FINDINGFIRST REFERENCE GUIDE

Compliance control map

The frameworks, controls, evidence and owners that carry a company through an audit.

FINANCIAL REPORTING
SOX ITGC
COSO 2013
PCAOB AS 2201

SECURITY ATTESTATION
SOC 2 (AICPA Trust Services Criteria)
ISO/IEC 27001:2022

HEALTH AND PAYMENTS
HIPAA Security Rule
PCI DSS v4.0.1

SECURITY BASELINES
NIST CSF 2.0
NIST SP 800-53 Rev. 5

PRIVACY
GDPR (EU)
CCPA / CPRA (California)

AI GOVERNANCE
NIST AI RMF
ISO/IEC 42001
EU AI Act

FRAMEWORKS AND REGULATIONS

FINDINGFIRST
Control assurance

CONTROL DOMAINS

Access to programs and data
Provisioning, quarterly access reviews, privileged access, segregation of duties

Program change
Approval, testing, emergency changes, separate deploy rights

Computer operations
Backups, job monitoring, incident handling

Program development
SDLC gates, testing, go live sign off

EVIDENCE AND TESTING

Test of design
Does the control, as written, address the risk?

Test of operating effectiveness
Did it run every time across the audit period?

Population and sampling
Complete populations, sample sizes set by how often the control runs

System reports
Proof each report is complete and accurate

OPERATING MODEL

ROLES
Control owners run the control
Risk and compliance oversee it
Internal audit tests it independently
External auditors attest

RISK AND CONTROL MATRIX
Every risk paired with a control, an owner, a frequency, the evidence and the framework reference

POLICIES AND STANDARDS
Access, change, data retention, acceptable use, vendor risk

MONITORING AND REMEDIATION
Deficiencies tracked to closure with owners, due dates and a retest

AUDIT READINESS CYCLE

1 SCOPE → 2 MAP → 3 TEST → 4 REMEDIATE → 5 ATTEST

FindingFirst

Describe a control problem. FindingFirst maps it to every framework it touches.
findingfirst.ai

General information only. Not audit, legal or accounting advice. Confirm requirements with your auditor. © 2026 The Hardwicke Advisory Group LLC