

WELCOME TO

# Maintaining Compliance with Freddie Mac's New Information Security Requirements

---

Alyssa Pugh, CISM, Security+  
GRC Content Manager  
Tandem, LLC

# 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.

# SESSION INFO



## AUDIO

If you cannot hear sound now, adjust or change your audio device.



## VIDEO

If you cannot see the presenter's face, let us know in the chat.



## QUESTIONS

Ask questions anytime through the GoToWebinar "Questions" panel.



## RESOURCES

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

-  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

## ABOUT THE PRESENTER



**Alyssa Pugh**  
GRC Content Manager

As a millennial, Alyssa grew up with technology at her fingertips. She has more than ten years of professional technical and information security experience. She currently serves as the GRC Content Manager for Tandem, where she participates in the development of cybersecurity content and educational resources. In addition to her passion for technology, Alyssa is also a wife, graphic designer, and video game enthusiast.

[LinkedIn.com/in/AlyssaPugh](https://www.linkedin.com/in/AlyssaPugh)

# Agenda

---

- About Freddie Mac
- New Requirements
- Notable Updates
- What Can You Do?
- Tandem Bonus Content



1302.2

## Information security

Effective 07/03/2023

### (a) Relevant terms

Seller/Service providers should be familiar with the following terms as they relate to information security requirements:

- **Authentication:** The process in which a system verifies the identity of an individual, usually based on some form of credential(s) (password/ID, token, etc.)
- **Encryption:** The process of encoding or obfuscating messages or information in such a way that only authorized parties can read it
- **Vulnerability management:** The process of identifying and testing known software vulnerabilities within a system and prioritizing remediation according to each vulnerability's likelihood of occurrence and how the exploitation of the vulnerability would impact the system

### (b) Information security minimum requirements

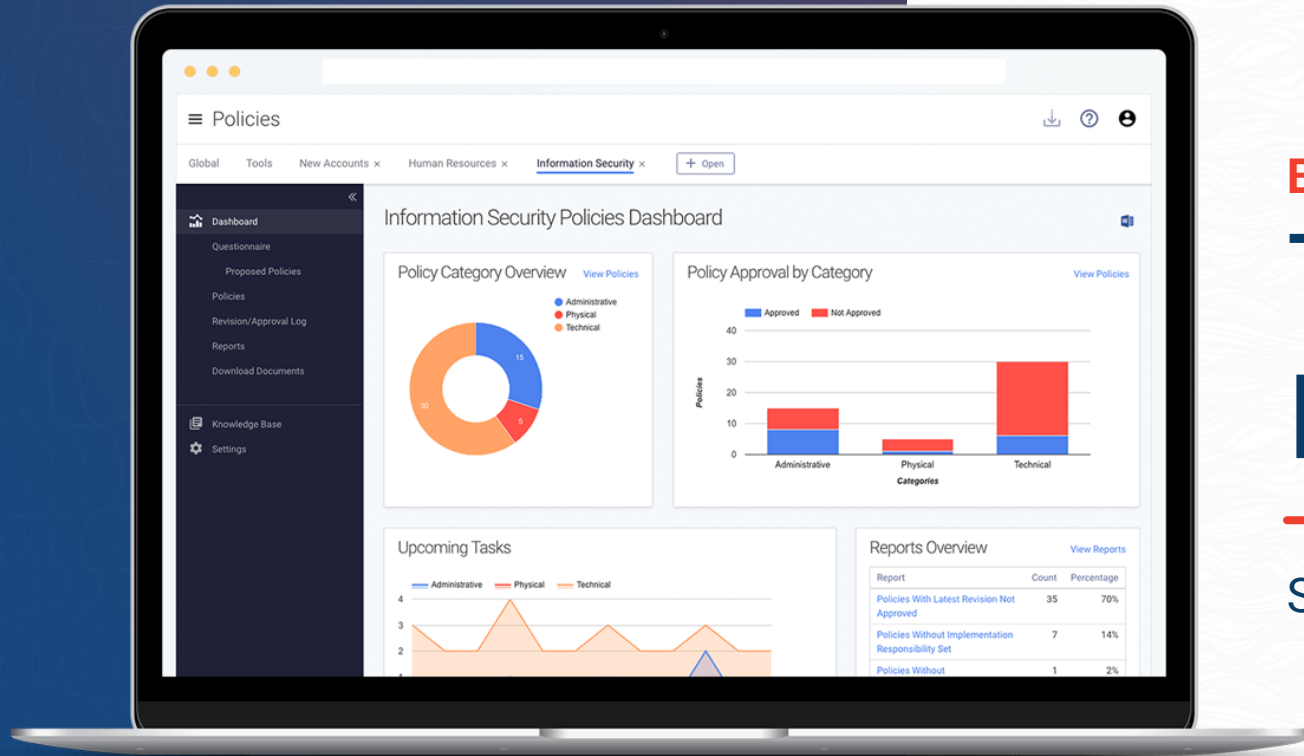
#### (i) Information security program

Seller/Service providers must define an individual or group of individuals responsible for the development of information security requirements, including the adoption, implementation, maintenance and administration of written minimum-security standards, policies and procedures that responsibly address critical issues such as user responsibilities (e.g., "Acceptable Use"); ownership of and access to information; baseline security practices; physical, administrative and technical security protection mechanisms and other requirements.

Not less than annually, Seller/Service providers must review and assess the adequacy of their information security policies and procedures used in connection with the selling and Servicing of Freddie Mac Mortgages to ensure compliance with the Guide, their other Purchase Documents and industry best practices (including as set forth by the Federal Financial Institutions Examination Council and National Institute of Standards in Technology). Upon request of Freddie Mac, Seller/Service providers must make their information security program policies and procedures available and provide an attestation of the adequacy of these policies and procedures, including following Freddie Mac's termination of a Seller/Service provider's right to sell or service Mortgages.

#### (ii) Human resources security

- **Pre-employment screening:** Seller/Service providers must conduct, or retain a qualified third party to conduct, thorough background verification checks (screening) for all candidates for employment or contractor status who will have access to Freddie Mac confidential information, Protected Information or Systems
- **Code of conduct or non-disclosure agreement:** Prior to being granted access to Freddie Mac confidential information, Protected Information or Systems, Seller/Service providers must require all employees, contractors and third parties to (i) sign a non-disclosure agreement or (ii) be subject to a code of conduct, which in either case includes obligations to restrict the use or disclosure of and to maintain as confidential all Freddie Mac confidential information
- **Protected Information and information related to or contained in Systems:** The code of conduct must be acknowledged by the employee, contractor or third party, and must address at least the following subjects:
  - Appropriate use of company assets
  - Information protection, including non-disclosure and confidentiality
  - Records management
  - Information security and privacy
  - Business courtesies



BONUS CONTENT

# Tandem & the New Requirements

Stick around after the educational part!



What type of organization do you currently work for?

How familiar are you with Freddie Mac's new Information Security Requirements?

# About Freddie Mac

# HISTORY

1938



Fannie Mae

1968



Ginnie Mae

1970



Freddie Mac

1972



Sallie Mae

1988



Farmer Mac

1989

2008

2023

-  Mixed-Ownership
-  Private / Government-Owned
-  Publicly Traded
-  Government-Sponsored Enterprise (GSE)



Is not your typical  
service provider

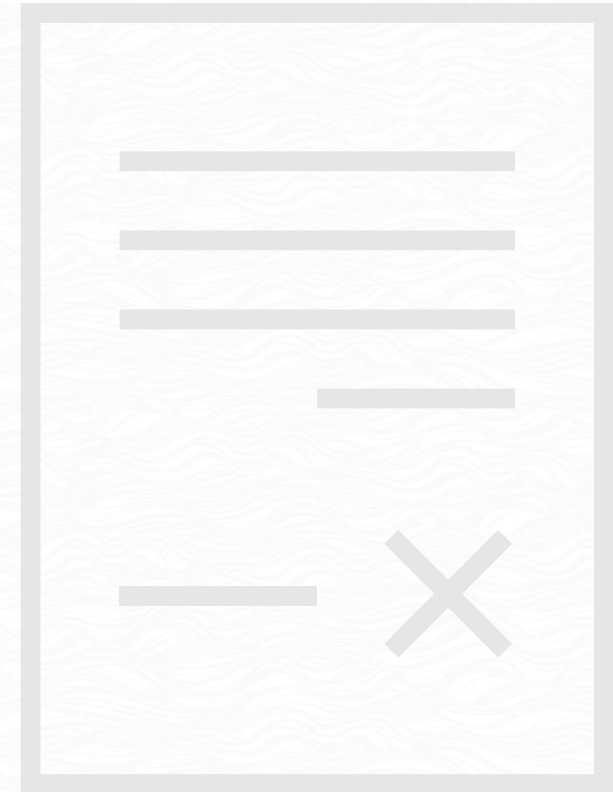


Provides an inherently  
risky service



Builds controls into the  
“Purchase Documents”

- 1 Purchase Contract & Confirmation
- 2 The Guide
- 3 Bulletins
- 4 Guaranty / Credit Enhancement Agreements
- 5 Servicer Success Scorecard
- 6 Guide Plus Additional Provisions
- 7 Loan Selling Advisor ®
- 8 “Any other document designated to be a Purchase Document by Freddie Mac”



Guide Home x +  
https://guide.freddie.mac.com

Freddie Mac Home Single-Family Division Multifamily Division Capital Markets Division Renters, Buyers and Owners

Freddie Mac Single-Family  
Guide Home Seller/Service Relationship Selling Servicing Search the Guide View All

Search *The Single-Family Seller Servicer Guide*  
What can we help you find? Search

Glossary  
AllRegs  
Uniform Instruments

Featured Resources Browse Guide Recent Bulletins Forms & Documents Upcoming Changes Archives

### Featured Resources

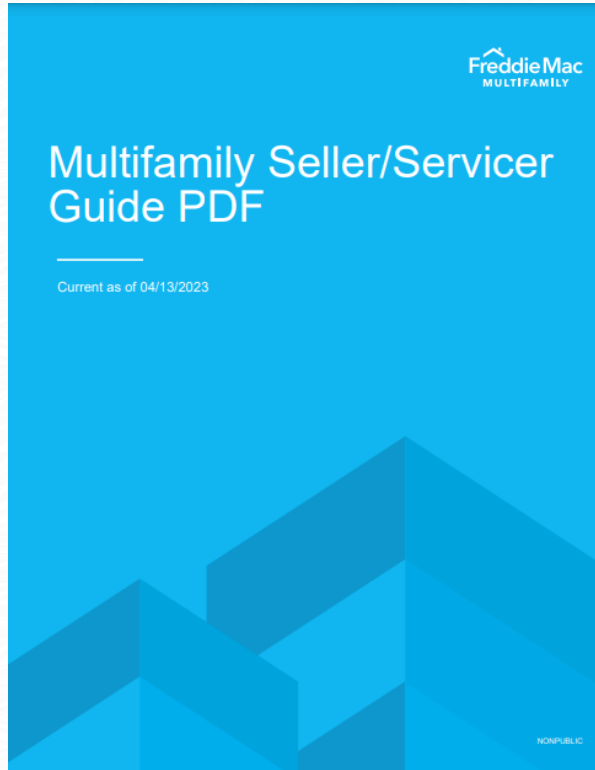
### Recent Bulletins

[View All Bulletins](#) →

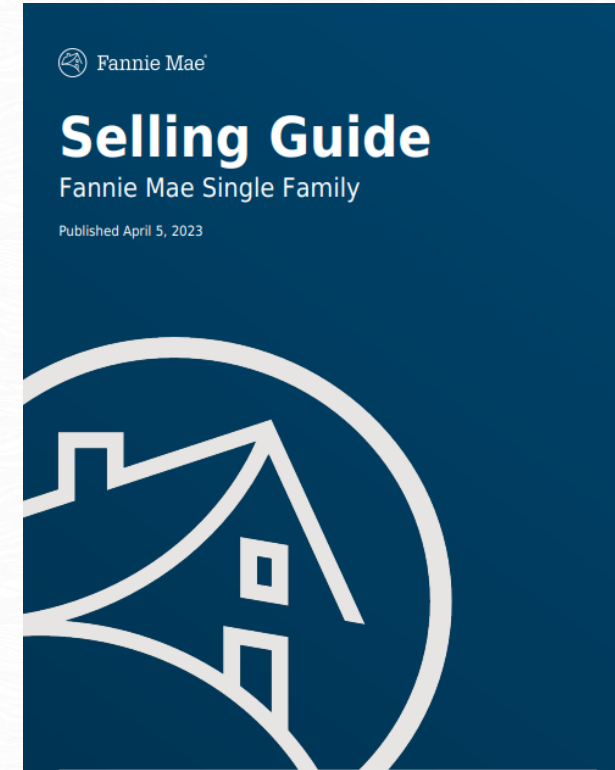
<b>Bulletin 2023-10</b> <b>Servicing</b> 04/12/2023 This Bulletin announces updates to Custodial Accounts, Servicing Contract Rights, BPO fees and more.	<b>Bulletin 2023-9</b> <b>Selling</b> 04/05/2023 This Bulletin announces updates to property appraisals, Condominium Projects, Servicing Contract Rights terminology, and more.	<b>Bulletin 2023-8</b> <b>Servicing</b> 03/29/2023 This Bulletin announces updates to the Payment Deferral and Disaster Payment Deferral and introduces new outreach requirements for low balance loans with non-interest bearing UPB.
---	--	---

# Single-Family Seller Servicer Guide

<https://guide.freddie.mac.com>



**Freddie Mac  
Multifamily Seller/Service Guide**  
Section 2.26 Information Security  
(Page 43)  
[Download PDF](#)



**Fannie Mae  
Single Family Selling Guide**  
Section A3-4-01 Confidentiality of Information  
(Page 136)  
[Download PDF](#)



When did Freddie Mac publish their FIRST minimum standards for information security programs?

**A** 1999

**B** 2005

**C** 2016

**D** 2021

# MAY 2, 2016



BULLETIN 2023-6

# Updated Information Security and Privacy Requirements

Effective Date: July 3, 2023

“We are updating Guide Chapter 1302 to enhance our information security and privacy requirements to be more consistent with industry standards.”

<https://guide.freddiemac.com/app/guide/bulletin/2023-6>

## Bulletin

Freddie Mac  
SINGLE FAMILY

TO: Freddie Mac Sellers

March 1, 2023 | 2023-6

### SUBJECT: SELLING UPDATES

This Guide Bulletin announces:

- **Asset and income modeler (AIM) for Direct Deposit**
  - An update to the delivery requirements for the [Automated Income Assessment with Loan Product Advisor® using Account Data](#) offering – June 1, 2023
- **Credit underwriting – July 3, 2023**
  - Updates to our requirements for [non-occupying Borrowers](#)
  - Updates to our requirements for excluding [assumed Mortgages](#) from the monthly debt payment-to-income ratio
- **Information security and privacy**
  - Updated [information security and privacy](#) requirements – July 3, 2023
- **Additional Guide updates**
  - Further updates as described in the [Additional Guide updates](#) section of this Bulletin

### EFFECTIVE DATE

All of the changes announced in this Bulletin are effective immediately unless otherwise noted.

### ASSET AND INCOME MODELER (AIM) FOR DIRECT DEPOSIT DELIVERY REQUIREMENTS

Effective for Mortgages delivered on and after June 1, 2023; however, Sellers may implement immediately

To improve efficiency for Sellers, we are no longer requiring the delivery of the valid value “H85” for ULDD Data Point *Investor Feature Identifier* (IFI) (Sort ID 368) for Mortgages using Automated Income Assessment with Loan Product Advisor using Account Data (Direct Deposits).

### System impacts

On June 1, 2023, Loan Selling Advisor® will be updated to prevent the delivery of the valid value “H85”. Sellers must update their systems accordingly.

The applicable Loan Product Advisor feedback message will also be retired on June 1.

Guide impacts: Sections 5904.6, 6302.10 and Exhibit 34

### Notice of changes to certain negotiated provisions

This paragraph serves as notice to Sellers with Purchase Documents that contain one or more negotiated provisions with terms related to Mortgages delivered using *Investor Feature Identifier* (IFI) “H85”. The changes to the delivery requirements in this Bulletin, and any corresponding Guide updates, supersede any such terms as of this Bulletin’s effective date.

### CREDIT UNDERWRITING

Effective for Mortgages with Settlement Dates on and after July 3, 2023

#### Mortgages including a non-occupying Borrower

We are updating Section 5103.1 to add a requirement that a non-occupying Borrower must not be an interested party to the transaction (i.e., the buyer or seller).

In addition, we are making the following updates:

- Specifying in Section 5103.1 that a non-occupying Borrower is 95% for offerings with LTV ratio of 95% or less
- Consolidating all requirements for a non-occupying Borrower (including all requirements for a non-occupying Borrower) in Section 5103.1
- Removing from Section 5103.1 the requirement that a non-occupying Borrower must not be an interested party to the transaction

#### Exclusion of payment on assumed Mortgage

Currently, we permit the payment on an assumed Mortgage to be made by the fully executed assumption agreement.

- Specify that the payment on an assumed Mortgage by the borrower must be made by the fully executed assumption agreement.
- Add the requirement that the payment on an assumed Mortgage by the borrower must be made by the fully executed assumption agreement.

Guide impact: Section 5401.2

### INFORMATION SECURITY AND PRIVACY

Effective July 3, 2023

We are updating Guide Chapter 1302 with industry standards. These updates include:

- Revisions to our information security and privacy requirements:
  - Incident management
  - Mobile computing
  - Auditing, logging and monitoring
- New requirements related to information security and privacy, including:
  - Information security and privacy requirements
  - Information security and privacy requirements
- An update confirming that the Protected Information Retention Policy applies to all service Mortgages

Seller/Service providers must have a Freddie Mac Protected Information Policy.

Bulletin

Additional information will be announced in a future Guide Bulletin to provide Seller/Service providers direction on how to report Non-Critical Privacy Events (as defined in Section 1302.2) and how to obtain information on specific relationships Freddie Mac may have with Related Third Parties.

Guide impacts: Section 1301.2 and Chapter 1302

### Additional resources

We encourage Seller/Service providers to review the following resources:

### ADDITIONAL GUIDE UPDATES

#### Correspondent XChange

Servicing-Released XChange Rights and helps Sellers easily add to the Guide Correspondent XChange.

Sellers that originate Freddie Mac loans through a Loan Selling Advisor to transfer Mortgages for cash. Currently, XChange executions, known as Operational Bifurcated Mortgage Representations and Warranties, are required for Operational Bifurcation Multi-Party Agreements as described in the Guide.

We are adding new Chapter 1302, Loan Selling Advisor, and updating the Guide to include adding the term “Operational Bifurcation Multi-Party Agreement” to the Guide.

Freddie Mac must approve Seller/Service providers questions about the new multi-party agreement will be effective May 3, 2023, supersede the existing program agreement.

Guide impacts: Chapter 6306

### Effective dates

For Sellers that are newly approved to participate in the program, the new multi-party agreement will be effective May 3, 2023, supersede the existing program agreement.

For Sellers already participating in the program, the new multi-party agreement will be effective May 3, 2023, supersede the existing program agreement.

Guide impacts: Chapter 6306

### Credit Fee updates

Effective for Mortgages with Settlement Dates on and after July 3, 2023

We are making applicable Guide updates to reflect the new industry standards.

Guide impacts: Sections 5103.1 and 5103.2

### Update to Exhibit 4A, Seller/Service Provider Information

We updated Exhibit 4A to reflect the new industry standards.

Deed of Trust was revised to reflect the new industry standards.

Guide impacts: Exhibit 4A

### Additional resources

We encourage Seller/Service providers to review the following resources:

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

• [Freddie Mac Seller/Service Provider Information](#)

• [Freddie Mac Protected Information Policy](#)

**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

# New Requirements



Mobile Computing



Auditing, Logging, & Monitoring



Software & Application Development Life Cycle (SDLC)



Incident Management



Access Control: Cloud Computing



Have a written “Mobile Devices” policy.



Get it approved by management.



Communicate it with personnel.



Make sure it addresses best practices.

## 1302.2(b)(viii)

Seller/Service providers must maintain a written mobile device/computing management (MDM) policy that has been approved by management and communicated to all appropriate personnel. This policy must reflect current and best practices, specifying parameters including but not limited to:

- Approved and prohibited applications
- Cryptographic mechanisms to ensure data security
- Identity and access management requirements
- Software updates



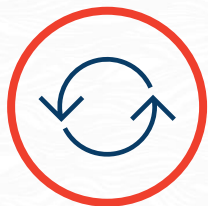
## Approved & Prohibited Applications



## Encryption



## Authentication



## Patch Management



### 1302.2(b)(viii)

Seller/Service providers must maintain a written mobile device/computing management (MDM) policy that has been approved by management and communicated to all appropriate personnel. This policy must reflect current and best practices, specifying parameters including but not limited to:

- Approved and prohibited applications
- Cryptographic mechanisms to ensure data security
- Identity and access management requirements
- Software updates



Related Policies

Related Policy
Data Retention
Employee Hiring
Employee Security Training
Hardware and Software
Incident Management
Remote Access
Security Testing
Software Patching
System Hardening
User Authentication
Committee/Team
Frequency
Quarterly
Quarterly

same security requirements for both organization-owned and personally-owned mobile devices should be enforced. BYOD devices are inherently less standardized than organization-owned devices and therefore may require additional security controls.

Implementation

Implement a process to:

- Require senior management approval before granting access to sensitive data to be accessed through mobile devices.
- Document approved mobile devices.
- Review approved mobile devices for changes in technology.
- Use a mobile device management (MDM) solution.
- Retain the authority to remotely wipe or disable mobile devices.
- Prohibit the use of mobile devices for unauthorized network access.
- Communicate security requirements to personnel on mobile devices.
- Follow organization policies for mobile devices that can no longer be used.

Secure Configuration

Before a mobile device is used for business purposes, ensure the device is configured securely.

- Require authentication for mobile devices, such as biometrics, PIN, or password.
  - Lock after a period of inactivity.
  - Remote wipe mobile devices if lost or stolen.
  - Lockout or auto-lock mobile devices if password is entered incorrectly.
  - Encrypt data on mobile devices.
  - Install patches and updates.
- In addition, verify that:
- The device is not modified.
  - The device has anti-malware software installed.

Mobile Device Management

Copyright © 2023

## Mobile Device Management (MDM)

Revision 1.0

Approval Pending

Securely provision, monitor, and manage mobile devices used for business purposes. Prohibit the use of unauthorized mobile devices.

### Commentary

The National Institute of Standards and Technology (NIST) defines a "mobile device" as:

*"A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source."*

For the purpose of this policy, the following items are considered to be "mobile devices."

- Laptops
- Phones (e.g., smartphones, cellphones, etc.)
- Tablets
- Wearables (e.g., smartwatches, smart glasses, etc.)
- Other portable devices (e.g., e-readers, digital assistants, navigation devices, digital cameras, etc.)

The use of mobile devices for business purposes is becoming more common due to technological advancements and operational efficiencies. Some examples of mobile device use for business purposes could include, but are not limited to:

- Connecting to the organization's network from a remote location (a.k.a., "remote access").
- Performing remote processing functions.
- Building resilience into business continuity objectives.
- Accessing, storing, or transmitting organization or customer information.
- Using work communication channels, like email, team collaboration tools, video conferencing, or file sharing.

To promote security, the organization needs to ensure effective mobile device controls are in place, and users are educated on security expectations.

At times, personnel may wish to use a personally-owned device to perform work-related duties. This is commonly referred to as "bring your own device" or "BYOD." If the organization elects to allow BYOD, the



## TANDEM POLICIES

# Mobile Device Management (MDM) Policy

[Tandem.App/MDM-Policy](#)



Have written guidelines for logging and monitoring.



Create written log retention and handling requirements.



Have an independent controls audit at least annually and in the event of a security or privacy incident.

## 1302.2(b)(xii)

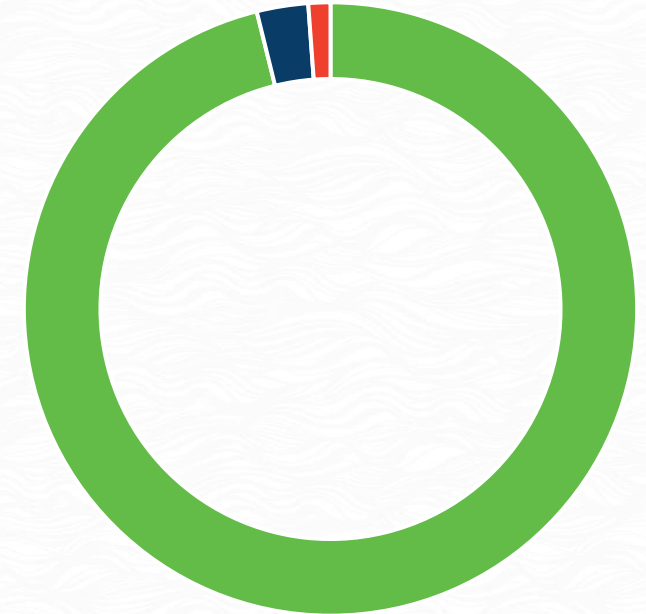
Seller/Service providers must:

- Develop, implement and maintain written guidelines and requirements for the logging and monitoring of activities and action within information systems. If the Seller/Service provider uses an enterprise log management function, the subject requirements must be integrated with such log management function.
- Develop, implement and maintain written log retention and handling requirements to ensure logs retain relevant, useable and timely information sufficient to identify user access and/or system activities.
- Perform an independent security assessment of the control environment not less than annually and upon the occurrence of any data Security Incident or Privacy Incident (defined below).

**BASELINE**

Audit log records and other security event logs are reviewed and retained in a secure manner.

- Yes **(96.13%)**
- Yes, with compensating controls **(2.71%)**
- No **(1.16%)**

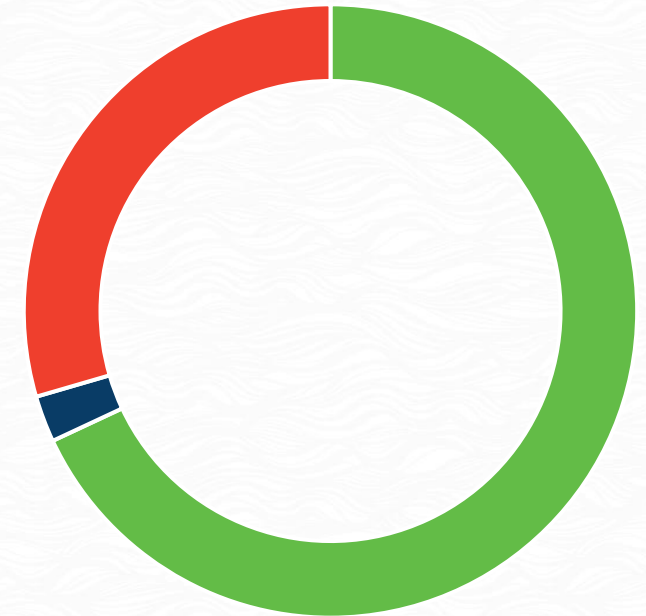




## INTERMEDIATE

Audit logs are backed up to a centralized log server or media that is difficult to alter.

- Yes (68.04%)
- Yes, with compensating controls (2.45%)
- No (29.51%)





“Log management is the process to generate, transmit, store, analyze, and dispose of log data. With respect to operations, a log is a record of events occurring within an entity’s systems and networks. Management should have a process to use logs to identify, track, analyze, and resolve problems that occur during day-to-day operations.”

**1**

Occurrence Logs

**2**

Anomaly Logs

**3**

Usage Logs

**4**

Activity Logs



## Logging can help with:

- Troubleshooting issues.
- Investigating potential incidents.
- Knowing “normal” baseline activity.
- Supporting ongoing improvements.

## Logging is hard because:

- There is a ton of data.
- Storage and capacity are limited.
- Analysis / response requires skill.
- False positives happen.



Upskill

- or -



Outsource



**CoNetrix**  
*Technology*

# Cybersecurity Monitoring & Compliance Services

[CoNetrix.com/Technology/  
Security-Monitoring-and-Reporting](https://CoNetrix.com/Technology/Security-Monitoring-and-Reporting)



Does your organization develop software internally?



## If your organization develops software:



Have a written “Software Development Life Cycle” policy.



Get it approved by management.



Make sure it addresses best practices, like:

- Separate production and testing environments
- Secure coding practices\*
- Open-source requirements
- Code deployment best practices

### 1302.2(b)(xiii)

If a Seller/Service provider develops applications or software that store, access, process or transmit Freddie Mac confidential information, Protected Information or connects to Systems, the Seller/Service provider must develop, implement and maintain a written SDLC process and policy that has been approved by management. This policy must include at minimum:

- Management and separation of production and development environments that reflect contemporary best practices
- Secure coding requirements
- Open-source requirements
- Code development and scanning pre- and post-deployment

**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



Have an Incident Response Plan.



Make sure it addresses best practices, like:

- Playbooks for incident response
- Necessary resources
- Clearly defined roles and responsibilities



Test the plan annually, unless formally activated.

## 1302.2(b)(xv)

Seller/Service providers must:

- Develop and maintain, and implement when triggered, an incident response plan that provides a roadmap for implementing incident response capabilities and defines the resources and management support needed.
- Annually, unless formally activated, test the effectiveness of the incident response plan and capabilities.



Roles & Responsibilities



Classification Strategies



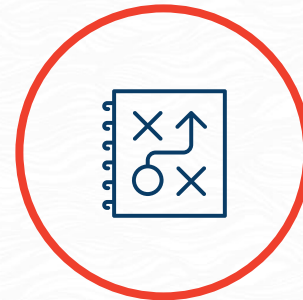
Handling Processes



Communication Guidelines



Evidence & Forensics Procedures



Category-Specific Playbooks



Incident Tracking System

WELCOME TO

# How to Create an Effective Incident Management Plan



---

Alyssa Pugh, Security+  
GRC Content Manager  
Tandem, LLC



WATCH THE SESSION

[Tandem.App/2021-Incident-Management](https://Tandem.App/2021-Incident-Management)



# RESOURCES



## ARTICLE

[7 Steps for Building a Successful Incident Response Team](#)



## ARTICLE & CHECKLIST

[Ransomware Incident Response Playbook](#)



## ARTICLE & CHECKLIST





[Third-Party Incident Response Playbook](#)



## SOFTWARE PRODUCT

[Tandem Incident Management](#)



-  Have a written “Cloud Computing” policy.
-  Get it approved by management.
-  Communicate it with personnel.
-  Review the policy on a regular basis.

## 1302.2(b)(xvii)(E)

When a Seller/Service provider consumes or provides cloud services that store, process, access or transmit Freddie Mac confidential information or Protected Information or connect to any System, the Seller/Service provider must maintain a formal cloud computing policy that has been approved by management and communicated to appropriate personnel, and the Seller/service provider must designate an owner to maintain and review the policy to ensure it consistently reflects industry best practices.





## VII EVOLVING TECHNOLOGIES

Entities use a variety of evolving technologies (e.g., cloud, zero trust architecture [ZTA], AI and ML, and IoT) that may impact architecture, infrastructure, and operations functions. This section provides general information relating to these evolving technologies and, when appropriate, certain risks and control principles discussed in prior sections of this booklet.

### VII.A Cloud Computing

Cloud computing environments are enabled by virtualization technologies, which allow cloud service providers to segregate and isolate multiple clients on a common set of physical or virtual hardware. NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.”<sup>86</sup> Cloud systems provide several benefits, including scalability of resources and consistency in deployment of controls across systems and software.

For the purposes of this section of the booklet, when the term “cloud service provider” is used, it refers to the provider offering cloud computing services. When the term “entity” is used, it refers to the client receiving cloud computing services.

As defined by NIST, “cloud computing has five essential characteristics, three service models, and four deployment models.”<sup>87</sup>

#### VII.A.1 Essential Characteristics

According to the NIST definition, cloud implementations take advantage of all of the following five “essential characteristics.”<sup>88</sup> Some entities may characterize their environment as “cloud computing” without it exhibiting all five characteristics. NIST describes the five essential characteristics as follows:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each third-party service provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

<sup>86</sup> Refer to [NIST SP 800-145, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology](#).

<sup>87</sup> [Ibid.](#)

<sup>88</sup> [Ibid.](#)

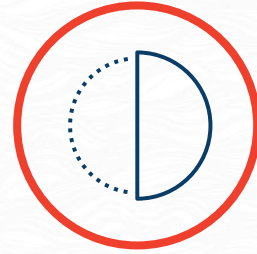
## FFIEC GUIDANCE

# Architecture, Infrastructure, & Operations Booklet Section VII.A Cloud Computing

[Read the Booklet](#)



Cloud Service  
Provider Selection



Data Segregation &  
Encryption



IT Asset Inventory



Geographic  
Restrictions



Access Control



Contractual  
Requirements



Mobile Computing



Auditing, Logging, & Monitoring



Software & Application Development Life Cycle (SDLC)



Incident Management



Access Control: Cloud Computing

**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

# Notable Updates



## Annual Review & Validation Requirements



## Policies



## Third Parties



## Termination Considerations



## Program Administration



## Security Testing

---

1302.2(b)(x)

Independent Pen Test

1302.2(b)(x)

Vulnerability Assessment

1302.2(b)(xii)

Independent Security  
Assessment



## Access Reviews

---

1302.2(b)(iii)

Physical Facilities

1302.2(b)(ix)

Wireless Networks

1302.2(b)(xvii)(B)

All User Access Privileges



## Admin Reviews

---

1302.2(b)(i)

Information Security  
Program

1302.2(b)(vii)

Firewall Rules

1302.2(b)(xvii)(D)

IT Asset Inventory to  
Actual Inventory



# CoNetrix *Security*

IT Audit,  
Penetration Test,  
and Vulnerability  
Assessment  
Services

[CoNetrix.com/Security](https://CoNetrix.com/Security)





- ✓ Data Loss Prevention (DLP)
- ✓ Mobile Device Management (MDM) - **NEW**
- ✓ Vulnerability Assessment
- ✓ Patch Management
- ✓ Software Development Life Cycle (SDLC) - **NEW**
- ✓ Encryption & Cryptography
- ✓ Cloud Computing - **NEW**



## Key Sections of an Information Security Policy

Dec 13, 2022  
Published Date: Dec 13, 2022



GRC CONTENT MANAGER  
Alyssa Pugh



1302.2(b)(ii)  
Nondisclosure Agreement  
- or - Code of Conduct



1302.2(b)(xvii)(F)  
Minimum Security  
Requirements



1302.3  
Exception to Third-Party  
Beneficiary Requirement



1302.1 | 1302.2(b)(i) | 1302.3

You are obligated to secure any Freddie Mac confidential information that you retain after termination of services.

1302.1

You are obligated to comply with the requirements. Failure to comply may result in termination of rights to Freddie Mac systems.

1302.2(b)(xvii)(A)

You are obligated to notify Freddie Mac within 24 hours of termination (or transfer) of an employee with a Freddie Mac systems user account.



1302.2(b)(i)

Designate a Responsible  
Person or Group



1302.2(b)(i)

Provide Attestation  
Upon Request\*



1302.2(b)(ii)

Require Personnel to Sign  
NDA / Code of Conduct



## Annual Review & Validation Requirements



## Policies



## Third Parties



## Termination Considerations



## Program Administration

**SUBMIT YOUR  
QUESTIONS!**

**We want to  
hear from you.**

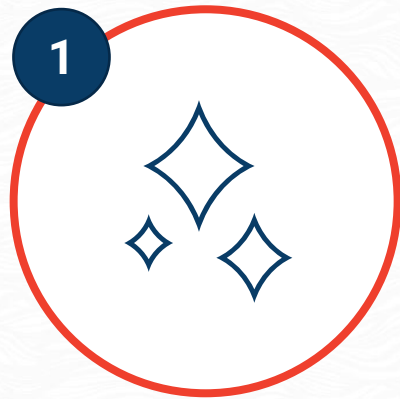
---

Use the “Questions” panel to:

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

# What Can You Do?

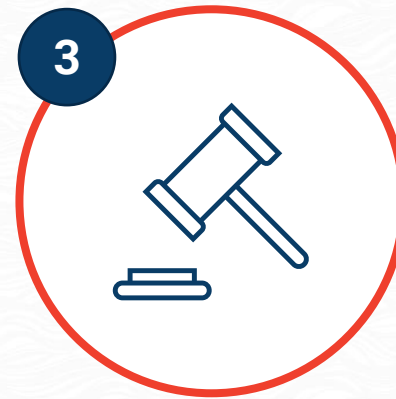
# STEP 1: REFOCUS



These are new requirements.



These are security best practices.



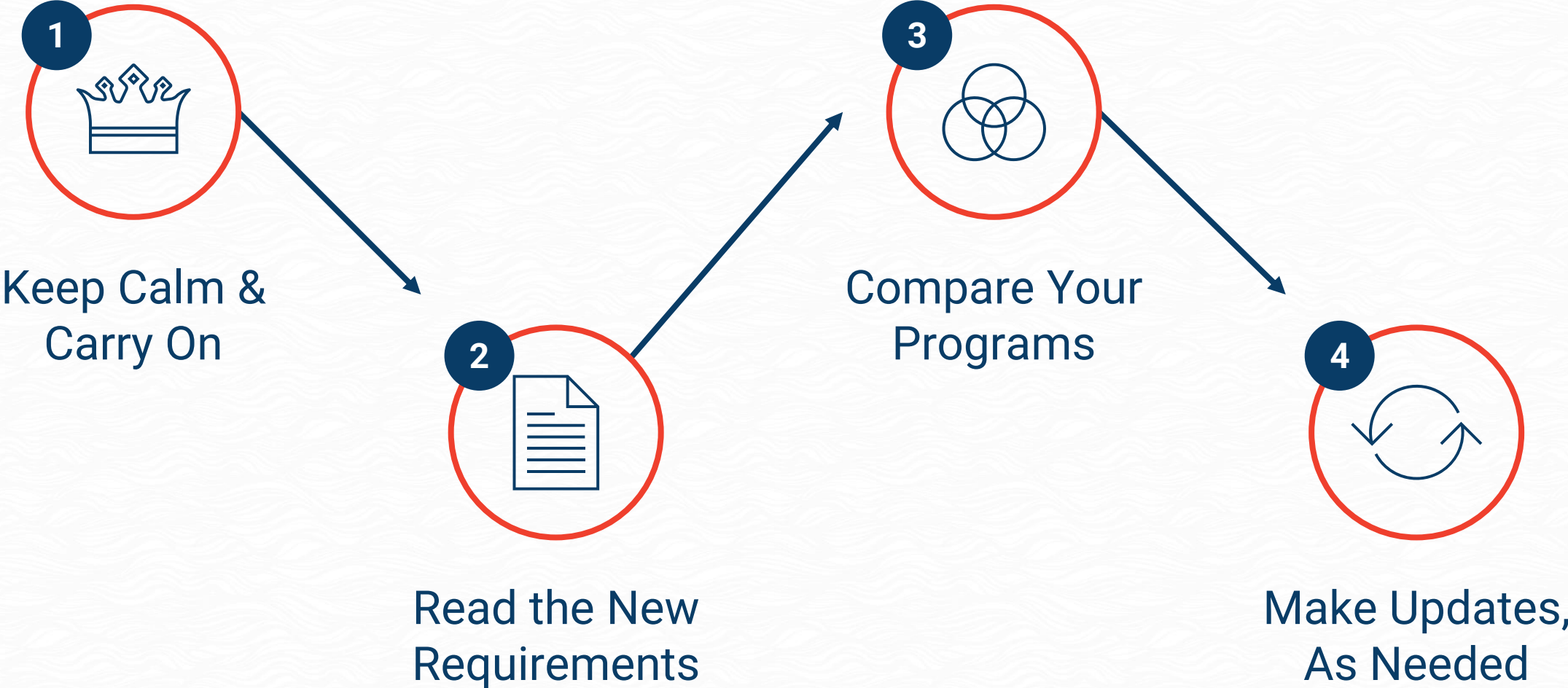
These are required by other agencies.

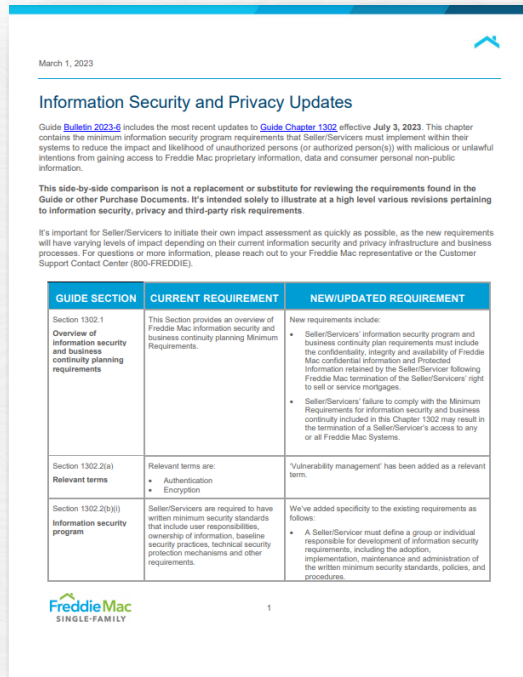


These are definitely do-able.



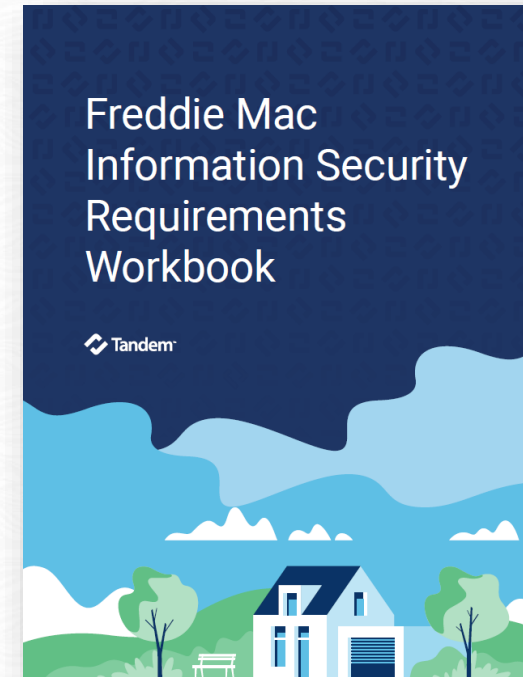
# STEP 2: TAKE ACTION





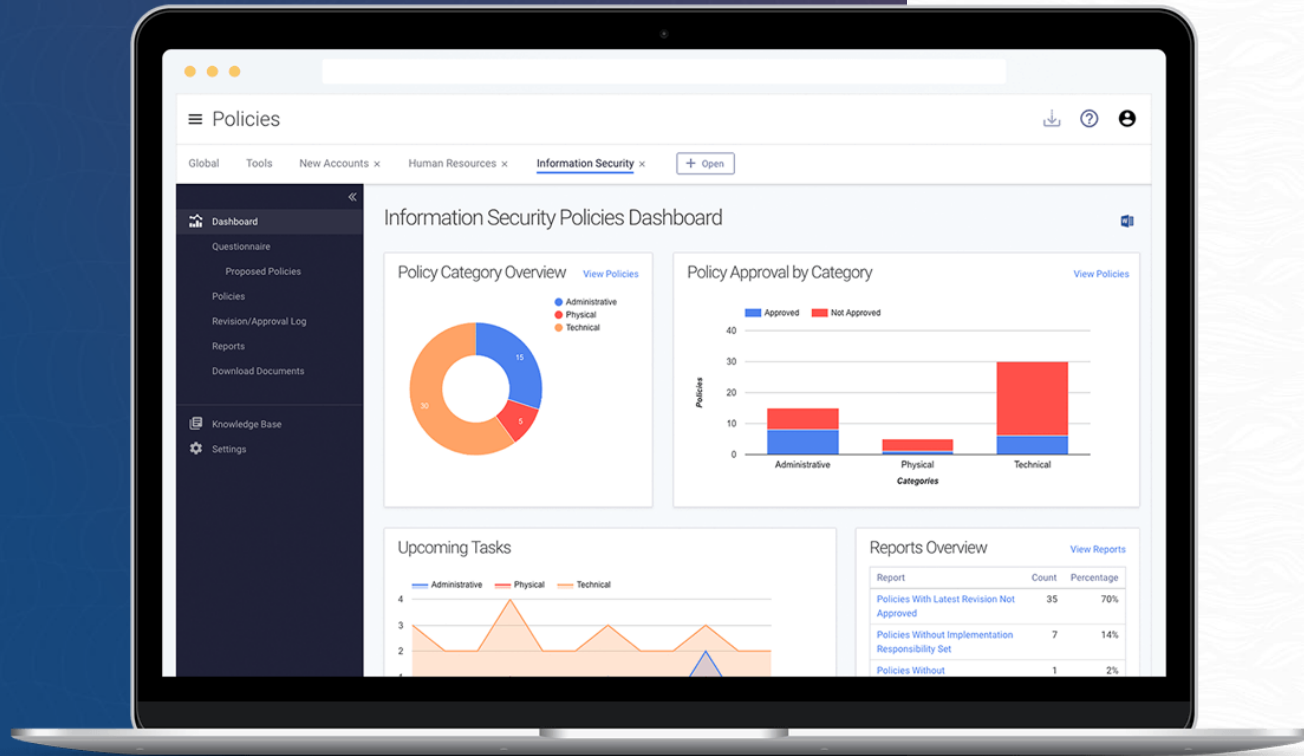
## Information Security and Privacy Updates Side-By-Side Comparison

[Download the Comparison](#)



## Freddie Mac Information Security Requirements Workbook by Tandem

[Tandem.App/Freddie-Mac-Workbook](https://Tandem.App/Freddie-Mac-Workbook)



**BONUS CONTENT**

# Tandem & the New Requirements

Fill out the survey for  
a chance to win!



THANKS FOR JOINING

# Maintaining Compliance with Freddie Mac's New Information Security Requirements

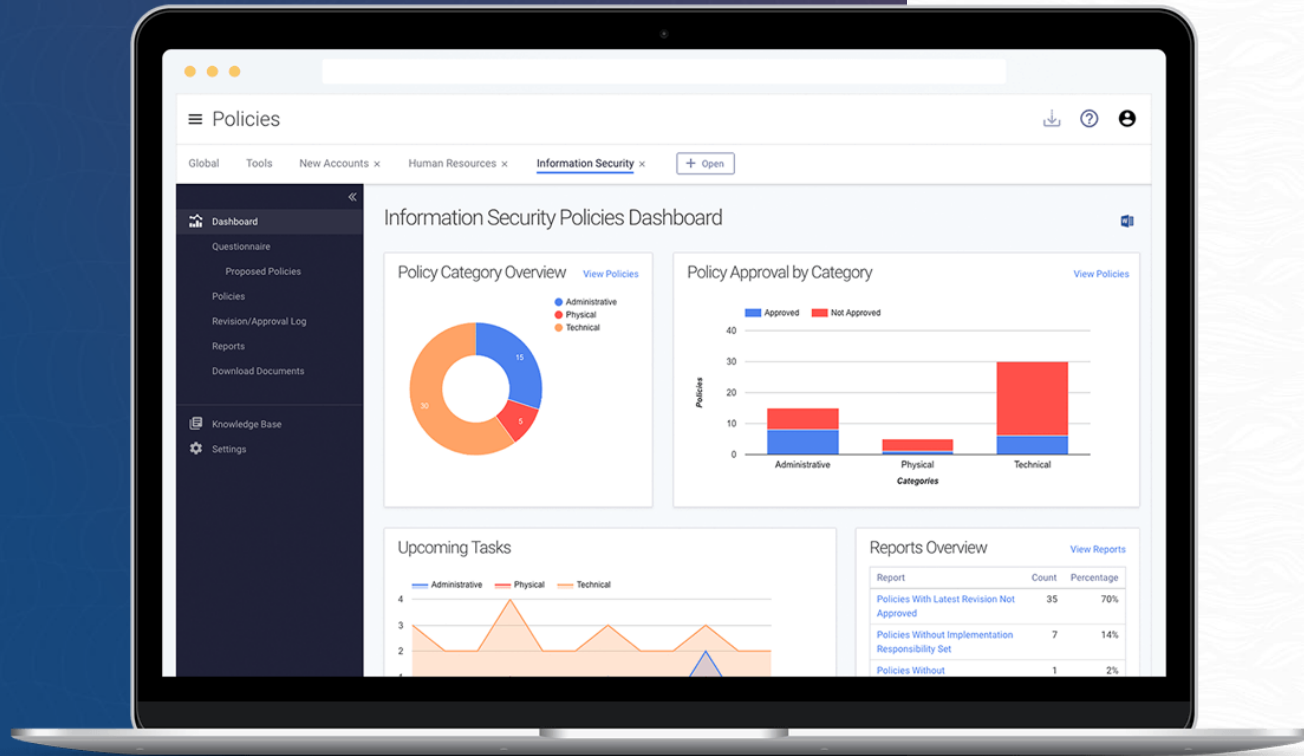
---

Alyssa Pugh, CISM, Security+  
[apugh@tandem.app](mailto:apugh@tandem.app)  
[LinkedIn.com/in/AlyssaPugh](https://www.linkedin.com/in/AlyssaPugh)



*Remember to complete the survey!*





**BONUS CONTENT**

# Tandem & the New Requirements



**COMPLETE THE SURVEY**  
Answer "Yes" on Question 4



**VISIT OUR WEBSITE**  
[Tandem.App/Demos](https://Tandem.App/Demos)



**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



THANKS FOR JOINING

# Maintaining Compliance with Freddie Mac's New Information Security Requirements

---

Alyssa Pugh, CISM, Security+  
[apugh@tandem.app](mailto:apugh@tandem.app)  
[LinkedIn.com/in/AlyssaPugh](https://www.linkedin.com/in/AlyssaPugh)



*Remember to complete the survey!*

