WELCOME TO

The Ins & Outs of Your Annual Report to the Board

Samantha Torrez-Hidalgo,
CSXF
Software Specialist
Tandem

Tandem

SESSION INFO

AUDIO/VIDEO

If you cannot hear sound or see the presentation now, adjust or change your settings.

SURVEY

At the end, fill out the survey for a chance to win an Amazon gift card.

RESOURCES

The slides, a recording, and certificate of attendance will be sent via email.

QUESTIONS

Use the “Questions” panel to chat with the presenter and Tandem team.

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting on ideas from this session.

- **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.

Tandem

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

Tandem™

A CoNetrix company

SUBMIT YOUR QUESTIONS!

We want to hear from you.

Use the “Questions” panel to:

- Ask a question
- Send a chat
- Share a story
- Connect with us

Tandem

ABOUT THE PRESENTER

Samantha Torrez-Hidalgo
Software Specialist

- 10 years IT / Service Industry Experience
- 7 years with Tandem
- Thrives working with her teammates
- Loves problem solving & helping others learn
- Conference speaker & published blog writer

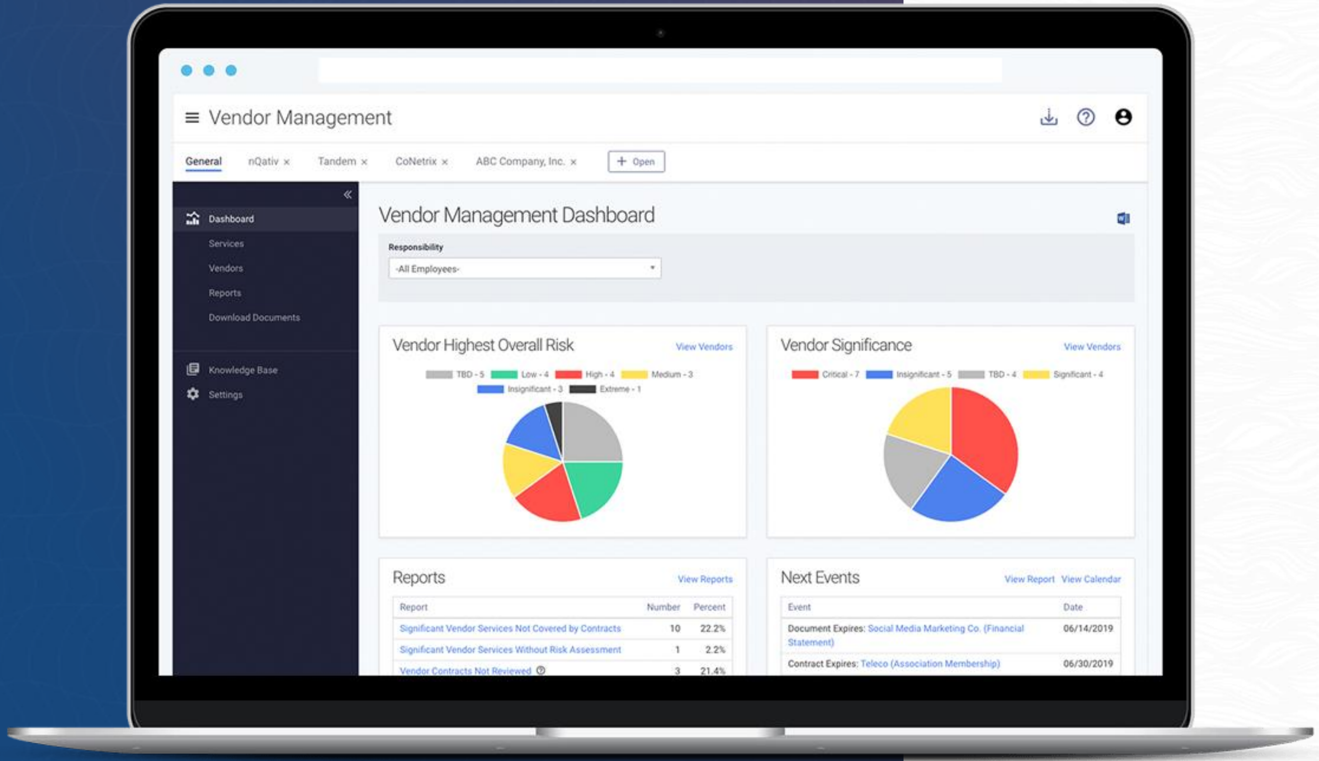
Linkedin.com/in/samanthatorrez

Agenda

- The Report to the Board & You
- Information Security & Your Board
- Identifying Risks
- Applying Controls
- Verifying Sufficiency
- **Bonus Content**: Tandem Product Showcase

BONUS CONTENT

Tandem Product Showcase



Responsibility: -All Employees-

Report	Number	Percent
Significant Vendor Services Not Covered by Contracts	10	22.2%
Significant Vendor Services Without Risk Assessment	1	2.2%
Vendor Contracts Not Reviewed	3	21.4%

Event	Date
Document Expires: Social Media Marketing Co. (Financial Statement)	06/14/2019
Contract Expires: Teleco (Association Membership)	06/30/2019

POLL QUESTION

How do you currently manage your annual report to the board?

The Report to the Board & You

Tandem

“Each organization shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the organization’s compliance with these guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.”

Part 208 Appendix D-2 III F

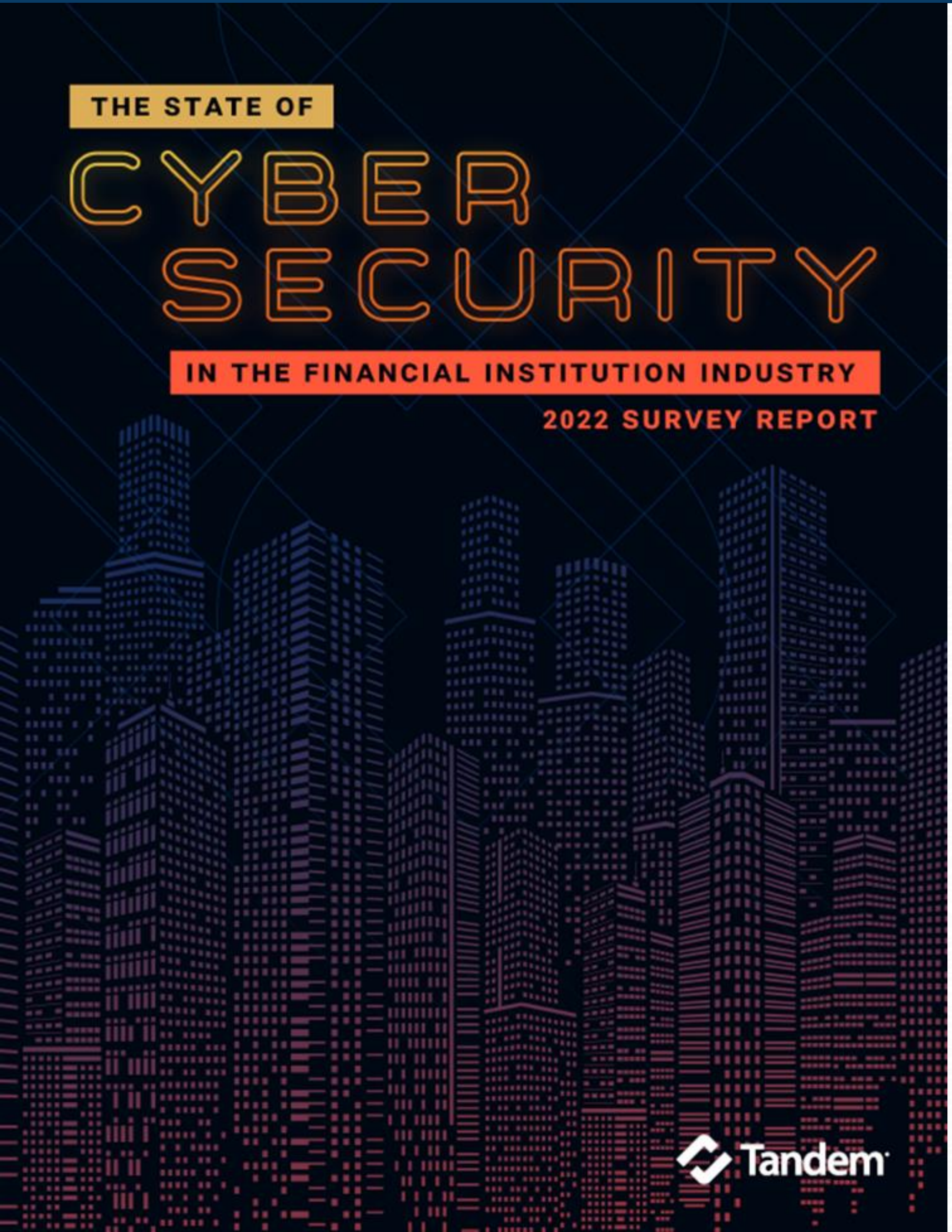
Why is this report so important?

1. Clear Communication
2. Clear Expectations
3. Discussion of Issues
4. Summary of Your Program

Information Security & Your Board

How well do you know your board and their backgrounds?

INFORMATION SECURITY & YOUR BOARD



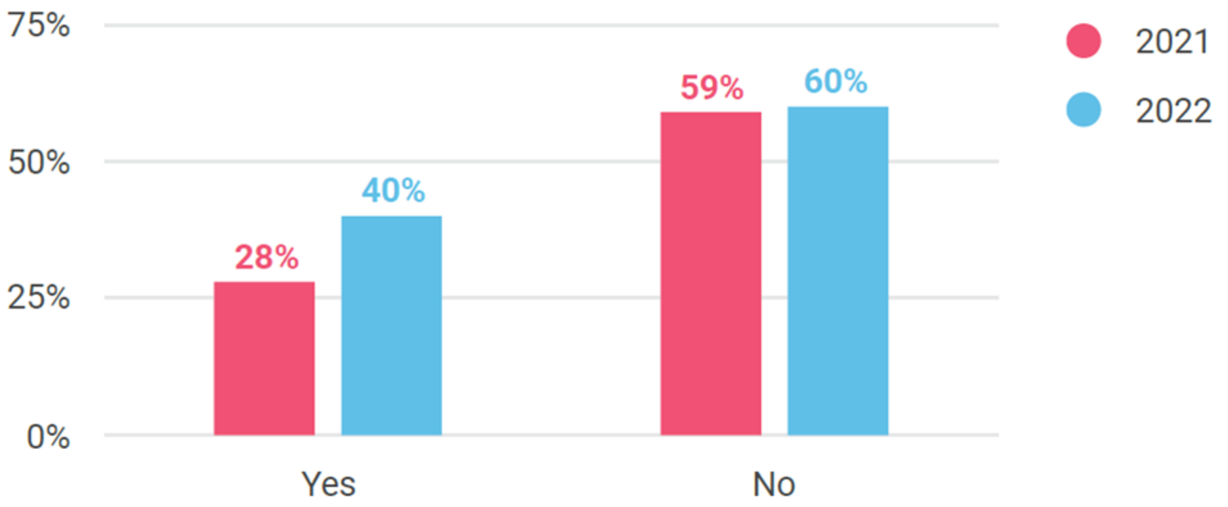
THE STATE OF CYBER SECURITY

IN THE FINANCIAL INSTITUTION INDUSTRY

2022 SURVEY REPORT

Tandem

PERCENT OF INSTITUTIONS WHO HAVE BOARD MEMBERS WITH IT / CYBER EXPERIENCE



WHAT THIS MEANS

The more often a Board is informed on cybersecurity, the more confident cybersecurity professionals are about the Board's ability to make informed decisions on technology matters.

https://tandem.app/state-of-cybersecurity-report

Tandem

POLL QUESTION

Do any of your board members have IT / Cyber experience?

INFORMATION SECURITY & YOUR BOARD

Status of Information Security Program

Designate Information Security Officer (ISO)

Notable Committees to Discuss

Tandem

Knowing Your Board

Background of Your Board

Familiarize Your Board

RESOURCES FOR YOUR BOARD

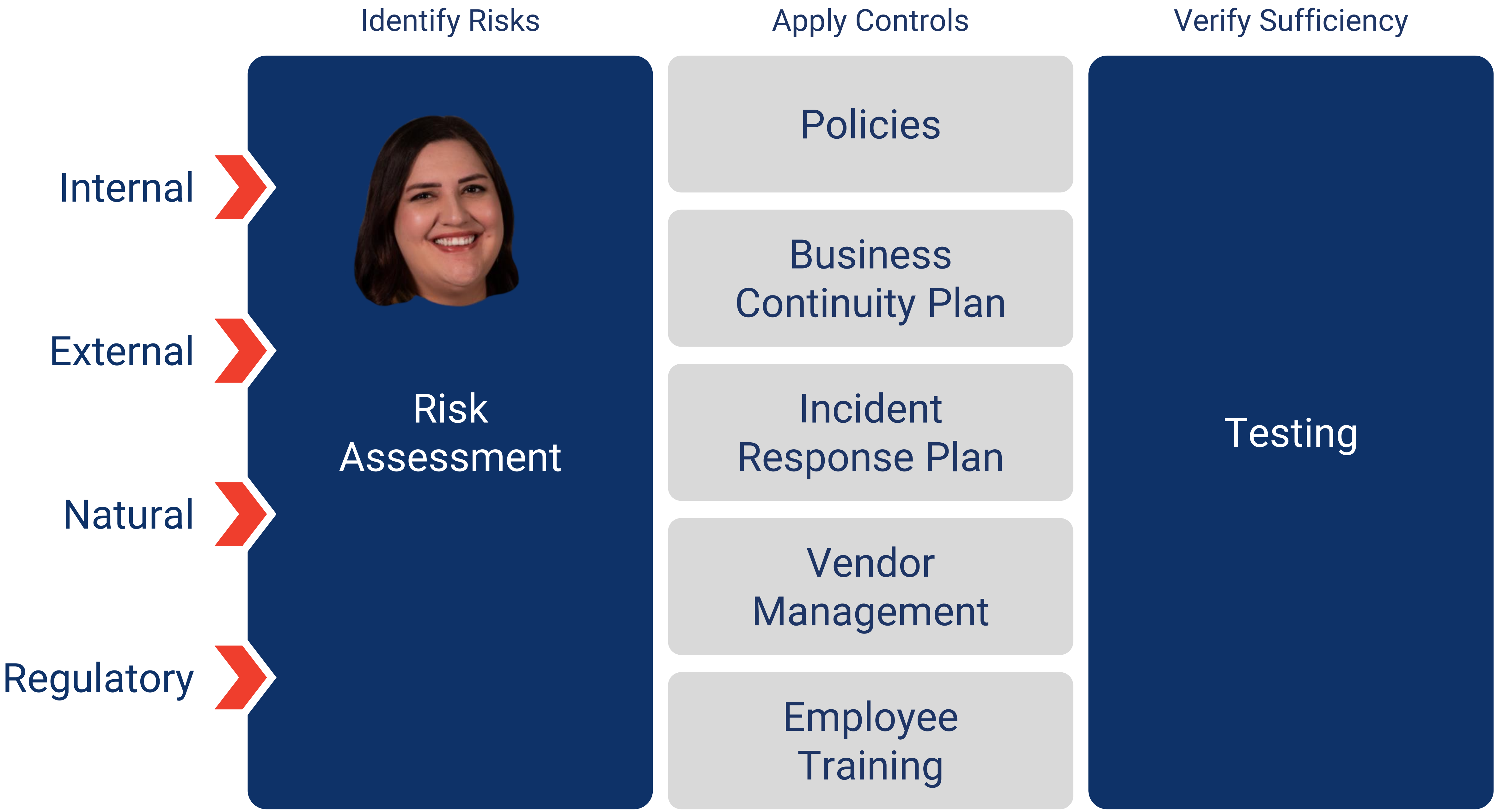
1 Verizon Annual Data Breach Investigations Report

2 CISA Shields Up

3 Malwarebytes Labs

Tandem

Risk Assessment



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Testing

RISK ASSESSMENT

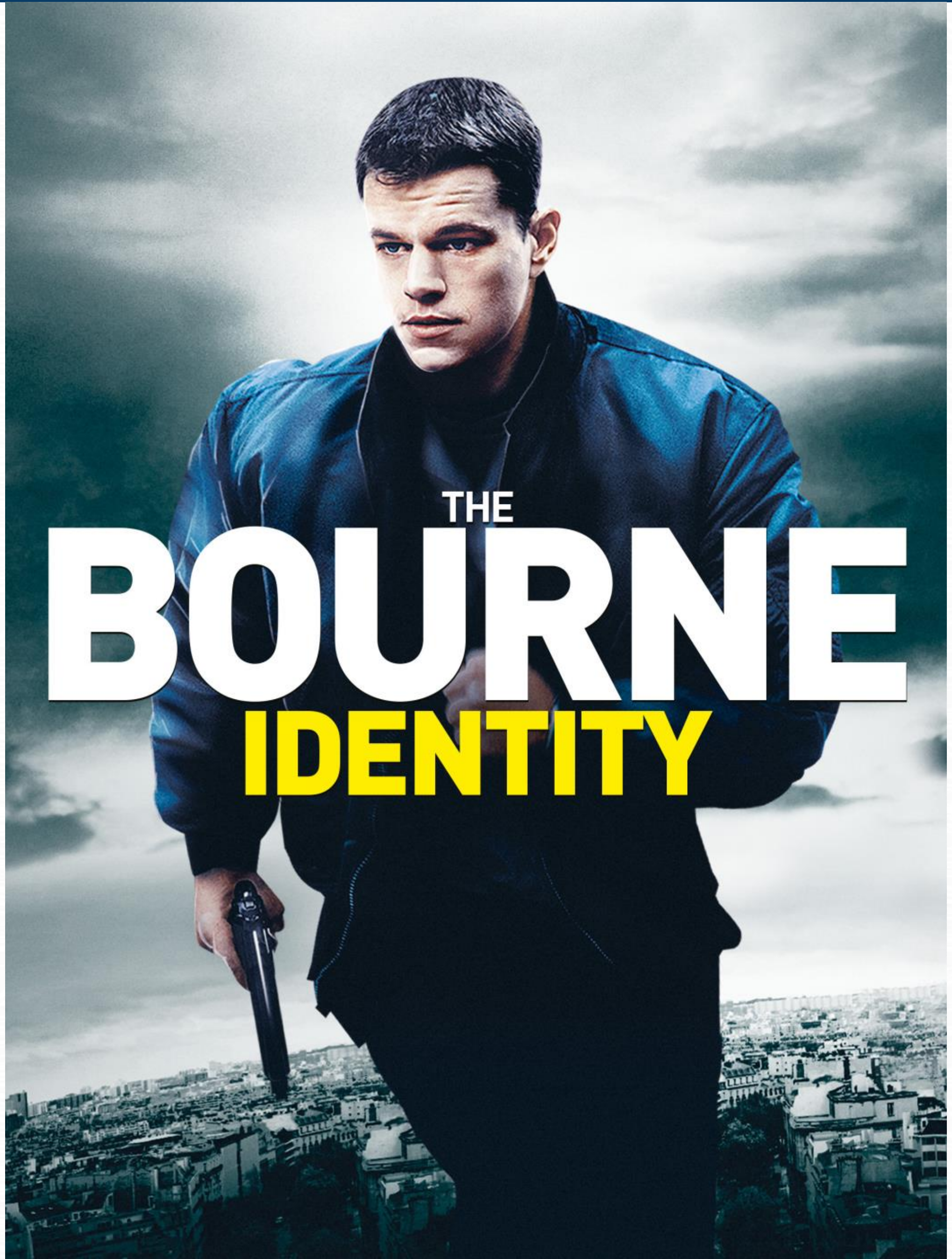
WHAT DO I INCLUDE?

Information Security Risk Assessment (ISRA)

Asset-Based Risk Assessments (ABRA)

RISK ASSESSMENT

Confidentiality



Availability

https://www.primevideo.com/detail/The-Bourne-Identity/0KVPNDG1N61Y1PPFGXWC102VSX

Tandem

RISK ASSESSMENT

CIA RATINGS & YOUR BOARD

Priority of Assets

Areas of Concern

New Risks

RISK ASSESSMENT

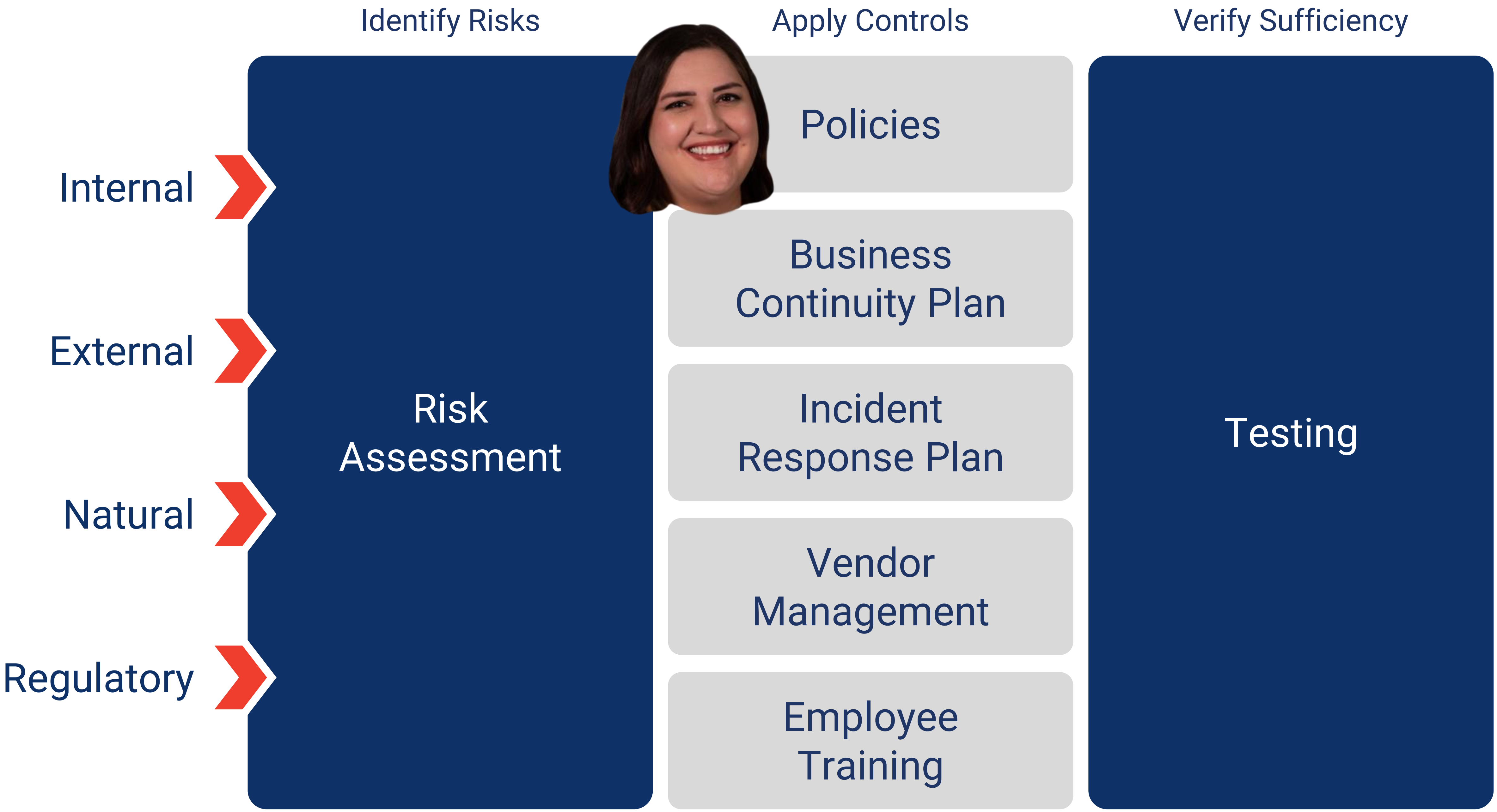
Include Information Security Risk Assessment

Include Asset-Based Risk Assessments

Discuss CIA Ratings

Tandem

Information Security Policies



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Testing

"Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities.“

FFIEC IT Examination Handbook, Information Security Booklet

Include & Prepare:

1. New, Updated, and Removed Policies

2. Purpose for Changes

3. High Level Discussion

SOMETHING TO THINK ABOUT…

Are your policies acting as controls for any risk assessments?

Don’t worry about reading every line of every policy.

Focus on discussing the important changes your board needs to know about.

INFORMATION SECURITY POLICIES

Mobile Device Management Policy

Incident Management Policy

Cloud Computing Policy

User Authentication Policy

INFORMATION SECURITY POLICIES

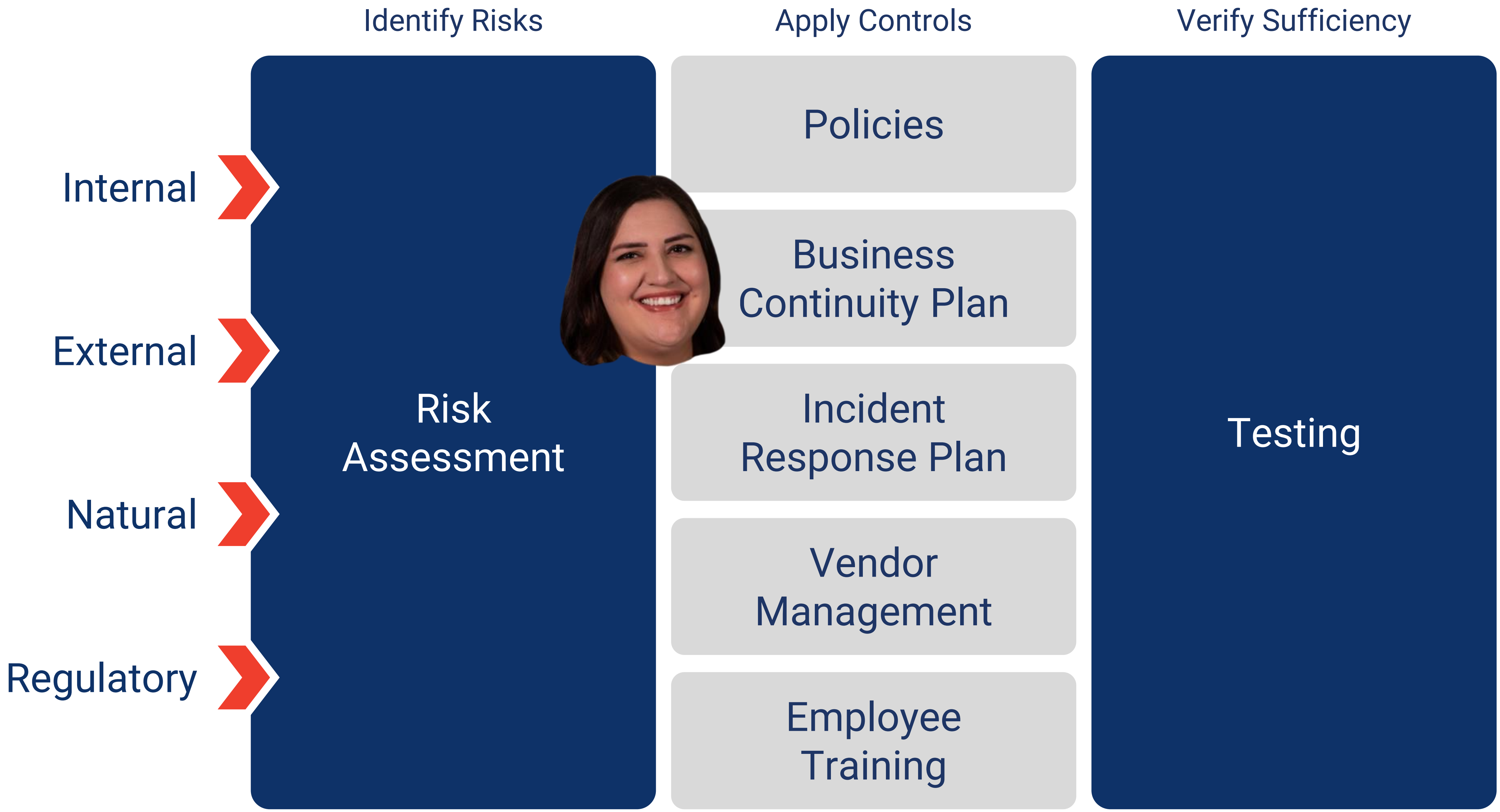
Policies as Controls

Keep It Simple

Discuss Important Changes

Business Continuity Plan

Tandem



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Testing

BUSINESS CONTINUITY PLAN

Business Processes

Preparedness Controls

IMPORTANT PREPAREDNESS CONTROLS

- Alternate Command / Data Center
- Customer Communication Plan
- Emergency Checklists
- Evacuation Procedures
- Emergency Lighting, Power, & Supplies
- System/Equipment Recovery Plans

BUSINESS CONTINUITY PLAN

Business Processes

Preparedness Controls

Recent Testing

Upcoming Testing

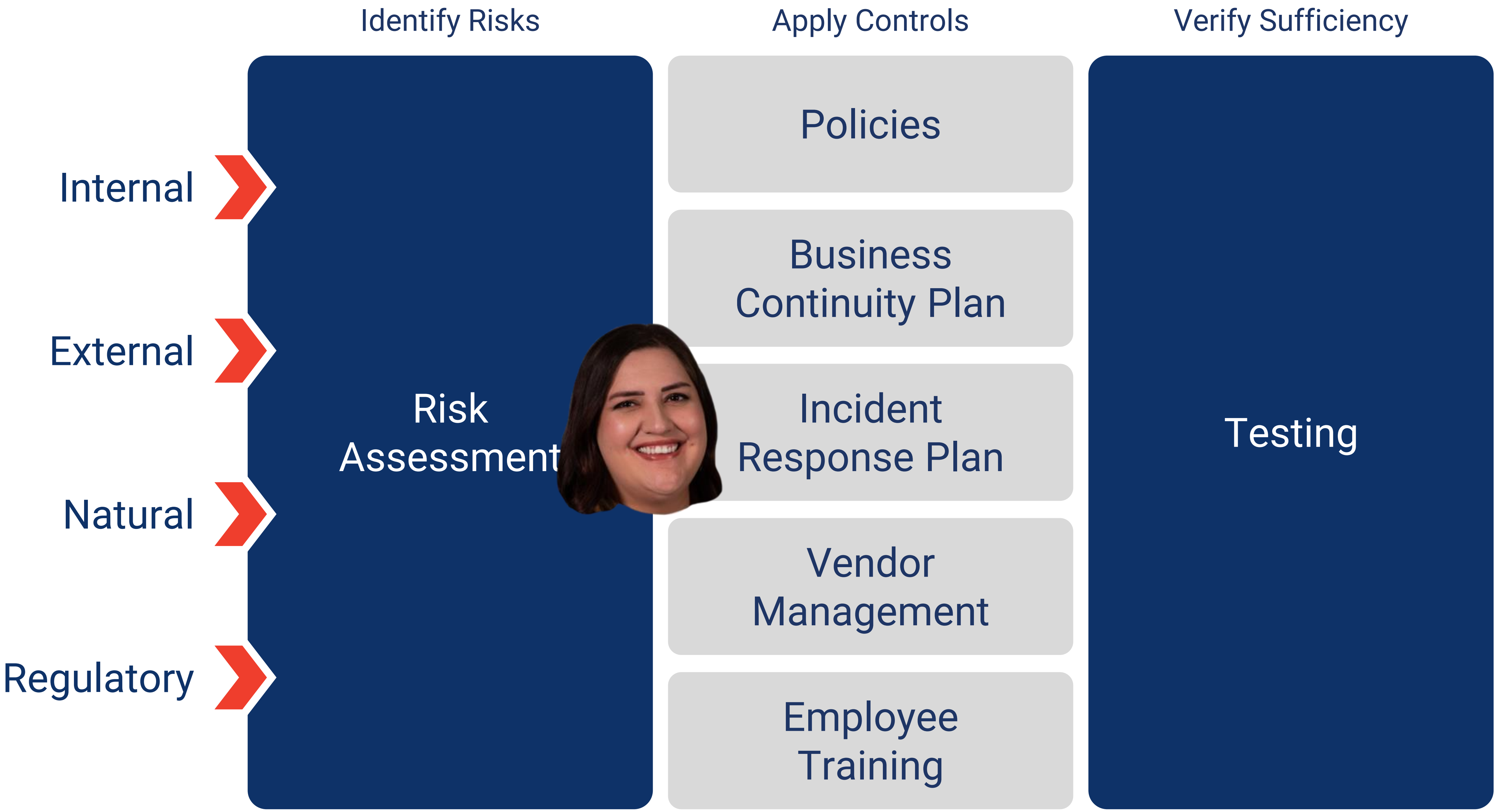
Business Processes

Preparedness Controls

BCP Tests

Incident Response Plan

Tandem



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

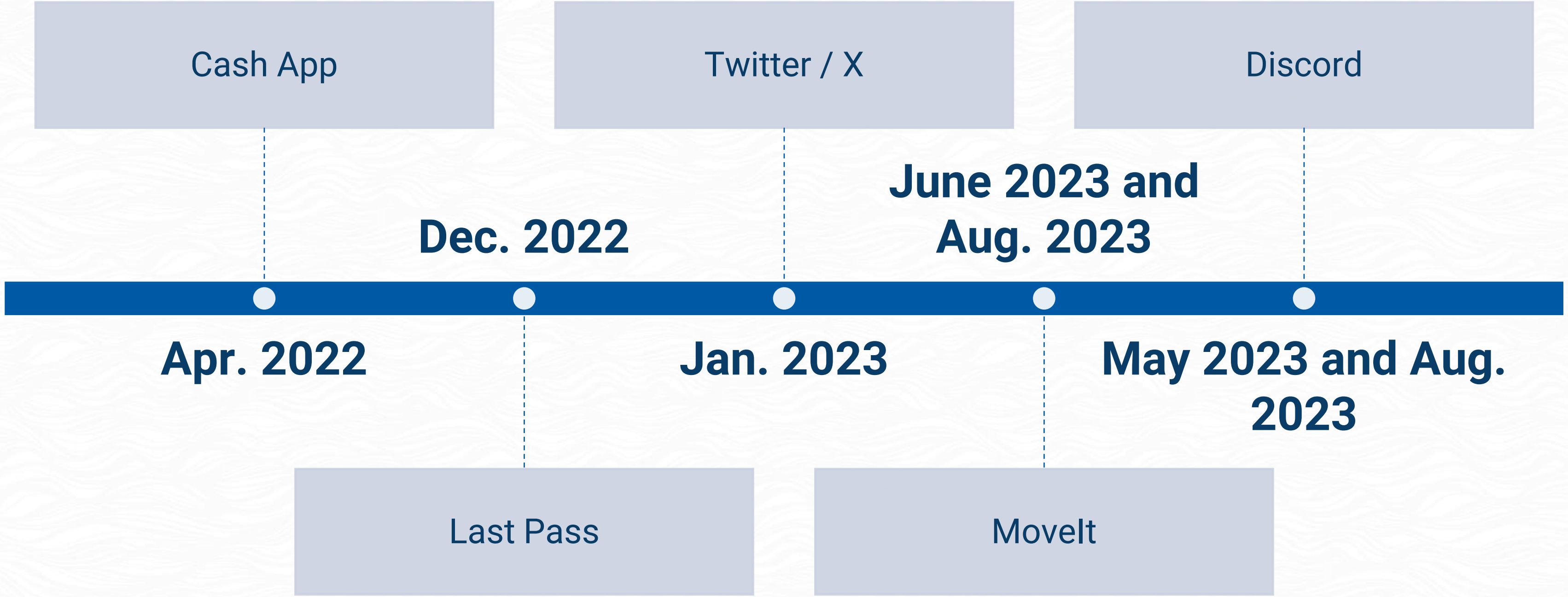
Incident Response Plan

Vendor Management

Employee Training

Testing

Recent Incidents



Cash App

Twitter / X

Discord

June 2023 and Aug. 2023

Dec. 2022

Apr. 2022

Jan. 2023

May 2023 and Aug. 2023

Last Pass

MoveIt

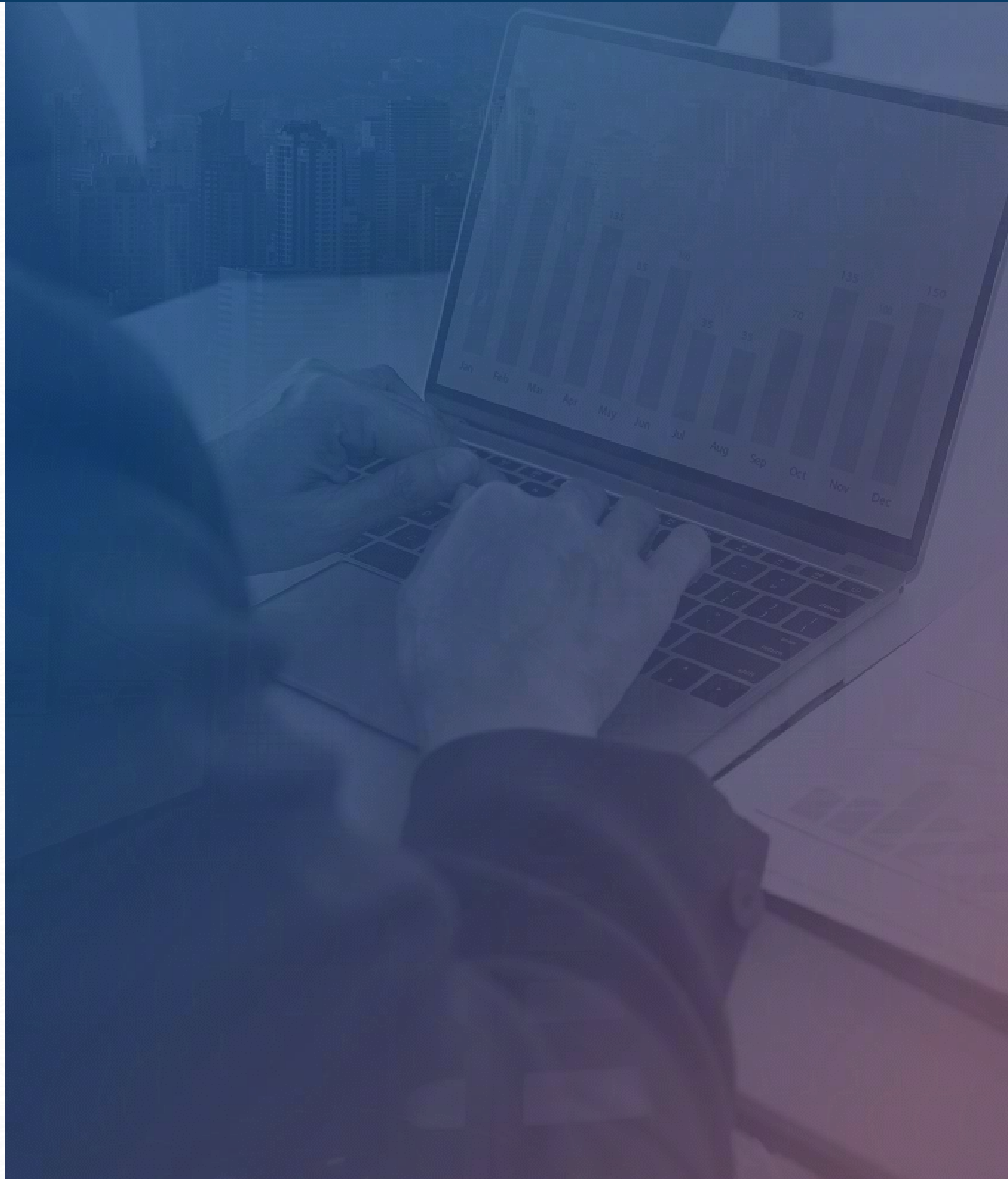
https://tech.co/news/data-breaches-updated-list https://www.upguard.com/blog/biggest-data-breaches-us

What should be included?

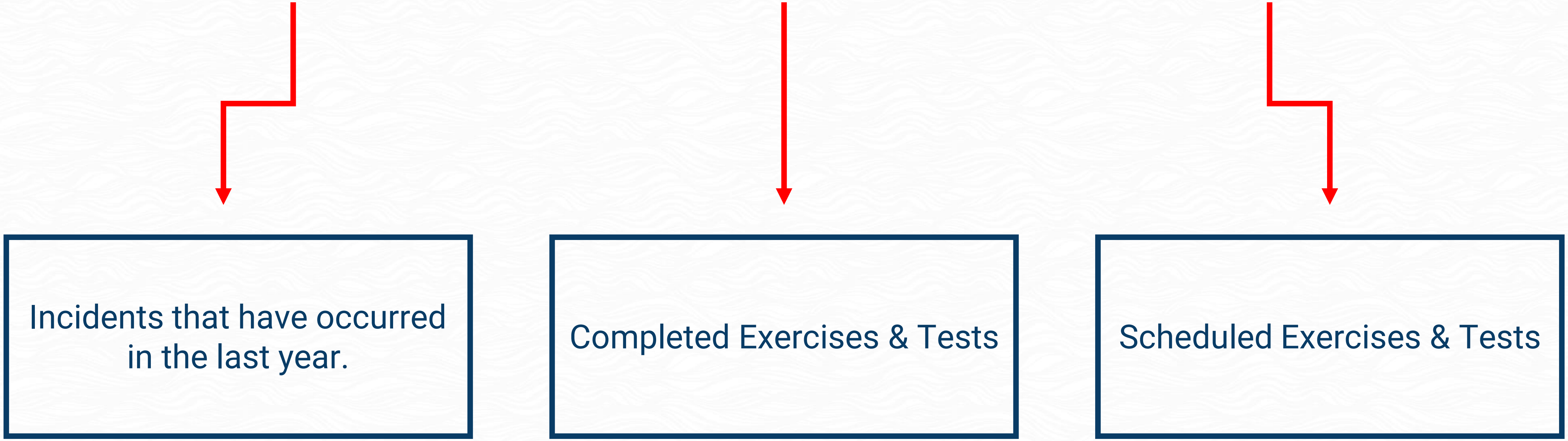
Incidents that have occurred in the last year.

WHAT ARE “NOTEWORTHY” INCIDENTS?

Third-Party Incidents	• Organization Data Compromised
Customer Incidents	• Customer Data Exposed
DDoS Incidents	• Sites Unavailable
Ransomware Incidents	• Organization Data Compromised / Unavailable
Theft Incidents	• Organization Property Stolen



What should be included?

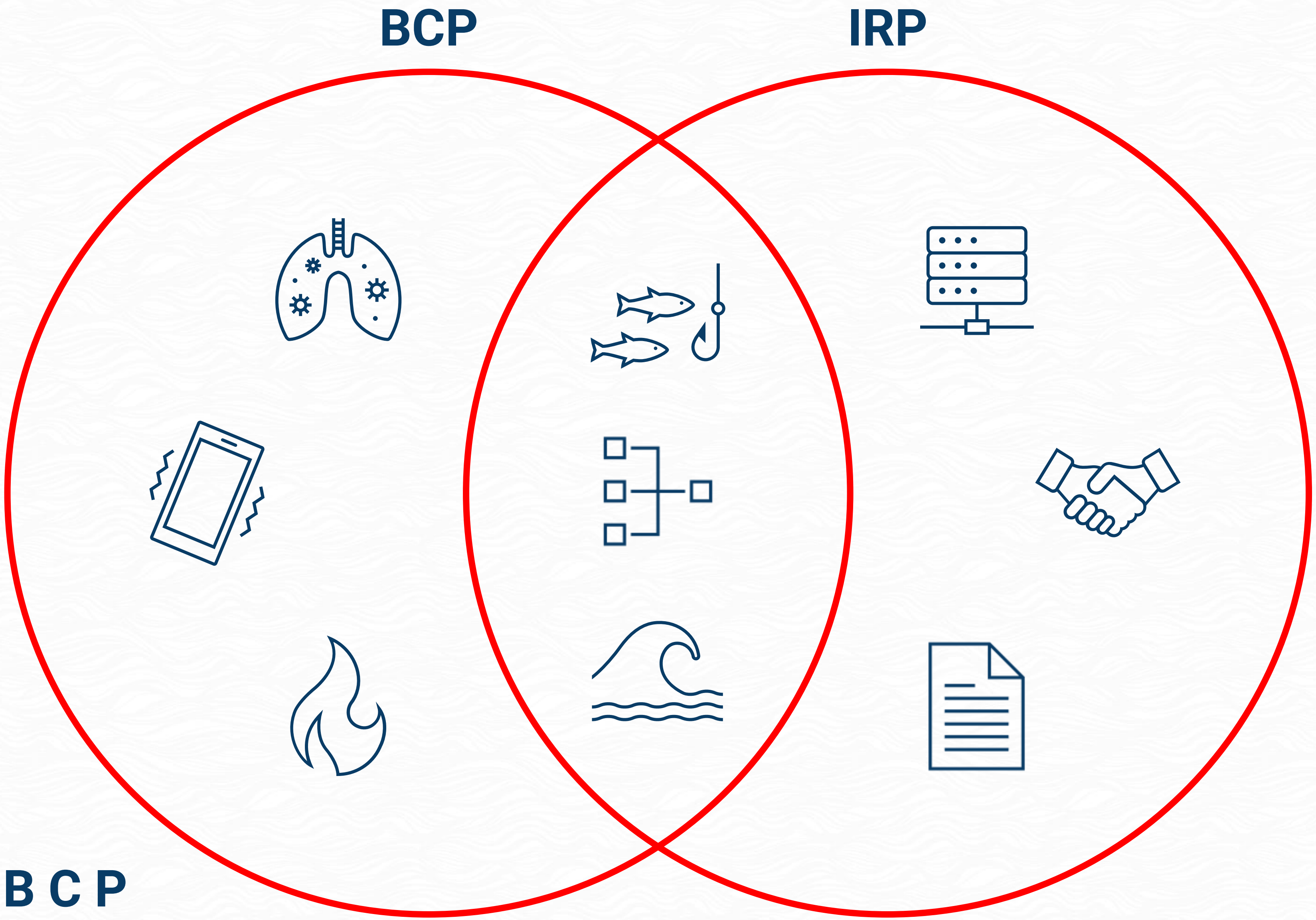


Incidents that have occurred in the last year.

Completed Exercises & Tests

Scheduled Exercises & Tests

INCIDENT RESPONSE PLAN



SHARED BCP & IRP TESTS

Tandem

INCIDENT RESPONSE PLAN

Understanding Incidents

Discussing Recent Incidents

Reviewing Testing Plans & Results

Vendor Management

Tandem

Identify Risks

Internal

External

Natural

Regulatory

Risk Assessment

Apply Controls

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Verify Sufficiency

Testing

VENDOR MANAGEMENT

Include ✓

New & Renewed Vendor Relationships

Don’t Include ⊘

All Vendors

Vendor Service, Significance, & Risk

1. Types of Services Renewed / Changed
2. Significance of Vendor Relationship
3. Risk of Vendor Relationship
4. Third-Party Incidents

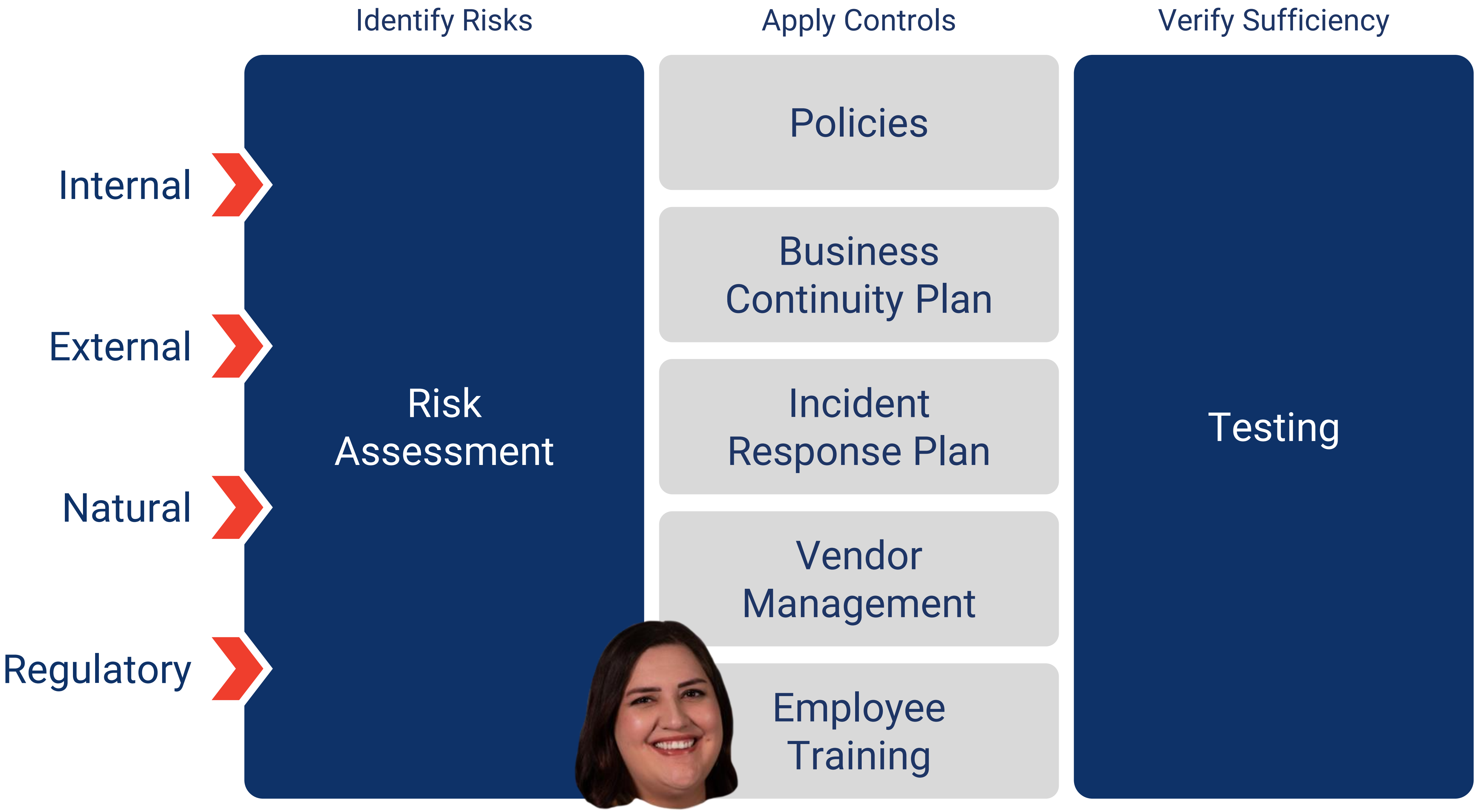
VENDOR MANAGEMENT

New & Renewed Vendor Relationships

Types of Services Updated

Third Party Incidents

Security Awareness Training



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Testing

POLL QUESTION

What type of security awareness training do your employees go through?

Tandem

POLL QUESTION

How frequently do your employees go through any type of security awareness training?

WHAT TYPE OF TRAINING DOES THIS INCLUDE?

- ☑ Acceptable Use Policy Training
- ☑ General Security Awareness Training
- ☑ Identity Theft Prevention Training (Red Flag)
- ☑ Security Incident Management Training
- ☑ Phishing Training

Date of Training

Who was Trained

Percentage Completed

SECURITY AWARENESS TRAINING

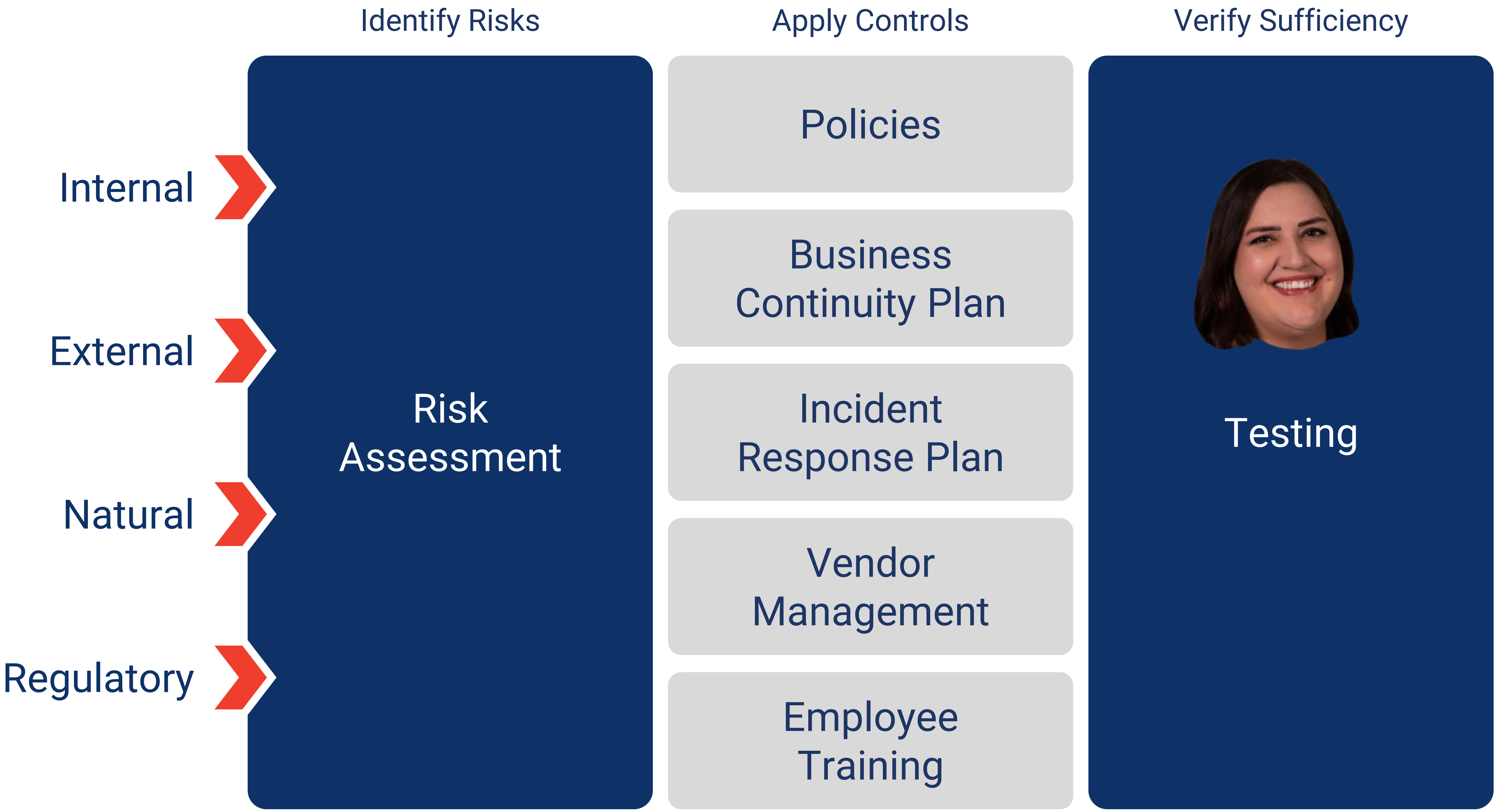
Variety of Courses

Learning Management System (LMS)

Details of Testing

Tandem

Assurance & Testing



Identify Risks

Apply Controls

Verify Sufficiency

Internal

External

Natural

Regulatory

Risk Assessment

Policies

Business Continuity Plan

Incident Response Plan

Vendor Management

Employee Training

Testing

ASSURANCE & TESTING

1 Audit

2 Penetration Test

3 Vulnerability Assessment

4 Self-Assessment

INCLUDE IN REPORT:

- ✓ Type of Testing
- ✓ Date of Testing
- ✓ Status (Complete & Incomplete)

HOW TO VERIFY YOUR CONTROLS

- BCP Testing
- External Vulnerability Scan
- Password Audit
- Social Engineering Audit

WHY DOES MY BOARD NEED TO KNOW ABOUT TESTING?

1

Are there unresolved issues?

2

Can they help you resolve these issues?

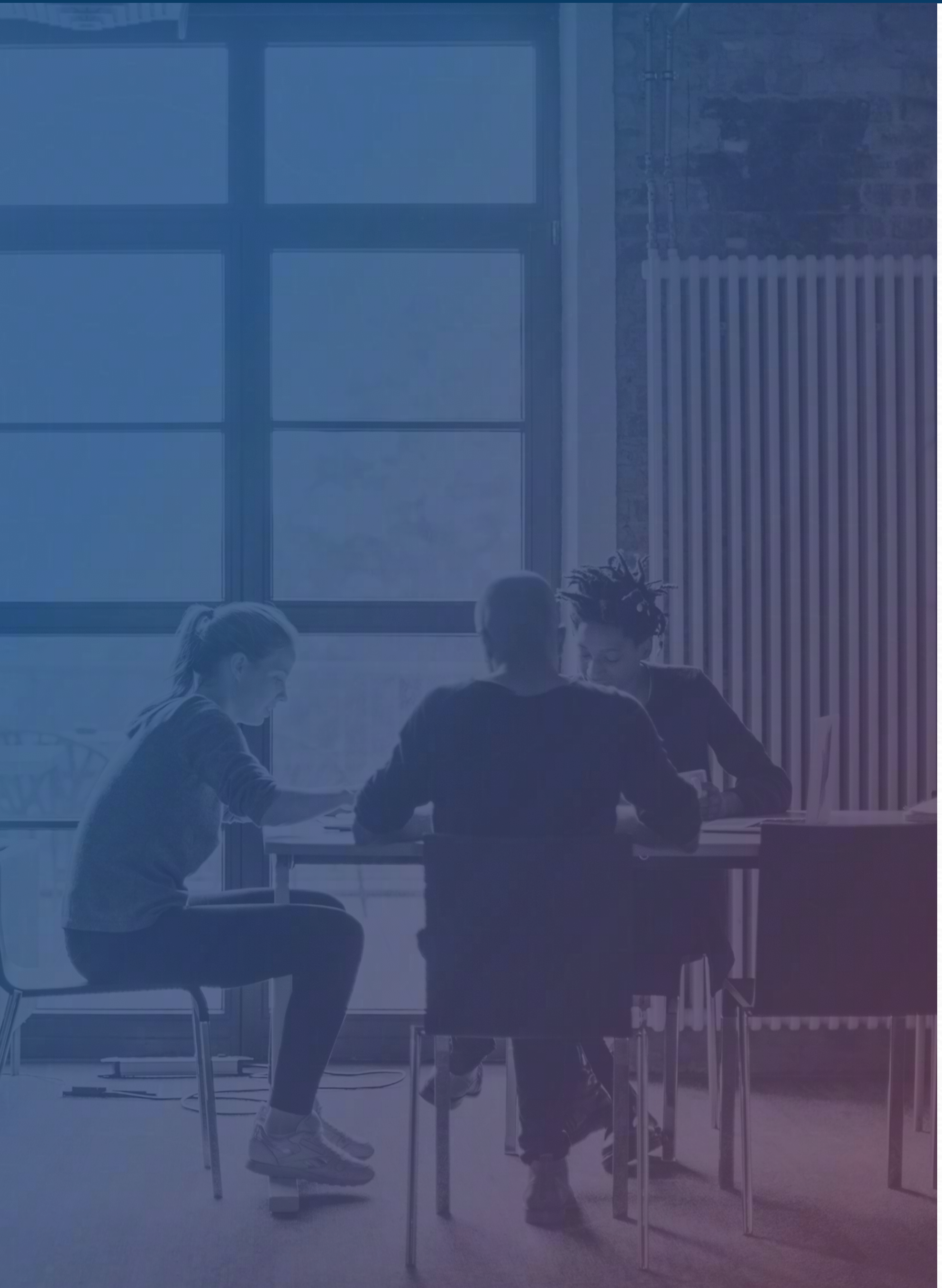
ASSURANCE & TESTING

Discuss Types of Testing

Additional Methods of Verification

Transparency about Unresolved Issues

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

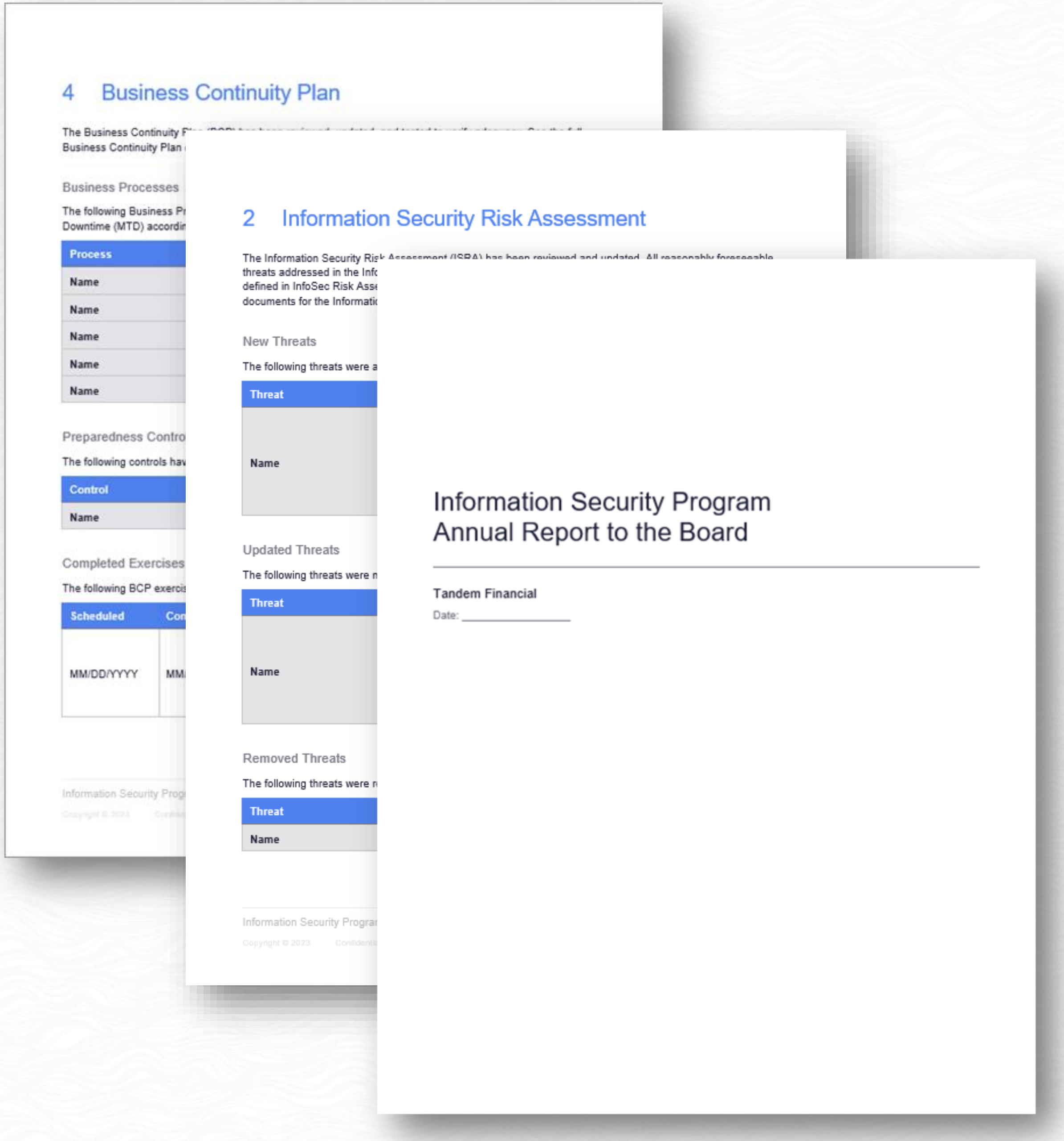


- The Report to the Board & You
- Information Security & Your Board
- Identifying Risks
- Applying Controls
- Verifying Sufficiency

Tandem

GOALS OF THE REPORT

- Showcase Your Work
- Provide Visibility for the Program
- Build a Positive Relationship
- Create Progress for the Future
- Save Them Money



4 Business Continuity Plan

The Business Continuity P
Business Continuity Plan

Business Processes

The following Business Pr
Downtime (MTD) accordin

Process
Name
Name
Name
Name
Name

Preparedness Contro

The following controls hav

Control
Name

Completed Exercises

The following BCP exercis

Scheduled	Con
MM/DD/YYYY	MM/

Information Security Prog

2 Information Security Risk Assessment

The Information Security Risk Assessment (ISRA) has been reviewed and updated. All reasonably foreseeable
threats addressed in the Info
defined in InfoSec Risk Asse
documents for the Informatio

New Threats

The following threats were a

Threat
Name

Updated Threats

The following threats were n

Threat
Name

Removed Threats

The following threats were r

Threat
Name

Information Security Progra

Copyright © 2023

Information Security Program
Annual Report to the Board

Tandem Financial

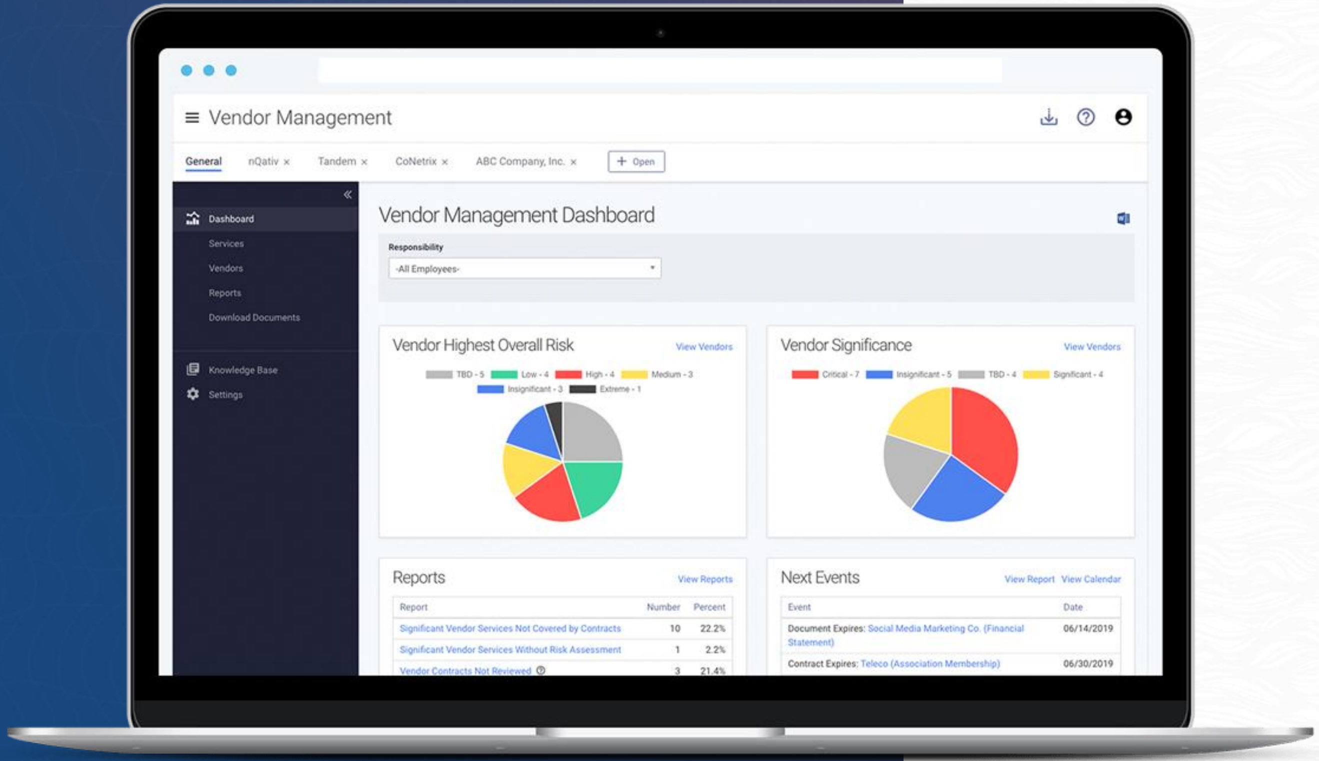
Date: ______________

RESOURCE

Annual Report to the Board Template

Download Now

Tandem



Vendor Management Dashboard

Responsibility: -All Employees-

Report	Number	Percent
Significant Vendor Services Not Covered by Contracts	10	22.2%
Significant Vendor Services Without Risk Assessment	1	2.2%
Vendor Contracts Not Reviewed	3	21.4%

Event	Date
Document Expires: Social Media Marketing Co. (Financial Statement)	06/14/2019
Contract Expires: Teleco (Association Membership)	06/30/2019

BONUS CONTENT

Tandem Product Showcase

SUBMIT YOUR QUESTIONS!

We want to hear from you.

- Ask a question
- Send a chat
- Share a story
- Connect with us

Tandem

Fill out the survey for a chance to win!

THANKS FOR JOINING

The Ins & Outs of Your Annual Report to the Board

Samantha Torrez-Hidalgo,
CSXF
storrez@tandem.app
Linkedin.com/in/samanthatorrez/

Remember to complete the survey!

Tandem