

LEVEL UP

Samantha Torrez-Hidalgo

The Ins & Outs of Your Annual Report to the Board

Risk & Compliance



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



Samantha Torrez-Hidalgo

CSXF

Tandem Software Specialist



3

What are we covering?

HERE'S THE PLAN

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



4



The Report to the Board & You

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

5

Why is this report so important?

THE REPORT TO THE BOARD & YOU

“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.”

[12 CFR Part 208 Appendix D-2 III F](#)



6

The Importance of the Report to the Board

THE REPORT TO THE BOARD & YOU

1

Clear Communication

2

Clear Expectations

3

Discussion of Issues

4

Summary of Your Program



7

Information Security & Your Board

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD



8

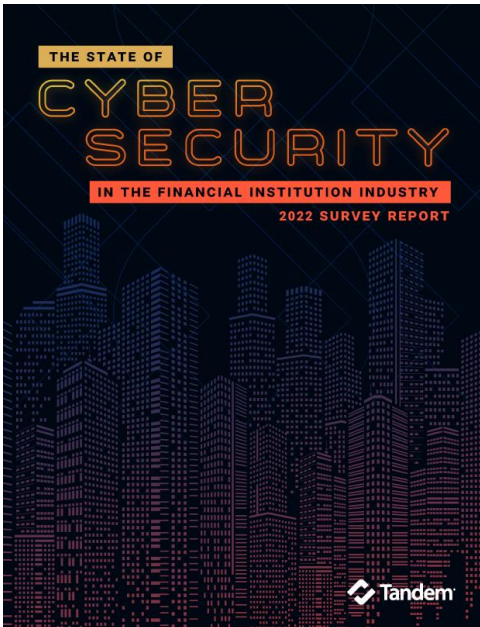
INFORMATION SECURITY & YOUR BOARD



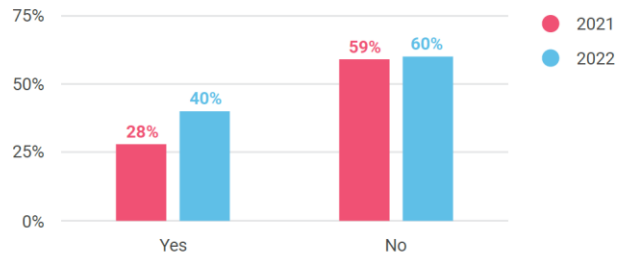
How well do you know your board and their backgrounds?



9



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>



10

INFORMATION SECURITY & YOUR BOARD

How many of you have board members with IT / Cyber experience?



11

Get Everyone on the Same Page

INFORMATION SECURITY & YOUR BOARD

Begin with items they are familiar with, like:

- Overall Status of InfoSec Program
- Designate ISO
- Notable Committees, such as:
 - Security Committee Members
 - Disaster Recovery Team Members
 - Incident Response Team Members



12

What's Important?

INFORMATION SECURITY & YOUR BOARD

**Knowing
Your Board**

**Background
of Your Board**

**Familiarize
Your Board**



13

Risk Assessment

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD



14



15

What to Include

RISK ASSESSMENT



- **Information Security Risk Assessment (ISRA)**
New, Updated, and Removed Threats
- **Asset-Based Risk Assessments (ABRA)**
New or Updated Risk Assessments



16

CIA Ratings & Your Risk Assessments

RISK ASSESSMENT



Confidentiality



Integrity



Availability



17

CIA Ratings & Your Board

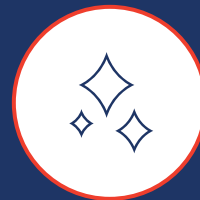
RISK ASSESSMENT



Priority of Assets



Areas of Concern



New Risks



18

What's Important?

RISK ASSESSMENT

**Include
Information
Security Risk
Assessment**

**Include Asset-
Based Risk
Assessments**

**Discuss
CIA Ratings**



Information Security Policies

The Ins & Outs of Your Annual Report to the Board



The Purpose of Policies in your Report

INFORMATION SECURITY POLICIES



"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



21



22

What to Include & Prepare

INFORMATION SECURITY POLICIES

New, Updated, & Removed Policies

1

2

Purpose for Changes

High Level Discussion

3



23

INFORMATION SECURITY POLICIES

Are your policies acting as controls for any risk assessments?



24

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

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



25

What's Important?

INFORMATION SECURITY POLICIES

Policies as Controls

Keep It Simple

Discuss Important Changes



26



Business Continuity Plan

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

27



28

What to Include & Prepare

BUSINESS CONTINUITY PLAN



Business Processes



Preparedness Controls



Important Preparedness Controls

Business Continuity Plan



Alternate Command Center & Alternate Data Center

Customer Communication Plan

Emergency Checklists

Emergency Lighting, Power, & Supplies

Evacuation Procedures

System/Equipment Recovery Plans



What to Include & Prepare

BUSINESS CONTINUITY PLAN



Business Processes



Preparedness Controls



Recent Testing



Upcoming Testing



31

What's Important?

BUSINESS CONTINUITY PLAN



32



Incident Response Plan

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

33



34

Recent Incidents

INCIDENT RESPONSE PLAN

- Facebook (Apr. 2021)
- LinkedIn (Apr. 2021)
- Cash App (Apr. 2022)
- Last Pass (Dec. 2022)
- Twitter (Jul. 2022, Jan. 2023)



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

35

What to Include & Prepare

INCIDENT RESPONSE PLAN

Incidents in the Last Year

1



36

What are “Noteworthy” incidents?

INCIDENT RESPONSE PLAN

- 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



37

What to Include & Prepare

INCIDENT RESPONSE PLAN

Incidents in the Last Year

1

2

Completed Exercises & Tests

Scheduled Exercises & Tests

3



38

Shared Tests Between BCP & IRP



INCIDENT RESPONSE PLAN

Phishing & Malware Problem



Stolen Documents



Flood (Data Center)



39

What's Important?

INCIDENT RESPONSE PLAN

Understanding Incidents

Discussing Recent Incidents

Reviewing Testing Plans & Results



40



Vendor Management

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

41



42

What to Include & Prepare

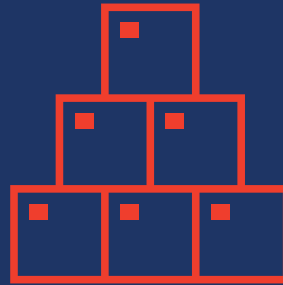
VENDOR MANAGEMENT

Include



New & Renewed Vendor Relationships

Don't Include



All Vendors



43

Vendor Service, Significance, & Risk

VENDOR MANAGEMENT

- Types of Services Renewed / Changed
- Significance of Vendor Relationship
- Risk of Vendor Relationship
- Third-Party Incidents



44

What's Important?

VENDOR MANAGEMENT

**New &
Renewed
Vendor
Relationships**

**Types of
Services
Updated**

**Third Party
Incidents**



45

Security Awareness Training

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD



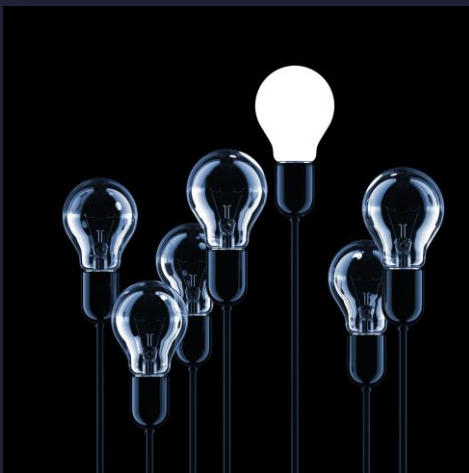
46



47

What type of Training does this include?

SECURITY AWARENESS TRAINING



COURSES

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

INCLUDE

- Date of Training
- Who was Trained
- Percentage Completed



48

What's Important?

SECURITY AWARENESS TRAINING

Variety of Courses

Learning Management System (LMS)

Branch System Testing



49

Assurance & Testing

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD



50



51


About Testing

ASSURANCE & TESTING

Audit	1
Penetration Test	2
Vulnerability Assessment	3
Self-Assessment	4

INCLUDE IN REPORT

- Type of Testing
- Date of Testing
- Status
 - Complete
 - Incomplete



52

Verifying Your Controls

ASSURANCE & TESTING



BCP
Testing



External
Vulnerability
Scan



Password
Audit



Social
Engineering
Audit



53

Why does my board need to know about testing?

ASSURANCE & TESTING



Are there
unresolved issues?



Can they help you
resolve these
issues?



54

What's Important?

ASSURANCE & TESTING

**Discuss Types
of Testing**

**Additional
Methods of
Verification**

**Transparency
about
Unresolved
Issues**



55



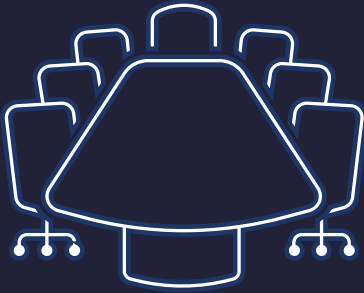
Summary

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD

56

Recap

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



57

The Board, the Report, & You

THE INS & OUTS OF YOUR ANNUAL REPORT TO THE BOARD



GOALS OF THE REPORT

- Showcase Your Work
- Provide Visibility for the Program
 - What's working?
 - What's *not* working?
 - What do you need to be successful?
- Build a Positive Relationship
- Create Progress for the Future



58



RESOURCE

Annual Report to the Board Template

[Download Now](#)




59

LEVEL UP

THANKS FOR JOINING!

The Ins & Outs of Your Annual Report to the Board

Samantha Torrez-Hidalgo
 CSXF, Tandem Software Specialist
 CoNetrix
storrez@tandem.app | [LinkedIn](#)



63