

# Why Some Frameworks Cost More:

## A Plain-English Look at Remediation Steps

Not all frameworks are created equal—and neither is the effort to implement them.

### Why Pricing Differs

Pricing isn't uniform because the complexity and scope of every framework vary.

Whether you're working with **HIPAA/HITRUST**, **PCI DSS v4.0**, **CPRA**, or others supported in Microsoft Purview Compliance Manager, each framework comes with unique challenges.

### Key Price Drivers

- **Improvement Action Volume & Control Complexity**
  - ISO 27001 may require 150+ tasks and controls.
  - SOC 2 could have considerably fewer.More actions = more technical work, consulting, and enablement.
- **Mandated Extras**

Certain frameworks require additional steps like:

  - Data Loss Prevention (DLP) implementation
  - Sensitivity labeling for safeguarding sensitive information

AuditAble scopes and charges only for what's required—no upselling.

### Effort Profiles by Framework

Here's how three common frameworks compare in Microsoft Purview Compliance Manager:

Framework	Policy & Governance	Technical & Config	Ongoing Assurance	Focus
HIPAA/HITRUST	High	Med-High	High	DLP, sensitivity labels, validated assessment
PCI DSS v4.0	Moderate	High	High	Network segmentation, secure coding, quarterly scans
CPRA	High	Moderate	Moderate	DSAR portal, consent mgmt., data inventory

## Cost Implications

- **HIPAA/HITRUST:** Privacy & security controls, PHI mapping, DLP labeling, validated assessments.
- **PCI DSS v4.0:** Infrastructure hardening, secure coding, vulnerability scanning, quarterly scans.
- **CPRA:** Legal compliance, DSAR workflows, consent management, vendor governance.

### About

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

The PCI DSS is a set of policies and procedures implemented for the security of all types of transaction. It also protects cardholders against misuse of their personal information. The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. One can keep your data secure, avoiding costly data breaches and protecting your employees and your customers.

[More info on PCI Security](#)

Compliance Manager > Assessments > PCI DSS v4.0 Assessment > Detect and block malware and viruses

Detect and block malware and viruses

Owner

Implementation status

Test status

Service

Testing type

Testing source

Details

Evidence

Related controls

How to implement

Microsoft recommends that your organization use an antivirus solution to detect and block malware and viruses. Consider configuring malicious code protection mechanisms to:

- Perform periodic scans of the information system
- Run real-time scans of files from external sources as the files are downloaded, opened, or executed
- Block or quarantine malicious code
- Send alerts to an administrator

Filter

Report

Filters

Regulation: Any

Related Controls	Control ID	Regulation
Anti-malware mechanisms and processes are active, m...	5.3.2	PCI DSS v4.0
Network intrusions and unexpected file changes are d...	11.5.1	PCI DSS v4.0
Network intrusions and unexpected file changes are d...	11.5.1.1	PCI DSS v4.0

Endpoint security | Antivirus

Overview

Summary

Identify endpoints

Active malware

Removal settings

Identify endpoints

Active malware

Identify endpoints

Active malware

Identify endpoints

Active malware

Identify endpoints

Active malware

Identify endpoints

Active malware

Identify endpoints

Active malware

Identify endpoints

Active malware

## About

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) mandate a set of federal requirements for protecting electronic Protected Health Information (ePHI) for U.S. healthcare institutions.

[More info on HIPAA/HITECH] (<https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf>)

Compliance Manager > Assessments > HIPAA/HITECH Assessment > Create and publish a retention label

This action is tested automatically. You can't edit implementation and testing status, but you can edit notes and add documentation. [Learn more](#)

### Create and publish a retention label

Save Save and close Cancel Edit details Export testing history

**Owner** **Implementation status** **Test status** **Service** **Testing type** **Testing source**

Assign owner Not Implemented Failed high risk Microsoft 365 Automatic Not Available

Details Evidence Related controls

Microsoft recommends that your organization use retention labels to classify content as required to comply with relevant regulations, standards, and policies. With retention labels, your organization can classify data across your organization for governance and enforce retention rules based on that classification. Your organization should consider making retention labels available to people in your organization so that they can classify content is a two-step process: first, you create the retention labels, and then you publish them to the locations you choose. When you publish retention labels, a retention label policy gets created.

Regulation: Any

Related Controls

☐ Time Limit (Required)

Control ID

Regulation

45 C.F.R. 164.308(a)(2)(ii)

HIPAA/HITECH

### Define label settings

We'll apply the settings you choose to labeled items

- ☐ **Retain items forever or for a specific period**  
Labeled items can't be permanently deleted during this period. You'll define how long the retention period is and what happens to items during and after the retention period in the next steps.
- ☒ **Enforce actions after a specific period**  
Labeled items won't be retained. You can decide whether they should be deleted, or relabeled when the period you specify in the next step ends.
- ☐ **Just label items**  
Choose this setting if you only want to classify labeled items. The items won't be retained and your users won't be restricted from editing, moving, or deleting them.

### Define the retention period

Specify how long the retention period should be.

Retain items for  
7 years

Start the retention period based on

- ☒ When items were created
- ☐ When items were last modified
- ☐ When items were labeled
- ☐ Product lifetime(event type)
- ☐ Expiration or termination of contracts and agreements(event type)
- ☐ Employee activity(event type)

### Define the period

Choose how long the period is and when it begins.

How long is the period?  
7 years

When should the period begin?

- ☒ When items were created
- ☐ When items were last modified
- ☐ When items were labeled

### Choose what happens after the period

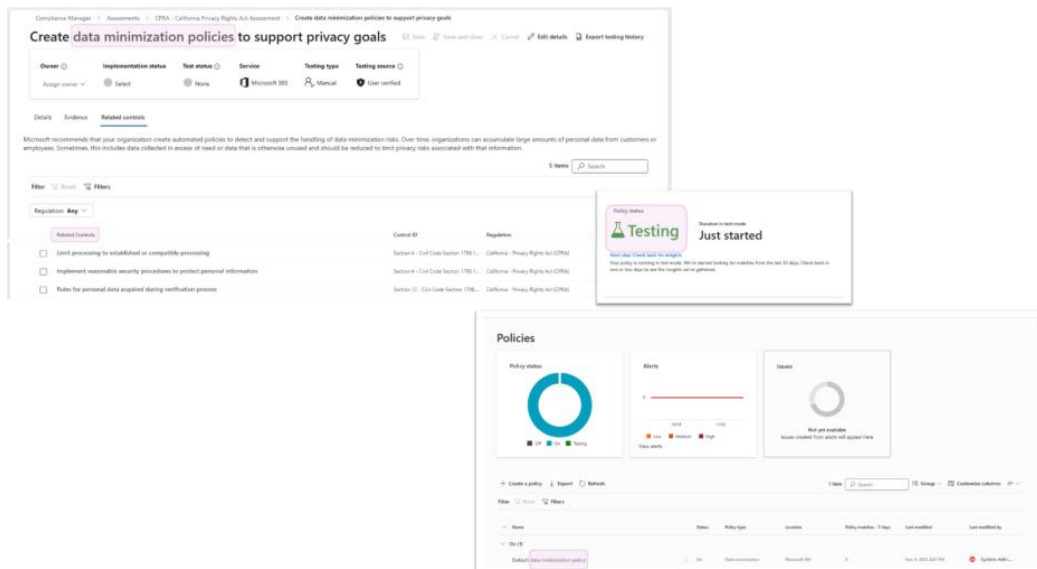
These settings determine what happens to items when the period ends.

- ☒ **Delete items automatically**  
We'll permanently remove labeled items from wherever they're stored.
- ☐ **Change the label**  
You can extend the period by choosing an existing label to replace this one with. [Learn more about retention labels](#)

About

The California Privacy Rights Act (CPRA) is an additional privacy regulation in California. The act amends portions of the California Consumer Privacy Act such as providing additional measure for sensitive personal information, expanding opt-out rights, enhancing other individual rights, and establishing a new California Privacy Protection Agency. Much of this regulation will go into effect in 2023 and will only apply to personal information collected by business on or after Jan 1, 2022. Subdivisions (m) and (n) of Section 1798.145, Sections 1798.160, 1798.185, 1798.199.10 through 1798.199.40, and 1798.199.95, shall become operative on the effective date of the Act. CPRA is applicable if your organization sells to, provides services to, or employs residents of California.

[More info on California CPRA](#)



## Transparency First

AuditAble establishes your compliance baseline and identifies exact controls and improvement actions upfront. You get a clear, itemized breakdown—no hidden work or surprise costs.

## Ready to Discover Your Effort Profile?

**Book your [readiness call](#) today** and get your framework's effort profile in 30 minutes—before you spend a dollar.

## Forwardable Summary (for internal champions):

Compliance costs vary because frameworks differ in complexity, technical requirements, and mandated extras. AuditAble prices based on real work—no surprises. [Book your readiness call

→ <https://outlook.office.com/book/AuditAbleComplianceEnablement@jadexstrategic.com/?ismsaljsauthenabled>]