SECOND EDITION

Foundations of an Information Security Program

Tandem®

About the Authors

Alyssa Pugh, CISM, CRISC, Security+
GRC Content Manager
Tandem, LLC
LinkedIn.com/in/AlyssaPugh

Meet Alyssa, an educator, expert, and content creator with a passion for helping people navigate the challenges of governance, risk management, and compliance (GRC). With more than ten years of professional technical and graphic design experience, she's on a mission to inspire others to level up their cybersecurity and third-party risk management practices, one control at a time.

Leticia Saiid, Security+
Chief of Staff | Chief Learning Officer
CoNetrix, LLC
LinkedIn.com/in/LeticiaSaiid

After earning a B.A. and a M.A. in Mathematics, Leticia joined CoNetrix, where she served as the Tandem Support Manager for several years. She built and directed Tandem's first team of support specialists. Leticia now serves as Chief of Staff and Chief Learning Officer where she focuses on corporate strategy, employee development, and training. In her free time, she enjoys mentoring college students, teaching phonics, and solving jigsaw puzzles.

About the Second Edition
Changes to this revision include updates from recent regulatory guidance and the 2024 Tandem Cybersecurity Report. In addition, a new section on cybersecurity Self-Assessments was added and the Vendor Management section was revised. Additional design and stylistic updates were applied to improve readability.

Disclaimer
This resource is for information purposes only. Businesses may use this resource to assist with their information security and compliance practices, but are encouraged to evaluate the risks and coordinate with appropriate legal counsel before acting on ideas from this document.

Contents

Introduction

Information security is about protecting the confidentiality, integrity, and availability of information created, stored, used, transmitted, and disposed of by the organization.

While information security applies to any type of data (physical or electronic), cybersecurity is often thought of as a subset of information security, focused on the protection of the technical systems which protect information.

A compromise of information security could result in serious adverse effects, such as:

- Noncompliance
- Breach of contract
- Service unavailability
- Reputation damage
- Loss of competitive advantage
- Loss of earnings or capital

Because of this, it is important for you to understand the foundational requirements of information security and promote a culture of security at your organization.

This resource exists to help you become more familiar with information security terminology and provide some best practices to help you lay the foundation for your information security program.

DID YOU KNOW?

When confidentiality, integrity, and availability are seen together, they are commonly referred to as the "CIA triad."

Confidentiality is about ensuring systems and data are only accessed by the right people at the right times.

Integrity is about ensuring systems and data are accurate.

Availability is about ensuring systems and data are accessible when they are needed.

Compliance Requirements

While having an information security program can benefit any organization, for financial institutions, it is also required. Here is a brief overview of the law, resulting regulations, and guidance related to having an information security program.

1999

The Gramm-Leach-Bliley Act (GLBA) of 1999 is the law that put the banking agencies into motion to create requirements for the protection of customer information. The specific requirement comes from GLBA Section 501(b).

2001

In response, the Interagency Guidelines Establishing Information Security Standards were published in 2001. These guidelines require financial institutions to develop and implement an information security program.

2002

One year later, the FFIEC published the first IT Examination Handbook, Information Security Booklet. The booklet serves as a guide and has been updated several times to accommodate for changes in technology.

Regulations & Standards

Each of the federal banking agencies has published information security regulations and standards. Here are the regulatory references for each.

- Federal Deposit Insurance Corporation (FDIC)
  12 CFR Part 364, Appendix B
- Federal Reserve Board (FRB)
  12 CFR Part 208, Appendix D-2
- Office of the Comptroller of the Currency (OCC)
  12 CFR Part 30, Appendix B
- National Credit Union Association (NCUA)
  12 CFR Part 748, Appendix A
- Farm Credit Administration (FCA)
  12 CFR Part 609
- Federal Trade Commission (FTC)
  16 CFR Part 314
- Securities and Exchange Commission (SEC)
  17 CFR Part 248

Guidance

The Federal Financial Institutions Examination Council (FFIEC) is made up of six voting members from the FDIC, FRB, OCC, NCUA, CFPB, and SLC.

The FFIEC regularly publishes guidance on information security and technology, with the most popular being the IT Examination Handbook. The handbook includes the following booklets:

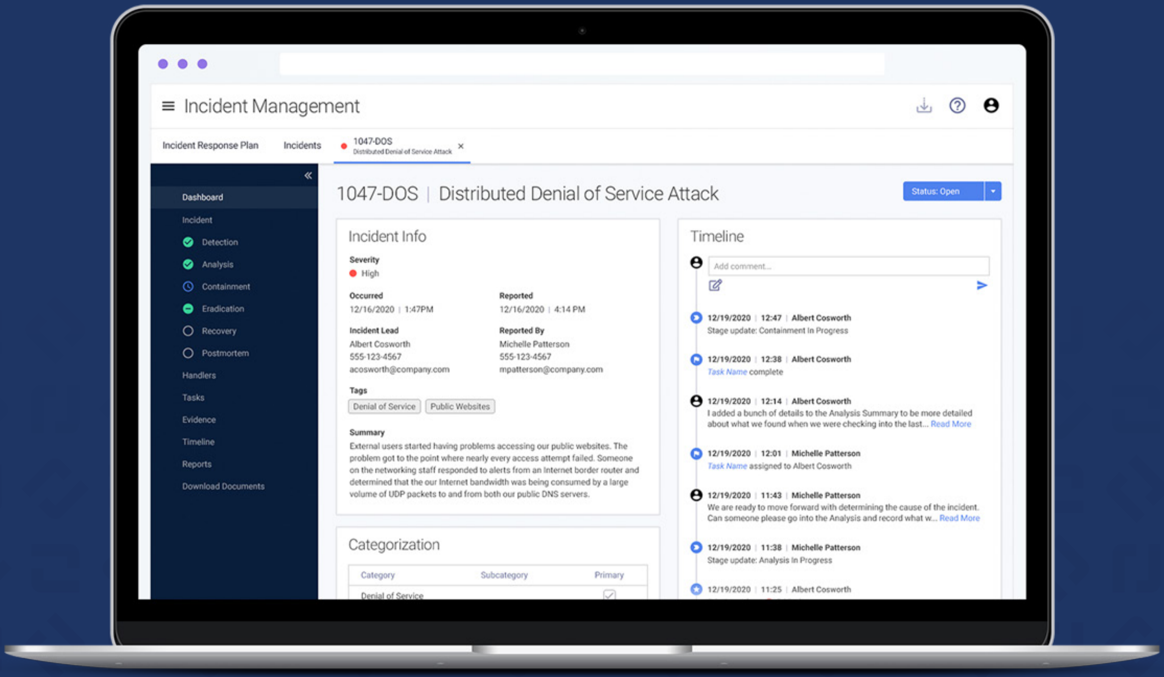
- Architecture, Infrastructure, & Operations
- Audit
- Business Continuity Management
- Development, Acquisition, & Maintenance
- Information Security
- Management
- Outsourcing Technology Services
- Retail Payment Systems
- Supervision of Technology Service Providers
- Wholesale Payment Systems

Several of the federal banking agencies also publish their own standalone guidance. For example:

- FDIC Financial Institution Letters (FILs)
- FRB Supervision & Regulation (SR) Letters
- OCC Bulletins
- NCUA Letters to Credit Unions

Easily Manage Information Security and Regulatory Compliance

Let Tandem carry the burden of new guidance, data tracking, document structure, and report generation. See what you are capable of when using the right tool for the right job.



1047-DOS | Distributed Denial of Service Attack

Incident Info

Severity
● High

Occurred
12/16/2020 | 1:47PM

Reported
12/16/2020 | 4:14 PM

Incident Lead
Albert Cosworth
555-123-4567
acosworth@company.com

Reported By
Michelle Patterson
555-123-4567
mpatterson@company.com

Tags
Denial of Service | Public Websites

Summary
External users started having problems accessing our public websites. The problem got to the point where nearly every access attempt failed. Someone on the networking staff responded to alerts from an Internet border router and determined that the our Internet bandwidth was being consumed by a large volume of UDP packets to and from both our public DNS servers.

Categorization

Category	Subcategory	Primary
Denial of Service		✓

Timeline

12/19/2020 | 12:47 | Albert Cosworth
Stage update: Containment In Progress

12/19/2020 | 12:38 | Albert Cosworth
Task Name complete

12/19/2020 | 12:14 | Albert Cosworth
I added a bunch of details to the Analysis Summary to be more detailed about what we found when we were checking into the last... Read More

12/19/2020 | 12:01 | Michelle Patterson
Task Name assigned to Albert Cosworth

12/19/2020 | 11:43 | Michelle Patterson
We are ready to move forward with determining the cause of the incident. Can someone please go into the Analysis and record what w... Read More

12/19/2020 | 11:38 | Michelle Patterson
Stage update: Analysis In Progress

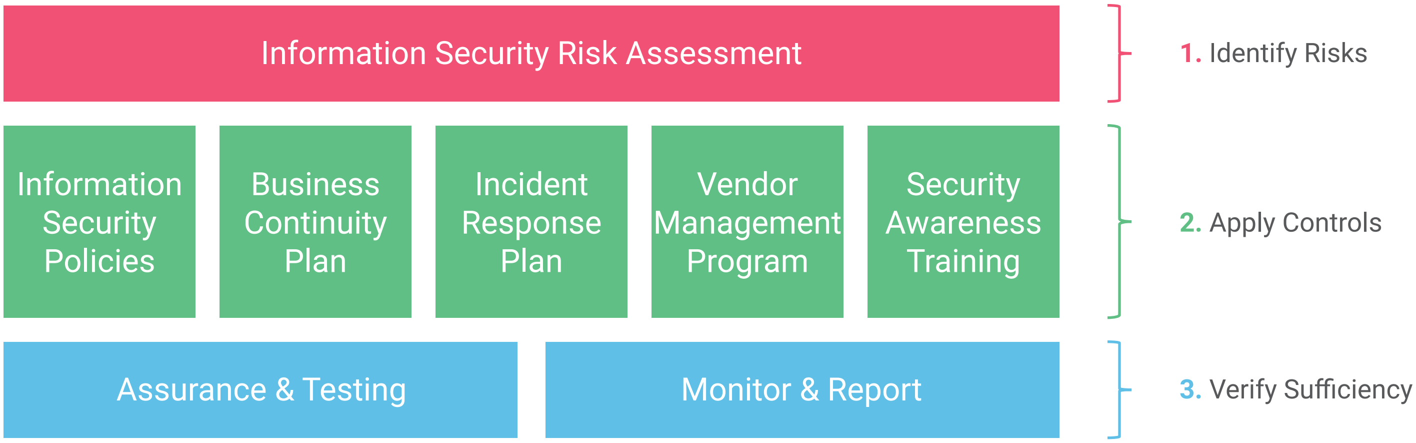
12/19/2020 | 11:25 | Albert Cosworth

Watch a Demo: Tandem.App/ISPDemo

Tandem®

Information Security Program

An information security program is created from individual components which will be discussed in the following sections. Here is an overview of how the program components work together.



Information Security Risk Assessment

1. Identify Risks

Information Security Policies

Business Continuity Plan

Incident Response Plan

Vendor Management Program

Security Awareness Training

2. Apply Controls

Assurance & Testing

Monitor & Report

3. Verify Sufficiency

The Information Security Officer

The role of the Information Security Officer (ISO) is to promote information security, while supporting the organization's overall strategic plans and objectives. According to the FFIEC IT Examination Handbook, Information Security Booklet, an ISO must have six key qualities.

1 Authority

2 Stature

3 Knowledge

4 Background

5 Training

6 Independence

Equipped with these qualities, the ISO is typically expected to:

- Develop, implement, and maintain the information security program.
- Coordinate with staff on information security initiatives, risks, and risk mitigation practices.
- Monitor emerging risks and ensure appropriate mitigating controls are implemented.
- Implement security awareness training for all personnel.
- Participate in information sharing groups.
- Communicate the status of the program with the Board of Directors, senior management, and other stakeholders.

While some organizations may have one individual fill the role of the ISO, others may fill the role with multiple individuals, with a committee, or even with a virtual ISO (vISO). Any of these options are acceptable, as long as the qualities and responsibilities are met.

Did you know? CoNetrix Security offers virtual ISO services and consulting. Learn more at CoNetrix.com/Security/vISO.

Risk Assessment

IDENTIFY RISKS

An information security risk assessment (a.k.a., “GLBA Risk Assessment”) identifies and measures the risk of information security threats. It starts with three steps.

1. **Identify & Classify Data**
   You cannot secure data if you do not know what data you have and how sensitive it is (e.g., public, private, restricted, etc.).

2. **Create an Asset Inventory**
   Identify the systems where the data is stored, processed, or transmitted. Rank the assets based on the data classifications.

3. **Assess the Risks**
   Conduct risk assessments to identify threats which could compromise the assets and data. Determine the likelihood and potential damage of each threat.

If you aren’t sure what kinds of threats to consider in your risk assessment, here are a few examples to get you started.

INTERNAL

- Technical Failures
- Employee Negligence
- Sabotage / Vandalism

EXTERNAL

- Malicious Actors
- Third-Party Failures
- Geopolitical Acts

NATURAL

- Fires
- Floods
- Earthquakes

LEGAL

- Noncompliance
- Data Governance Risks
- Legality Issues

Once you have identified and measured the risks facing your business and your data, you can then begin reviewing the controls your business has in place to mitigate the risk.

INTERAGENCY GUIDELINES

Section III.B

Each institution shall:

ONE
Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

TWO
Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

THREE
Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

INTERAGENCY GUIDELINES

Section III.C.1

Each institution shall design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities.

FUN FACT

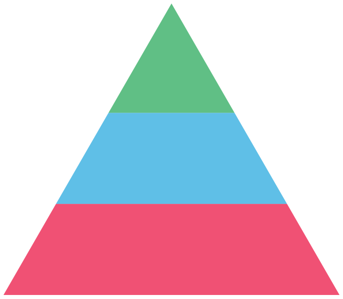
88% of financial institutions have a formal process in place to update policies as the institution's risk profile changes.

SOURCE
Tandem Cybersecurity Peer Analysis

Policies

APPLY CONTROLS

Information security policies, standards, and procedures define the organization's control environment.



Policies set the expectations which serve to guide the business.

Standards say how to implement the policies (i.e., controls).

Procedures communicate steps needed to carry out the standards.

Policies are a communication tool. As such, it can help to structure them in a consistent manner. For example:

1. **Policy Statement**
   A high-level summary of expected activities
2. **Commentary**
   Related context, justification, and/or definitions
3. **Implementation**
   The standards for carrying out the policy statement
4. **Responsibility**
   The personnel responsible for implementing this policy

It is best practice to have policies which define things like:

- Acceptable Use
- Access Controls
- Change Management
- Data Backup
- Encryption
- Email Security
- Incident Management
- IT Asset Management
- Mobile Devices
- Network Monitoring
- Remote Work
- Vendor Management

Business Continuity

APPLY CONTROLS

A business continuity plan (BCP) exists to ensure people, systems, and data would be protected and available in the event of adverse circumstances, like the ones identified in your risk assessment.

While the components of a BCP may vary based on the organization's needs, every BCP should involve the following.

Identify Business Processes
Create a list of the individual functions which are needed to make the business run.

Prioritize by Criticality
Determine how long the business could operate without each process and order based on that.

Determine Recovery Objectives
Create a list of steps which can be used to restore each process to normal operation.

Create Emergency Checklists
Plan for what your business' first steps will be whenever a business disruption occurs.

Perform Exercises & Tests
Practice your BCP to determine if it would be effective in an actual emergency.

It is best practice to make sure your plan defines things like:

RPO (Recovery Point Objectives)
The maximum period in which data can be lost without impacting the recovery of operations.

RTO (Recovery Time Objectives)
The planned recovery time for a process or system which should occur before reaching the MTD.

MTD (Maximum Tolerable Downtime)
The total amount of downtime which can occur without causing significant harm to the business.

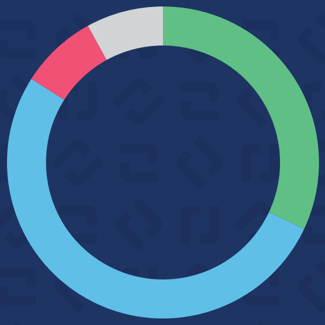
INTERAGENCY GUIDELINES

Section III.C.1.h

Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazard, such as fire and water damage or technological failures.

FUN FACT

84% of financial institutions say BCP exercises and tests are very or somewhat useful in improving the institution's security posture.



SOURCE
2024 Tandem Cybersecurity Report

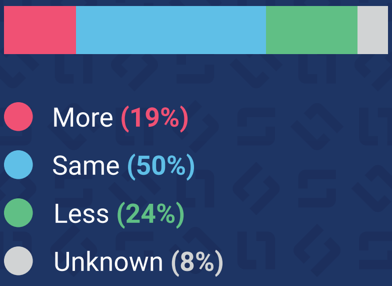
INTERAGENCY GUIDELINES

Section III.C.1.g

Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

DID YOU KNOW?

More than two-thirds of financial institutions experienced the same or a greater number of incidents than they did in the previous year.

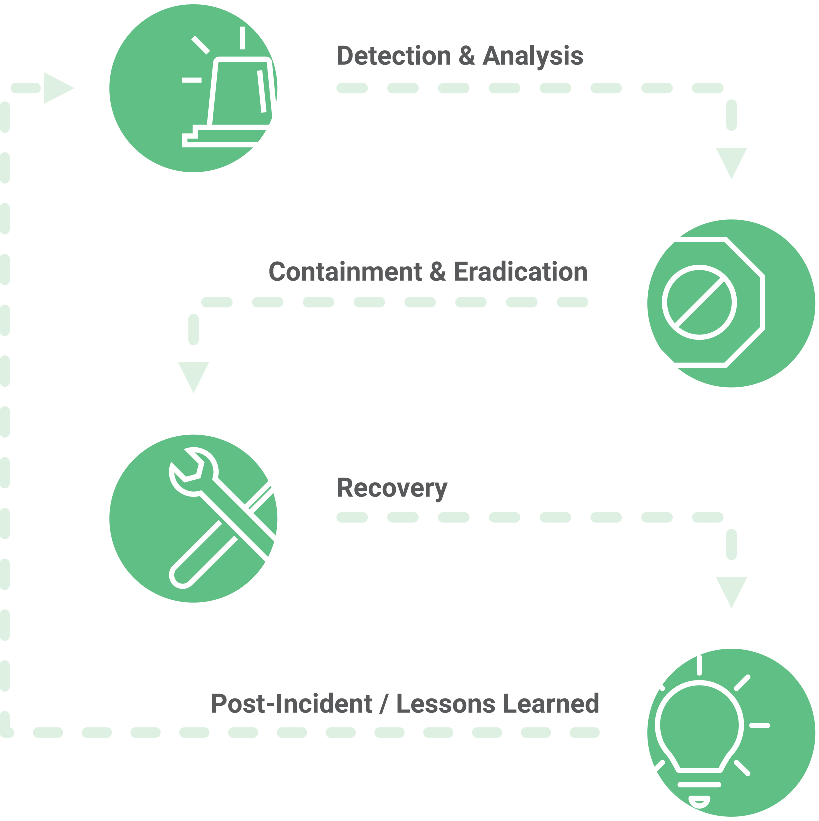


SOURCE
2024 Tandem Cybersecurity Report

Incident Response

APPLY CONTROLS

An incident is an event which compromises the confidentiality, integrity, or availability of information or an information system. In today's day and age, having a plan to manage incidents is a "must have" for any organization. An effective incident response plan covers these phases.



Detection & Analysis

Containment & Eradication

Recovery

Post-Incident / Lessons Learned

Additional components of an incident response plan include:

1. A definition of who does what during an incident
2. A plan to assess the nature and severity
3. Contact information and communication templates
4. Instructions for how to correctly handle evidence
5. Plans for managing third-party incidents
6. A formal incident tracking process and system

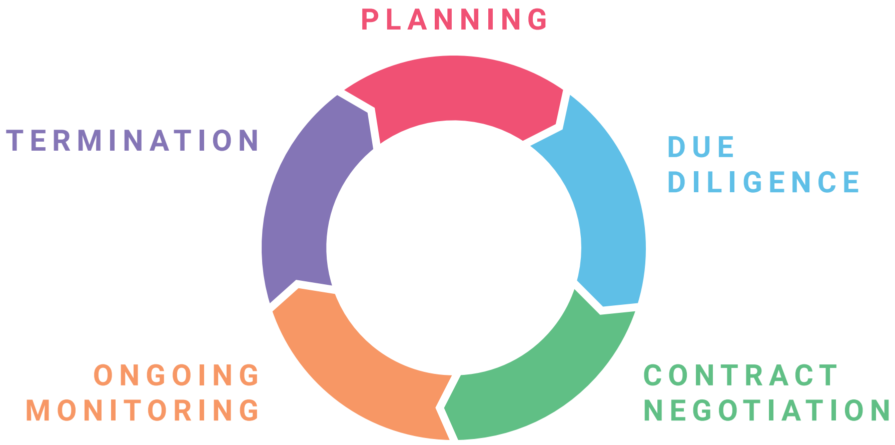
An incident response plan is not intended to be an exhaustive list of every action to be performed when an incident happens. Instead, it exists to give your team the resources they need to minimize the impact of an incident on the business.

Vendor Management

APPLY CONTROLS

Vendor management exists to oversee the organization's relationships with third-party service providers. As vendors operate as an extension of your business, it is important to ensure they secure information in the same way that you would.

A vendor management program is based on the following lifecycle, and helps protect the company and its customers from potential threats.



Learn more about this topic in our Vendor Management Workbook.
Get your copy now: Tandem.App/Vendor-Management-Workbook

GUIDANCE

"Credit unions should complete a risk assessment prior to engaging in a third party relationship to assess what internal changes, if any, will be required to safely and soundly participate. Risk assessments are a dynamic process, rather than a static process, and should be an on-going part of a broader risk management strategy."

NCUA Supervisory Letter 07-01

"[P]eriodically conducting risk assessments for each third-party relationship supports a banking organization's determination of whether risks have changed over time and to update risk management practices accordingly."

Interagency Guidance on Third-Party Relationships: Risk Management

Risk Assessment

Governance & Structure

A vendor management

Responsibility of a ven can also leave a lot of

As a vendor manager, outsourced relationshi choose, expectations

BY THE NUME

We asked more than 3 was structured. Here's

- Centralized: Mana
- Centralized: Mana
- Centralized: Mana
- Decentralized: Ma
- Centralized: Mana

SOURCE
Tandem Survey, August 202

Vendors vs. Third Parties

There are several terms often used inte business arrangement with an externa using the terms as follows.

Third Party
Any business arrangement between a another entity, by contract or otherwise

Vendor
A subset of a third party, including enti with whom the business has a contrac commerce.

Third-Party Service Provider
A subset of vendors who provide outsc services to the business.

While it is a best practice to have an in third-party relationships, the term "ven the relationships which need heightene activities they perform.

For example, here are some third-party would likely **not** need to manage as ve

- Regulators
- Emergency Services
- Law Enforcement

That said, here are some examples of vendor management program.

- Outsourced Services
- Consultants
- Referral Arrangements

6

Tandem

Vendor Management Workbook

INTERAGENCY GUIDELINES

Section III.D

Each institution shall:

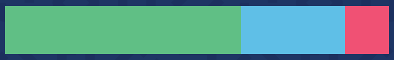
ONE
Exercise appropriate due diligence in selecting its service providers.

TWO
Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines.

THREE
Where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their obligations. As part of this monitoring, an institution should review audits, summaries of test results, or other equivalent evaluations of its service providers.

FUN FACT

Using the vendor management program as a decision making tool is becoming a more common practice.



● It is a decision driver (59%)

● It is a guideline (26%)

● It is for compliance (11%)

SOURCE
2024 Tandem Cybersecurity Report

Training

APPLY CONTROLS

Training promotes awareness of security topics and ensures all team members know their roles in protecting information. Some common security awareness training topics include:

1. **Acceptable Use**
   How technology resources are allowed to be used
2. **Endpoint Security**
   Physical and technical security for workstations
3. **Strong Authentication**
   Complex passwords and multi-factor authentication
4. **Social Engineering**
   Phishing, vishing, smishing, and impersonation
5. **Unauthorized Disclosure Methods**
   Removable media, email, and social media
6. **Incident Management**
   Preventing, detecting, and responding to incidents

FREQUENCY

Employees should receive security awareness training at least annually and more often, as needed. Some factors which could result in increased training need include:

- Current events
- Job functions
- Prior training results

METHODS

Training can come in a variety of flavors, including:

- In person
- Online courses
- Video recordings
- Policy documents
- Phishing campaigns
- Educational emails

Whatever frequency and methods you choose, the key to having an effective training program is finding what works best for your team.

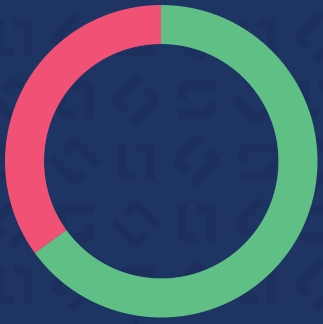
INTERAGENCY GUIDELINES

Section III.C.2

Each institution shall [...] train staff to implement the institution’s information security program.

FUN FACT

64% of financial institutions provide two to five hours of security awareness training for employees each year.



SOURCE
2024 Tandem Cybersecurity Report

Assurance & Testing

VERIFY SUFFICIENCY

Assurance and testing is about being able to monitor and evaluate the information security program's adequacy and effectiveness. Some assurance and testing methods include:

Audits which review the program and compare results with a set of industry standards, guidelines, and best practices.

Self-assessments which identify controls, benchmark maturity, and help develop a growth plan. Learn more on the next page.

Penetration tests which subject systems to real-world attacks to identify flaws in processes and controls.

Vulnerability assessments which scan and identify weaknesses, like unpatched systems, weak credentials, or misconfigurations.

The best assurance and testing program is one that is implemented in layers to ensure adequate:

- Coverage
- Frequency
- Depth
- Independence

When a deficiency is identified through the assurance and testing process, it is often referred as a "finding." Findings can be prioritized by risk and should be addressed in a timely manner to ensure the business remains secure.

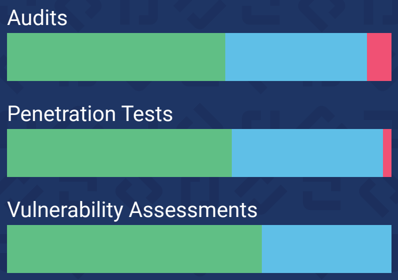
INTERAGENCY GUIDELINES

Section III.C.3

Each institution shall [...] regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

FUN FACT

Most financial institutions find assurance and testing methods very or somewhat useful in improving the institution's security posture.

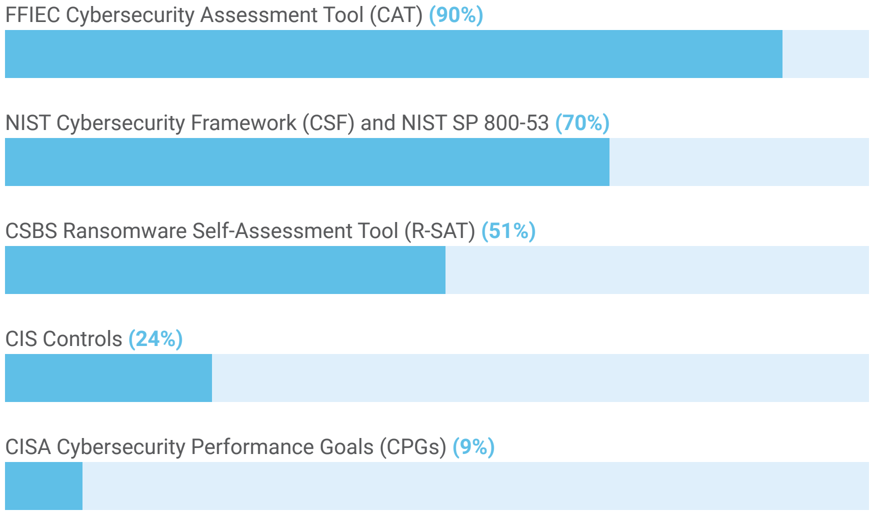


SOURCE
2024 Tandem Cybersecurity Report

Self-Assessments

A self-assessment is a form of assurance and testing, designed to identify and evaluate the cybersecurity controls helping you manage risk. Most self-assessments are based on a cybersecurity framework.

According to the 2024 Tandem Cybersecurity Report, the most popular cybersecurity frameworks in community financial institutions are:



SOURCE
2024 Tandem Cybersecurity Report

While these numbers will likely shift in coming years (e.g., due to the CAT sunset, the release of financial services sector CPGs, etc.), we expect financial institutions will continue to implement and find value from framework assessments.

ASSESSMENT BENEFITS

Performing a framework assessment offers several benefits.

1 **Current vs. Desired State Comparison**
It helps you know what controls you currently have implemented and if there are any common control gaps or weaknesses.

2 **Easy-to-Understand Reporting**
It helps you report control status to key stakeholders (e.g., the Board, management, examiners, auditors, service providers, etc.).

3 **Peer Analysis**
Using a software tool, like Tandem Cybersecurity, can show how your assessment results measure up to your peers. (Optionally and anonymously, of course.)

REGULATORY GUIDANCE

FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness

August 28, 2019

"The Federal Financial Institutions Examination Council (FFIEC) members today emphasized the benefits of using a standardized approach to assess and improve cybersecurity preparedness.

The members note that firms adopting a standardized approach are better able to track their progress over time, and share information and best practices with other financial institutions and with regulators.

Institutions may choose from a variety of standardized tools aligned with industry standards and best practices to assess their cybersecurity preparedness. [...]

FFIEC members welcome collaborative approaches to advance and support cyber preparedness and enhance the efficiency and effectiveness of the supervisory process. While the FFIEC does not endorse any particular tool, these standardized tools support institutions in their self-assessment activities."

Monitor & Report

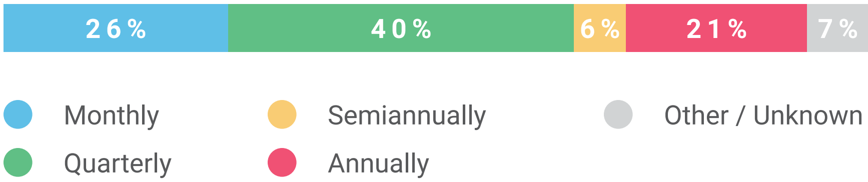
VERIFY SUFFICIENCY

An information security program is not a once-and-done kind of thing. It is a living document which needs to be updated on a regular basis to address changes in things like:

- Technology
- Sensitivity of information
- Internal and external threats
- Business goals and arrangements

The organization's Board of Directors is ultimately responsible for the information security program, including its successes and failures. As such, it is required to be reported to the Board at least annually and more often, as circumstances require.

Most financial institutions report to the Board more often than annually.



SOURCE
2024 Tandem Cybersecurity Report

The Board of Directors is expected to provide a credible challenge to the program. This process includes:

1 Being actively engaged.

2 Asking thoughtful questions.

3 Exercising independent judgment.

The Board of Directors is also expected to formally approve the written information security program and each of the program's components.

INTERAGENCY GUIDELINES

Sections III.E & F

MONITOR
Each institution shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes.

REPORT
Each institution 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 [...] should discuss material matters related to its program.

DID YOU KNOW?

Financial institutions who report to the Board on a more frequent basis experience higher levels of confidence in the Board's understanding of cybersecurity issues facing the business.

The ISO Annual Schedule

Maintaining a great information security program is not something that happens overnight. It takes time, effort, and lots of planning. So, now that we know what goes into an information security program, let's put it onto a schedule.

Try it yourself! Download a fillable scheduling tool at Tandem.App/ISO-Schedule-Tool.

ISO Annual Schedule: Quick Start (Sample)

If you are new to the ISO role, we recommend keeping it simple. The first and most important thing you need to do is **get to know your program**. Plan to spend a month looking at each component. Be sure to leave a month open for your IT audit and/or exam. Be aware of any months that could be busy with special projects and build in some flex time. Here's an example of what that could look like.

JAN	Security Awareness Training
FEB	Business Continuity Plan
MAR	Annual IT Exam
APR	Risk Assessments
MAY	Vendor Management
JUN	Family Vacation & Special Projects
JUL	Incident Response
AUG	Report to the Board
SEP	Assurance & Testing (User Access Reviews)
OCT	Policies
NOV	Annual IT Audit
DEC	Holiday Activities

DID YOU KNOW?

When asked about circumstances negatively impacting the success of the institution's cybersecurity strategy, the most selected answer was a lack of time. While it might be easy to overlook, this means scheduling and planning is a critical part of an ISO's job.

SOURCE
2024 Tandem Cybersecurity Report

Lack of time (84%)

Lack of integration (51%)

Lack of personnel (42%)

Lack of budget (39%)

ISO Annual Schedule: Full Schedule (Sample)

If you're ready to take your ISO schedule to the next level, we recommend following a three-step process to 1) determine the frequency of your activities, 2) set goals on a calendar, and 3) track (and learn from!) your progress.

STEP 1: DETERMINE FREQUENCY & TIME NEEDED

For each activity, first identify how many times per year the activity needs to be done (Frequency). Then, identify how long you will need to complete the activity (Weeks Needed). Use these numbers to put your activities on a calendar. Having these estimates allows you to add up the total number of weeks of work to determine what reasonably fits in a calendar year. Here's an example.

ACTIVITY	FREQUENCY (PER YEAR)	WEEKS (PER ACTIVITY)	TOTAL TIME (WEEKS)
Review Risk Assessments	1	3	3
Review Policies	1	3	3
Review Business Continuity Plan (BCP)	1	3	3
Review Incident Response Plan (IRP)	1	2	2
Review Vendor Management Program	1	2	2
Review Cybersecurity Self-Assessment(s)	1	1	1
Perform BCP Exercise / Test	1	1	1
Perform IRP Exercise / Test	1	1	1
Prepare for & Respond to IT Audit	1	2	2
Prepare for & Respond to Penetration Test	1	1	1
Prepare for & Respond to IT Examination	1	2	2
Administer Training (SAT & AUP)	1	1	1
Review User Access to Critical Applications	1	1	1
Create & Present Report to the Board	4	1	4
Coordinate Special Projects	2	2	4
Attend Conferences / Professional Development	2	1	2
Vacation & Celebrate Holidays	6	1	6
Send & Review Simulated Phishing Exercises	12	0.2	2.4
Perform Vendor Oversight	12	0.2	2.4
Run Vulnerability Scans	12	0.2	2.4
			UNBOOKED WEEKS
			1.8

TIP: Keep this number above zero, otherwise you will overbook yourself. Overbooking can lead to stress and burnout from unmet and unrealistic expectations.

STEP 2: SCHEDULE ACTIVITIES ON A CALENDAR

Using your list from Step 1, distribute your activities onto an annual calendar to set yourself up for success (see the next page for an example). You can always move activities around as things change, but you can't make more weeks in a year.

STEP 3: IDENTIFY GOALS

For each activity, include what "done" looks like. For example, what does it mean to review your risk assessments? Maybe "done" is to read each one and ensure all important assets are included. This may not fit on your one-page calendar, but it could be written out as part of your reminders.

4 Tips for Building a Successful Schedule

There are a few things most people forget when building a schedule for the first time. Here's a starter list to help you skip over these novice mistakes.

EXPECT THE UNEXPECTED

Do not overbook your month.
There is a finite amount of time and a guarantee of surprises. Life happens and things can throw off your goals and plans. That's expected! Build margin into your schedule. Consider the year to be 48 weeks instead of 52. Know that "needing a week" doesn't mean 40 straight hours, but more like 20-30. Account for the time it takes to start and stop, put out fires, and just be a human.

PLAN FOR AUDITS & EXAMS

Plan now for the unexpectedly full days later.
You may not be leading your audits and exams, but you will be replying to request lists and meetings galore when they are happening. Plan for this disruption by dedicating an activity slot for each audit or exam. Consider what other kinds of "busy seasons" you have in your year that are going to take up space.

USE YOUR TOOLS

Your mind is for having ideas, not holding them.
Don't use your brain power to remember your projects and schedule. Instead, use your tools! Create a recurring calendar reminder for the beginning of each month that includes the four activities you will do that month and your goal of "done."

CELEBRATE MILESTONES

You are doing important and remarkable things.
Take time to mark them! When you complete your activities across a month, a quarter, a special project, or something similar, throw yourself a party! This can look like a gold star on a chart, going out for coffee with a coworker, having lunch with your team, or finding someone to high-five. When we reward ourselves for our work, our work becomes more rewarding to do.

TRY IT YOURSELF!

Tandem.App/ISO-Schedule-Tool

ISO Annual Schedule: Four Week View (Sample)

JANUARY	FEBRUARY	MARCH
Administer SAT & AUP Enroll employees. Require completion by 01/31.	**Review BCP** Review systems/equipment and software. Check for interdependencies.	**IT Exam** Respond to request list items.
Report to the Board Prepare for and present quarterly report.	**Review BCP** Coordinate with department heads. Review emergency locations and checklists.	**IT Exam** Be available for on-site visit and meetings.
Monthly Activities • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Test BCP** Schedule tabletop exercise.	**Monthly Activities & Personal Time** Spring Break with Family.
Review BCP Review business processes. Update Business Impact Analysis (BIA).	**Monthly Activities** • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Special Projects** Security team meeting. Respond to findings. End of quarter report.

APRIL	MAY	JUNE
Monthly Activities & Attend Conferences Tandem KEYS Conference	**Report to the Board** Prepare for and present quarterly report.	**Personal Time** Family vacation.
Risk Assessments Review critical assets.	**Vendor Management** Review policy and program. Confirm all third parties are included in the program.	**Special Projects** Research AI / emerging technology for business.
Risk Assessments Review threats. Address current risks.	**Vendor Management** Include recent guidance best practices.	**Monthly Activities** • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans
Risk Assessments Review mitigating controls.	**Monthly Activities** • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Special Projects** Security team meeting. End of quarter report.

JULY	AUGUST	SEPTEMBER
Report to the Board Prepare for and present quarterly report.	**Test IRP** Schedule tabletop exercise.	**Personal Time** Life Event (e.g., childbirth, weddings, anniversary trips, care for parents, etc.).
Incident Response Plan Review policy and program.	**Cybersecurity Assessment** Review cybersecurity framework assessment(s).	**Assurance & Testing** Penetration Test
Incident Response Plan Confirm all incidents were adequately documented.	**Attend Conferences** ISACA GRC Conference	**Monthly Activities & Special Projects** Prep for Cybersecurity Awareness Month (Oct.)
Monthly Activities • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Monthly Activities** • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Special Projects** Security team meeting. Respond to findings. End of quarter reporting.

OCTOBER	NOVEMBER	DECEMBER
Monthly Activities • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans	**Report to the Board** Prepare for and present quarterly report.	**Monthly Activities** • Phishing Exercises • Vendor Due Diligence • Vulnerability Scans
Policies Read through policies and confirm accuracy.	**IT Audit** Respond to request list items.	**Assurance & Testing** Perform user access review.
Policies Review meeting minutes from committees/teams.	**IT Audit** Be available for on-site visit and meetings.	**Special Projects** Security team meeting. Respond to findings. End of quarter reporting.
Policies Update revision dates. Create follow-up tasks.	**Monthly Activities & Personal Time** Holidays with Family.	**Personal Time** Holidays with Family.

Further Reading

FFIEC IT EXAM HANDBOOK

- Architecture, Infrastructure, & Operations
- Audit
- Business Continuity Management
- Development, Acquisition, & Maintenance
- Information Security
- Management
- Outsourcing Technology Services
- Retail Payment Systems
- Supervision of Technology Service Providers
- Wholesale Payment Systems

EXAMINATION PROGRAMS

- FDIC & FRB Information Technology Risk Examination (InTREx) Program
- OCC Cybersecurity Supervision Work Program (CSW)
- NCUA Information Security Examination (ISE)

GOVERNMENT FRAMEWORKS

- FFIEC Cybersecurity Assessment Tool (CAT)
- NIST Cybersecurity Framework (CSF)
- CISA Cybersecurity Performance Goals (CPG)
- CSBS Ransomware Self-Assessment Tool (R-SAT)

REGULATIONS & GUIDANCE

- NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
- FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness
- Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers (FDIC, FRB, & OCC)
- Cyber Incident Notification Requirements for Federally Insured Credit Unions (NCUA)
- Proposed Rule: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (CISA)
- Interagency Guidance on Third-Party Relationships: Risk Management (FDIC, FRB, & OCC)
- Evaluating Third-Party Relationships (NCUA)

TANDEM BLOG

Risk Assessment

- What is a GLBA Risk Assessment?
- What is an IT Audit Risk Assessment?
- 3 Reasons for a Remote Work Risk Assessment

Policies

- Key Sections of an Information Security Policy
- 6 Tips for Writing an Information Security Policy
- Policies vs. Standards vs. Controls vs. Procedures
- How to Conduct a Policy Review Meeting

Business Continuity

- What is Business Continuity Planning?
- Difference Between RTO, RPO, and MTD
- BCP Exercises & Tests: Frequently Asked Questions

Incident Response

- Best Practices to Prepare for Security Incidents
- 6 Phases of an Effective Incident Response Plan
- Incident Response Plan Communication Guidelines
- 7 Steps for a Successful Incident Response Team

Vendor Management

- What is Vendor Management?
- How to Perform a Vendor Risk Assessment
- A More Accurate Way to Collect Due Diligence
- The Vendor Manager's Guide to Subcontractors

Training

- Security Incident Management Training
- 5 Ways to Improve Your Phishing Test Results
- 12 Simulated Phishing Templates to Cover Your Year
- Phishing Spotlight: Tax Season Scams

Assurance & Testing

- How to Respond to an Audit or Exam Finding
- What Framework Do I Replace the FFIEC CAT With?

Information Security Officer

- Understanding the Role of an ISO
- 6 Key Qualities of ISOs
- What to Do if Your ISO Leaves
- 4 Things to Consider Before Hiring a vISO

The State of Cybersecurity Report

Each year, a panel of Tandem security and compliance experts analyze survey data from hundreds of security professionals to understand how financial institutions are managing cybersecurity.

Vendor Management
Observation: Incidents Caused by Third-Party Vendors Increased
Diving Further
INSTITUTION PERSPECTIVE ON THE VENDOR
Commentary
Training
Observation: Institutions Feel More
CONFIDENCE IN CYBERSECURITY TRAINING
Diving Further
TRAINING HOURS COMPARED WITH TRAINING
Board Oversight
Observation: Majority Update the Bo
FREQUENCY OF BOARD UPDATES
Diving Further
REPORTING FREQUENCY BY ASSET SIZE
Commentary
2024
CYBER SECURITY REPORT
FOR THE FINANCIAL INSTITUTION INDUSTRY
Tandem

Download The State of Cybersecurity Report by Tandem to see more insights like the ones in this document, and learn more about how your organization's practices compare with your peers.

Get Your Copy: Tandem.App/Report

About Tandem

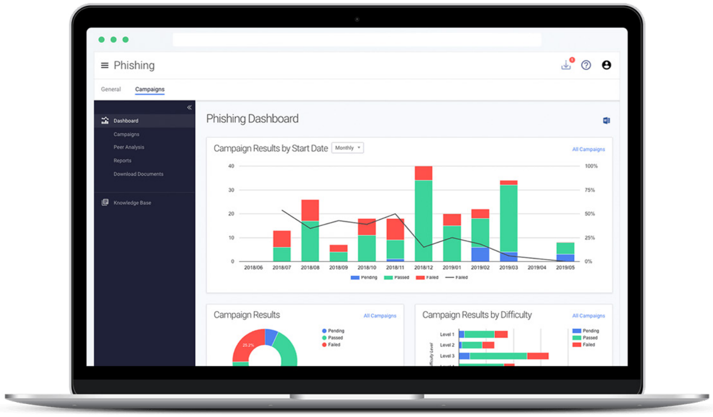
WHO WE ARE

Tandem, LLC is one of four companies owned by CoNetrix, LLC. Tandem grew out of the confidence that there is a solution for every problem. A problem our clients experienced was the burden of information security compliance.

First, we supported our clients by helping them maintain their documents, but it didn't take long to decide that a software solution could help more people, faster. In 2007, we began developing the do-it-yourself compliance application for information security, now known as Tandem.

We named our product Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs. We bring software built by information security experts to help you create, organize, and manage your information security program.

We believe you have what it takes to manage information security and regulatory compliance. With the right tool, you can do it fast. Learn more about how Tandem can help you at Tandem.App.



OUR PRODUCTS

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

Tandem®

info@tandem.app
844-698-9800