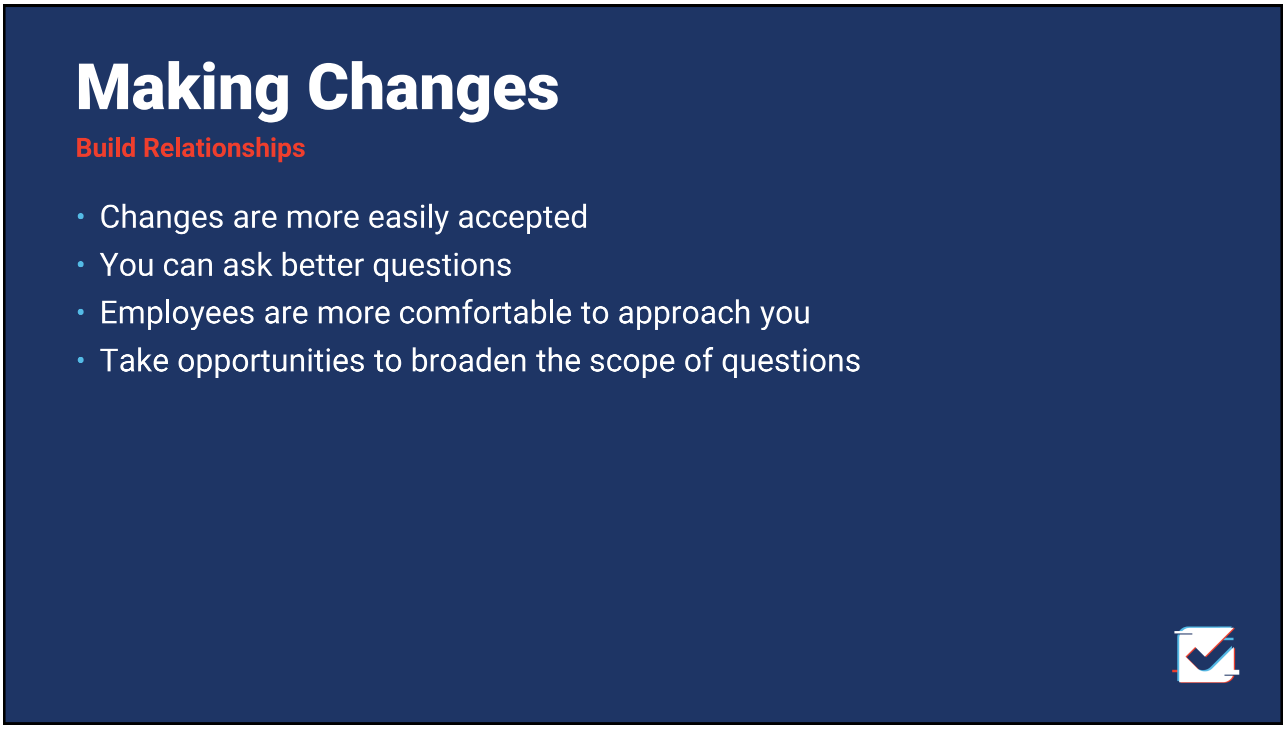
30



Making Changes

- Learn your role first
- Push for changes that have the biggest impact
- Choose your battles
- Use your experts
- Build relationships

31

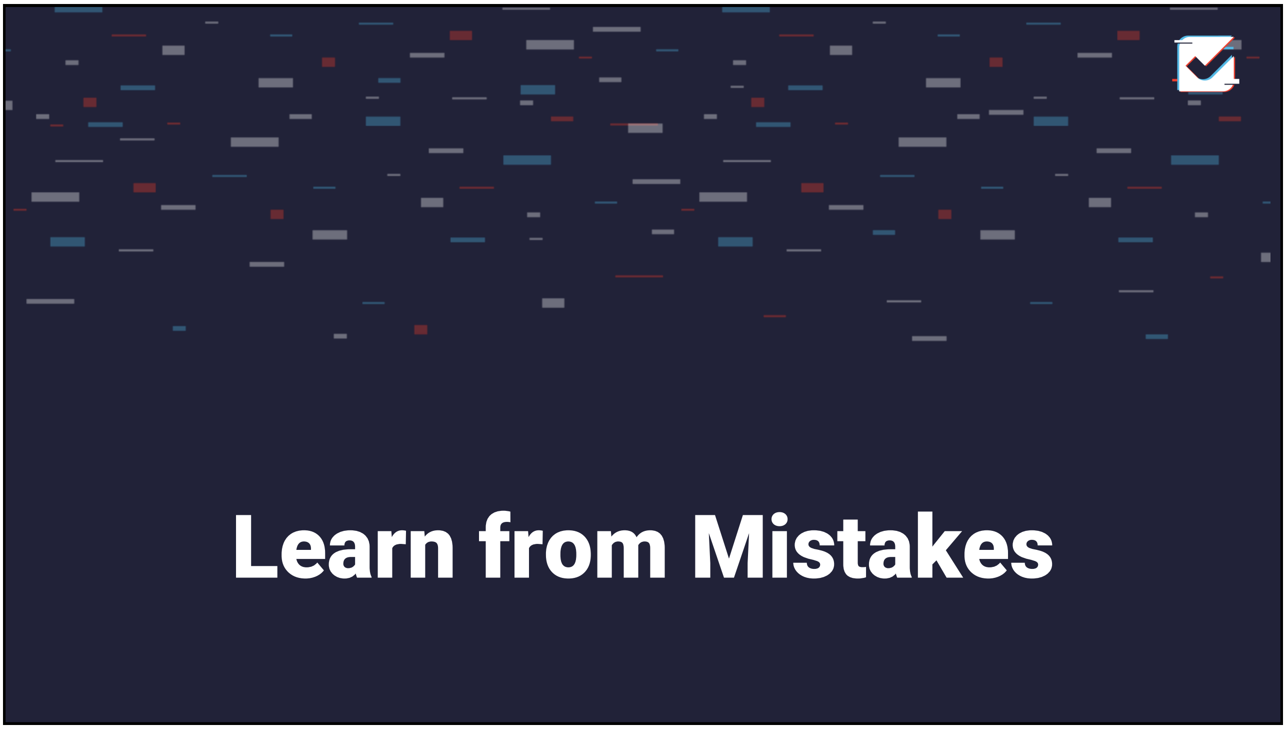


Making Changes

Build Relationships

- Changes are more easily accepted
- You can ask better questions
- Employees are more comfortable to approach you
- Take opportunities to broaden the scope of questions

32



Learn from Mistakes

33

Learn from Mistakes

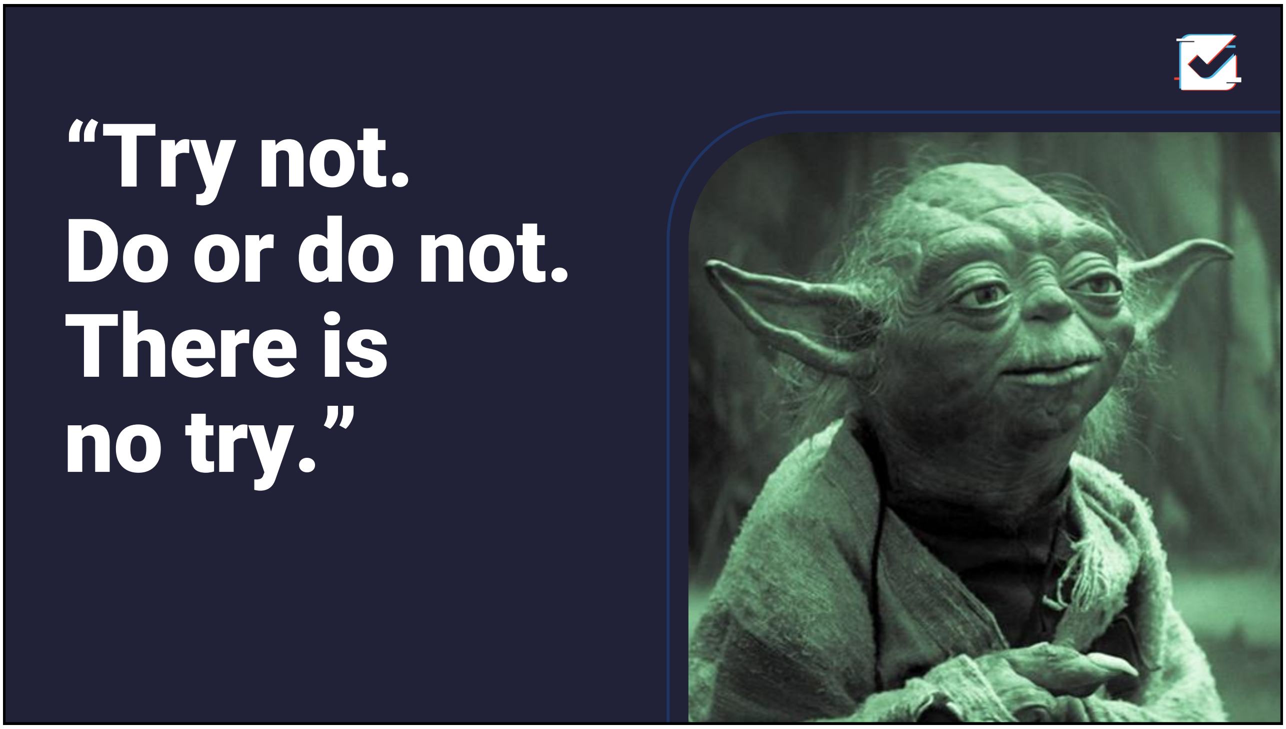
- Taking on too much
- Not using your experts
- Manually repeating the same actions
  - Automate these
- Not enough training for new hires

34

Review

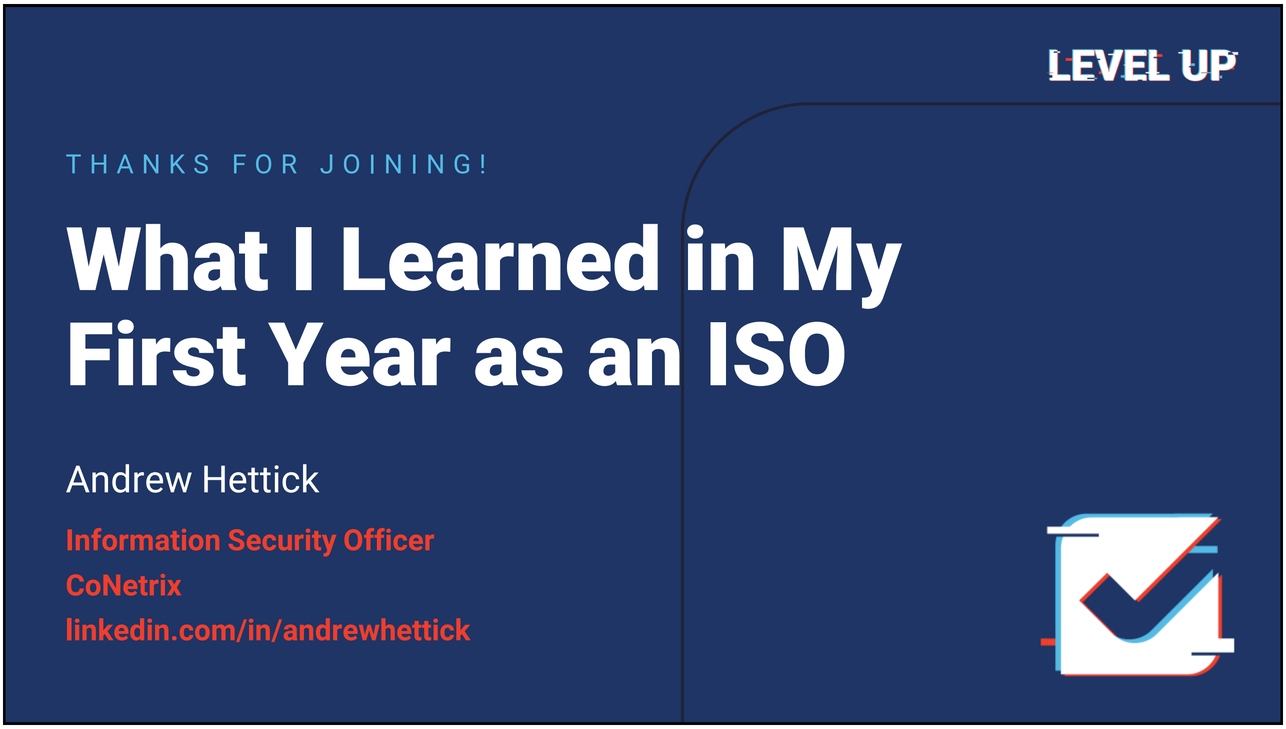
1. Know your role
2. Make a plan
3. Make impactful changes
4. Learn from mistakes

35



“Try not.
Do or do not.
There is
no try.”

36



THANKS FOR JOINING!

What I Learned in My First Year as an ISO

Andrew Hettick

Information Security Officer

CoNetrix

linkedin.com/in/andrewhettick

37