Foundations of an Information Security Program

Table of 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.

Regulations & Guidance

While having an information security program can benefit any organization, for financial institutions, it is also a requirement. 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

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

Interagency Guidelines

The Interagency Guidelines were codified by each of the federal banking agencies. Here is the regulatory reference 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

The Handbook

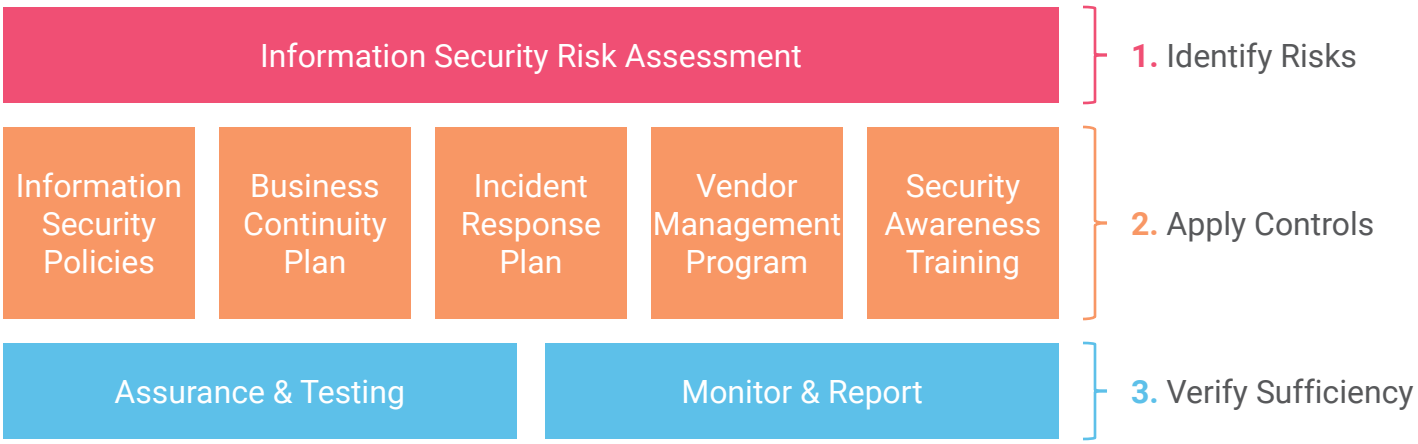
The Federal Financial Institutions Examination Council (FFIEC) is made up of representation from each of the federal banking agencies.

The FFIEC's IT Examination Handbook is the most well-known guidance they have published and includes the following booklets:

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

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.



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 regarding 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 information security program with the Board of Directors, senior management, and business unit managers.

While some organizations may have one individual fill the role of the ISO, others may fill the role with multiple individuals or with a committee. FFIEC guidance makes it clear any of these options are acceptable, as long as the qualities and responsibilities are met.

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.

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.).

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

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.

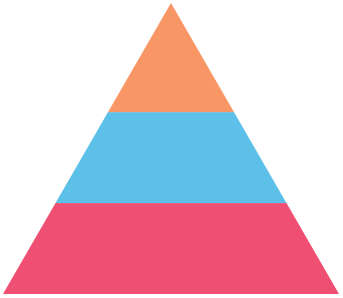
TWO
Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

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

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 the 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

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

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

SOURCE
Tandem Cybersecurity Peer Analysis

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.

Here are a few key BCP acronyms you should know.

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

RTO (Recovery Time Objective)
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

98% of financial institutions say BCP exercises and tests are very or somewhat useful in improving the institution's security posture.

SOURCE
Tandem Survey 2022

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.

Per the National Institute of Standards and Technology (NIST), a good incident response plan has six phases.

Additional components of an incident response plan include:

1. **Roles & Responsibilities**
   A definition of who does what during an incident
2. **Classification Strategies**
   A plan to assess an incident's nature and severity
3. **Communication Guidelines**
   Contact information and communication templates
4. **Evidence & Forensics Procedures**
   Instructions for how to correctly handle evidence
5. **Third-Party Incident Handling Processes**
   Plans for managing incidents at a third party
6. **Incident Tracking System**
   A formal way to track the response process

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.

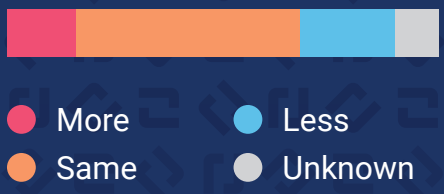
INTERAGENCY GUIDELINES

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 in 2022 than in previous years.



SOURCE
Tandem Survey 2022

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 process.

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.

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

METHODS

Training can take a variety of forms, including:

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

The key is finding which training methods work best for your team.

FREQUENCY

Employees should receive security awareness training **at least annually** and more often, as need arises.

Some factors which could result in increased training need include:

- Current events
- Job functions
- Prior training results

INTERAGENCY GUIDELINES

Section III.C.2

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

FUN FACT

65% of financial institutions provide two to five hours of security awareness training for employees each year.

SOURCE
Tandem Survey 2022

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 and guidelines.

Self-assessments which benchmark control maturity and help develop a growth plan.

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, misconfigurations, or weak credentials.

The best assurance and testing program 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.

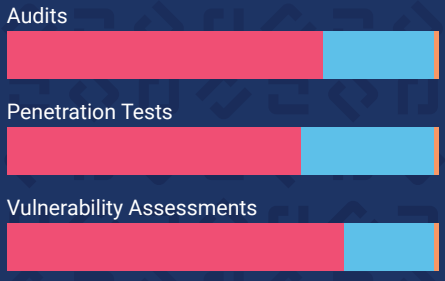
INTERAGENCY GUIDELINES

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
Tandem Survey 2022

Monitor & Report

VERIFY SUFFICIENCY

An information security program is not a once-and-done kind of thing. It is a living document which needs 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.

- Annually
- Twice a Year
- Quarterly
- Every Other Month
- Monthly
- Other / I Don't Know

Source: Tandem Survey 2022

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 judgement.

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.

SOURCE
Tandem Survey 2022

Further Reading

RISK ASSESSMENT

Tandem Blog
What is a GLBA Risk Assessment?
Reasons to Conduct a Remote Work Assessment

Information Security Booklet
II.A Risk Identification
II.C.5 Inventory and Classification of Assets

Architecture, Infrastructure, & Operations Booklet
III.A Data Governance and Data Management
III.B IT Asset Management

POLICIES

Information Security Booklet
II.C.1 Policies, Standards, and Procedures
II.C.3 Control Types

Architecture, Infrastructure, & Operations Booklet
II.C Policies, Standards, and Procedures

BUSINESS CONTINUITY

Tandem Blog
What is Business Continuity Planning?
Difference Between RPO, RTO, and MTD

Information Security Booklet
II.C.21 Business Continuity Considerations

Architecture, Infrastructure, & Operations Booklet
III.F Resilience
V.D Environmental Controls
VI.B.4 Backup and Replication Processes

Business Continuity Management Booklet

INCIDENT RESPONSE

Tandem Blog
Best Practices to Prepare for Security Incidents
6 Phases of an Effective Incident Response Plan

Information Security Booklet
III.C Incident Identification and Assessment
III.D Incident Response

Architecture, Infrastructure, & Operations Booklet
VI.C.4 Event, Incident, and Problem Management

Business Continuity Management Booklet
V.F.1 Incident Response

NIST Computer Security Incident Handling Guide

VENDOR MANAGEMENT

Tandem Blog
What is Vendor Management?
How to Perform a Vendor Risk Assessment
Review Your Vendor's SOC Report in 15 Minutes
A More Accurate Way to Collect Due Diligence

Information Security Booklet
II.C.20 Oversight of Third-Party Service Providers

Architecture, Infrastructure, & Operations Booklet
III.E Oversight of Third-Party Service Providers

Business Continuity Management Booklet
IV.A.5 Third-Party Service Providers

Outsourcing Technology Services Booklet

Agency Guidance
- FDIC FIL-44-2008
- FRB SR 13-19 / CA 13-21
- OCC Bulletin 2013-29
- NCUA SL 07-01

TRAINING

Tandem Blog
Phishing Spotlight: Tax Season Scams
Phishing Spotlight: COVID-19 SBA Scam

Information Security Booklet
II.C.7(e) Training

Business Continuity Management Booklet
VI Training

ASSURANCE & TESTING

Information Security Booklet
IV.A Assurance and Testing

Audit Booklet

MONITOR & REPORT

Information Security Booklet
I Governance of the Information Security Program
II.D Risk Monitoring and Reporting
III.B Threat Monitoring
IV.A.4 Assurance Reporting

Architecture, Infrastructure, & Operations Booklet
VI.D Ongoing Monitoring and Evaluation

Business Continuity Management Booklet
IX Board Reporting

Management Booklet

INFORMATION SECURITY OFFICER

Tandem Blog
Understanding the Role of an ISO
6 Key Qualities of ISOs
What to Do if Your ISO Leaves

Information Security Booklet
I.B Responsibility and Accountability

Management Booklet
I.A.2(c) Chief Information Security Officer

TANDEM 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.

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

Tandem.App/State-of-Cybersecurity-Report

About the Author

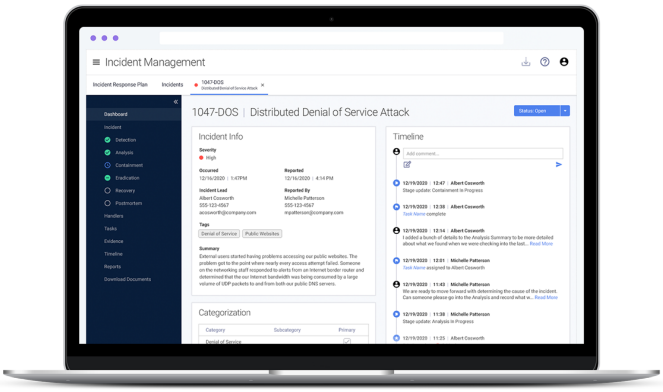
WHO WE ARE

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

Copyright © 2022
Tandem, LLC
info@tandem.app
844-698-9800