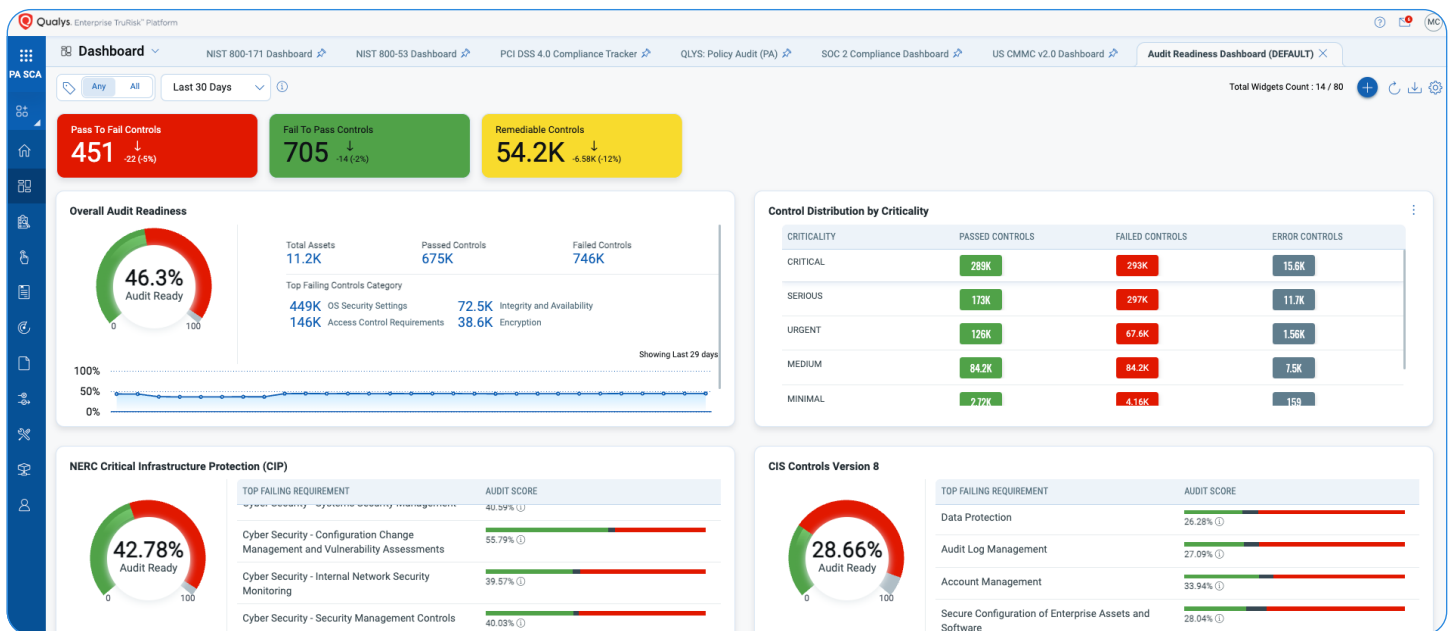


Qualys Policy Audit with Audit Fix

From Detection to Audit Readiness with AI-Powered Compliance

Audit Readiness Gap in the AI Age

Staying audit ready has grown more difficult every year. In today's rapidly changing environments, systems evolve faster than traditional audit cycles were designed to track. Compliance frameworks continue to multiply while evidence remains scattered across spreadsheets, screenshots, ticketing systems, and institutional knowledge. A single misconfigured setting or undocumented change can turn months of preparation into audit findings, and the gap often remains invisible until an auditor uncovers it.



The Future Is Continuous Audit Readiness

Organizations can no longer treat audits as point-in-time events. The challenge is not preparing for the audit but maintaining readiness every day between audits. Qualys Policy Audit helps organizations achieve that goal by combining continuous discovery, risk-based prioritization, and automated remediation through Audit Fix in a single workflow. It identifies the configuration issues most likely to impact compliance outcomes, automates remediation where possible, and continuously maintains audit evidence. The result is not a faster scramble before the audit. It is continuous confidence that systems, controls, and evidence are already aligned with auditor expectations.

The 5-Step Audit Readiness Workflow



Policy Audit transforms audit readiness into a continuous process, helping teams discover assets, identify gaps, remediate issues, and maintain compliance in a single closed-loop workflow.

Workflow Step	Policy Audit
1. Discover Assets and Map Controls Continuously discover servers, databases, middleware, cloud resources, and endpoints, and map them to controls across 100+ compliance frameworks.	
2. Detect Misconfigurations and Control Drift Identify failing controls, policy violations, and configuration drift in near real time across 500+ technologies.	
3. Prioritize Audit-Critical Risks Use TruRisk, MITRE ATT&CK, ransomware exposure, and business context to focus on the findings most likely to impact audit outcomes.	
4. Automate Control Remediation Remediate failed controls at scale with Audit Fix, integrating remediation workflows, validation, and rollback capabilities.	
5. Monitor Continuously and Prove Compliance Generate audit-ready evidence from a single source of truth and continuously monitor for drift to maintain always-on audit readiness.	

What Customers Are Saying



<p>“Policy Audit rapidly restored network compliance visibility and extended coverage beyond vulnerabilities. Standardized reports significantly reduced audit effort, letting leadership make informed, risk-based decisions with confidence”.</p> <p>Insurance & Banking Group Compliance & Security Leadership Financial Services / Insurance</p>	<p>“Audit-ready reports with clear compliance insights accelerated executive approval, streamlining the investment decision and showcasing immediate value and ROI”.</p> <p>Infrastructure Services Firm Security & Governance Team Infrastructure / Technology</p>
<p>“Audit readiness reports gave us compliance gap visibility, actionable insights, and remediation recommendations to help reduce manual effort with reports as our single source of truth”.</p> <p>Government / Public Sector IT Compliance Office Government / Public Sector</p>	<p>“With CIS benchmark checks and audit-ready evidence, we can confidently demonstrate compliance outcomes to internal and external stakeholders and prepare for audits proactively”.</p> <p>Healthcare Organization Security & Compliance Team Healthcare</p>

Customer outcomes drawn from Qualys Policy Audit success stories. Names available under reference agreements.

Proven ROI: From Visibility to Audit Readiness

90%

Less manual effort

Automated evidence collection and real-time reporting.

95%

Fewer audit failures

Gaps surfaced and closed before auditors find them.

50%

Lower audit costs

Always-ready evidence and reports, zero manual prep.

From finding misconfigurations to staying continuously audit-ready — Policy Audit turns visibility into measurable outcomes.

What Sets Policy Audit Apart

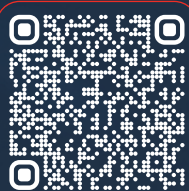
Policy Audit goes beyond traditional check-the-box tools with four differentiators that turn compliance into a continuous, risk-informed program.

Differentiator	Policy Audit
End-to-end audit automation Automate evidence collection, control mapping, and gap analysis across 100+ mandates and 500+ technologies, reducing manual effort by up to 90%.	
Risk-based prioritization with TruRisk™ Move from checklists to risk-informed compliance. The Qualys Detection Score (QDS) and TruRisk rank failing controls by business impact, asset exposure, and threat context, so teams fix what matters most first.	
Automated remediation with Audit Fix Close gaps at scale using out-of-the-box or custom CAR scripts and golden policies, with validation and rollback while maintaining hardened controls through CI/CD and ITSM workflows.	
Effortless audit-ready reporting One data collection generates multiple framework reports cross-mapped to 100+ benchmarks (CIS, NIST, PCI DSS 4.0, DORA, FedRAMP), giving auditors a unified, real-time view.	



Ready to Operationalize Continuous Audit-Readiness?

Learn how Qualys can help you prepare for your next audit.



Book a Demo

Qualys Policy Audit supports the following mandates for report generation. The mandates are categorized by region or sector for your quick reference.

Australia

- The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)
- Australian Signals Directorate Information Security Manual (ISM)
- Australian Signals Directorate - Essential Eight Maturity Model
- APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in Information and Information Technology

Brazil

- Brazilian General Data Protection Law (LGPD)

Canada

- Personal Information Protection and Electronic Documents Act
- Annex 3A (Security Control Catalogue) to IT Security Risk Management: A Lifecycle Approach (ITSG-33)

European Union (Not a Country)

- The Network and Information Systems (NIS 2 Directive) (EU) 2022/2555
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554
- General Data Protection Regulation (GDPR)
- European Union Agency for Network and Information Security

France

- ANSSI 40 Essential Measures for a Healthy Network

North America (Not a Country)

- NERC Critical Infrastructure Protection (CIP)

Qatar

- Qatar 2022 Cybersecurity Framework National Information Assurance Policy

Saudi Arabia

- Saudi Aramco SACS-002 Third Party Cybersecurity Standard
- Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework (CSF)
- Essential Cybersecurity Controls

Singapore

- Technology Risk Management (TRM) Guidelines
- Monetary Authority of Singapore (MAS) - Notice 834: Cyber Hygiene Practices

South Africa

- Protection of Personal Information Act (POPI Act)

Spain

- Royal Decree 311/2022 - Annex II (MEDIUM)
- Royal Decree 311/2022 - Annex II (HIGH)

- Royal Decree 311/2022 - Annex II (BASIC)
- Royal Decree 311/2022

United Arab Emirates (UAE)

- NESAI UAE Information Assurance Standards (IAS)

United Kingdom

- Cyber Essentials: Requirements for IT Infrastructure
- National Cyber Security Centre

United States

- NCSC Basic Cyber Security Controls (BCSC)
- US Gramm Leach Bliley Act (GLBA)
- US Food & Drug Administration (FDA)
- Criminal Justice Information Services (CJIS) Security Policy
- Control Objectives for Information and Related Technologies (COBIT)
- CERT Resilience Management Model
- California Consumer Privacy Act of 2018 (SB-1121)
- 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
- NIST 800-53 (Special Publication)
- New York State Department of Financial Services 23 NYCRR 500
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Microsoft Cloud Security Benchmark
- IRS Publication 1075
- Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C:1996
- Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline
- Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Acquisition Regulation (FAR)
- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008-7012
- Cybersecurity Maturity Model Certification (CMMC) Level 5
- Cybersecurity Maturity Model Certification (CMMC) Level 4
- Cybersecurity Maturity Model Certification (CMMC) Level 3
- Cybersecurity Maturity Model Certification (CMMC) Level 2
- Cybersecurity Maturity Model Certification (CMMC) Level 1
- Cybersecurity Maturity Model Certification (CMMC)
- US Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2
- US Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1
- The NIST Cybersecurity Framework (CSF)

- Sarbanes-Oxley Act: IT Security
- NIST Special Publication 800-171
- NIST Cyber Security Framework (CSF)
- NIST AI 100-1 - Artificial Intelligence Risk Management Framework, January 2023
- CSA 405(d) - Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations
- CSA 405(d) - Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations

Global

- SWIFT Customer Security Controls Framework - Customer Security Programme v2024
- SWIFT Customer Security Controls Framework - Customer Security Programme v2023
- SWIFT Customer Security Controls Framework - Customer Security Programme v2021
- SWIFT Customer Security Controls Framework - Customer Security Programme v2019
- Secure Controls Framework (SCF)
- Payment Card Industry Data Security Standard (PCI-DSS) v4.0

- Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1
- ISO/IEC 27001:2022
- ISO/IEC 27001:2013
- Critical Systems Cybersecurity Controls
- Cloud Controls Matrix (CCM)
- CIS Controls v8.1
- CIS Controls v8.0
- CIS Controls

India

- Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)
- IRDAI Guidelines On Information and Cyber Security for Insurers

Malaysia

- Risk Management in Technology (RMiT)

New Zealand

- New Zealand Information Security Manual (NZISM)

Qualys Policy Audit extends support to over 500 technologies, including major platforms such as Windows, Unix, Mac, databases, and network devices. It also covers a wide array of specialized and exotic technologies that fall outside the scope of standard CIS benchmarks, ensuring comprehensive security and compliance coverage across diverse IT environments.

Some of the technologies supported by Qualys Policy Audit:

Applications

- VMware Horizon
- Microsoft .NET Framework
- Microsoft Exchange Server
- Skype for Business Server
- SharePoint Server

Container Security

- Docker CE/EE
- Kubernetes

Databases

- Apache Cassandra
- Apache Hadoop
- IBM DB2 z/OS
- Redis
- SAP Adaptive Server Enterprise
- IBM z/OS Security Server
- RACF
- HP Safeguard

Network Devices

- Extreme Networks VOSS
- Cisco FTD
- Nokia SROS
- Brocade Fabric
- Ivanti Connect Secure
- IBM Datapower Gateway
- A10 Advanced Core OS
- AudioCodes Session

Border Controller

- Aruba EdgeConnect OS
- Citrix NetScaler
- Riverbed SteelHead RiOS
- Cisco SD-WAN
- Cisco UCS Manager
- Riverbed SteelHead Interceptor
- Gigamon GigaVUE-OS
- INFOBLOX NIOS

Security Applications

- Windows 2019 Server Certification Authority

Operating Systems

- CBL-Mariner Linux
- Google Container Optimized OS
- Red Hat Enterprise Linux
- CoreOS
- Checkpoint MDS
- Virtuozzo Linux
- Kali GNU/Linux
- Microsoft Azure Linux
- Alibaba Cloud Linux
- CloudLinux OS
- CentOS Stream
- VMware Photon OS
- Bottlerocket OS
- IBM VIOS
- IBM i 7.x
- Azure Stack HCI
- Windows 2025 Server

Printers

- Xerox VersaLink
- HP Printers
- Samsung Printers

Storage

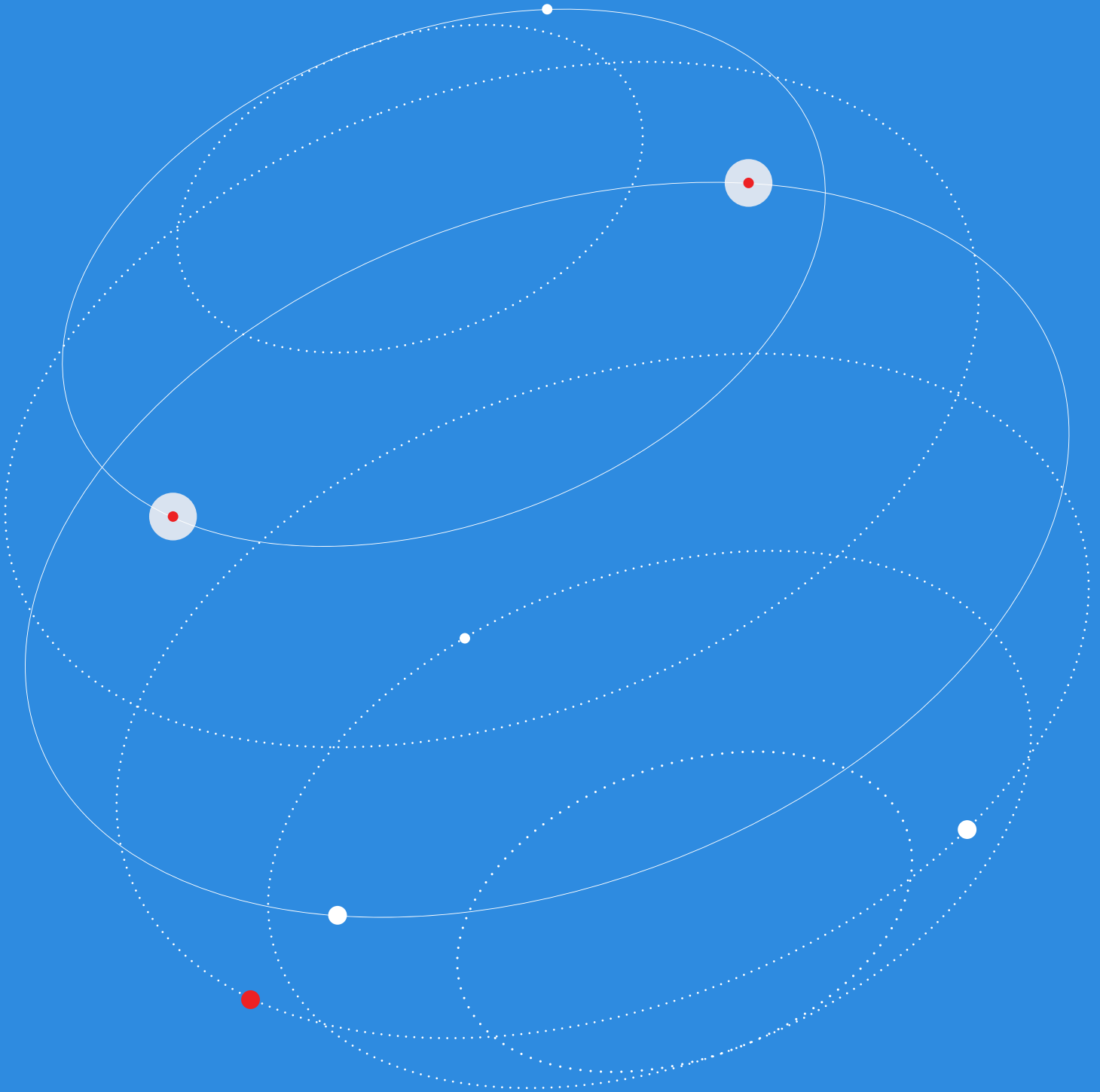
- Data Domain OS
- NetApp Data ONTAP

Virtualization

- Citrix
- XenApp/XenDesktop
- Citrix Hypervisor
- Red Hat OpenShift Container Platform

Web Services

- IBM WebSphere
- MQ Nginx
- VMware vFabric Web Server
- Oracle HTTP Server



About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit qualys.com