Mac compliance in 4 phases

Why Mac compliance matters

Reduce risk

Avoid fines, legal exposure, and reputational damage from non-compliance

Build trust

Protect sensitive business and employee data with aligned security controls

Strengthen security

Close gaps before they become vulnerabilities

Regulatory landscape

CIS Benchmarks
GDPR HIPAA NIS2
DORA ISO 27701

1. Preparation

User accounts & profiles

Create user roles and define access needs early.

Organizational policies

Align rules, permissions and ownership across stakeholders

Compliance scope

Identify which industry and regional requirements apply

Compatibility check

Confirm devices, apps and tools support your compliance approach

2. Setup & configuration

Apply benchmarks

Enforce CIS Level 1 or 2 standards across your fleet

Configuration profiles

Use standardized profiles to apply settings consistently

Core security

Enable encryption, system protections, and app controls

3. Testing & rollout

Verify functionality

Test apps and system features before broad deployment

Security audits

Review configurations and controls before go-live

Pilot group

Start with a smaller group to validate rollout in practice

Onboarding

Provide clear guidance and support for end users

4. Ongoing maintenance

Audits

Review compliance regularly

Updates

Keep OS and security patches current

Monitoring

Track threats and compliance status continuously

Adapt

Adjust controls as regulations and policies evolve

Key Apple enablers

DDM & Blueprints

Policy-based configuration that helps devices stay aligned automatically

Smart Groups

Dynamic grouping that helps IT target settings and actions automatically

Compliance benchmarks

Built-in workflows to audit and enforce security standards

+ Self Service+

End-user access to approved apps, updates and key device actions

Get the full guide for a deeper look at compliance benchmarks, enforcement workflows and practical steps for managing Mac compliance more efficiently.

Get the full guide

www.jamf.com