



Audit Readiness Report

for NIST 800-53 (Special Publication)

Generated for **Sales Qualys Corporate Demo**

Oct 08, 2026

Powered By



01

Audit Readiness Summary

Audit Readiness for NIST 800-53 (Special Publication)

Top 5 Failing NIST 800-53 (Special Publication) requirements

03

Recommendations

Recommended Remediation Actions

Risk Reduction Recommendations

Best Practices Recommendations

02

Audit Insights

Top Failing Controls in NIST 800-53 (Special Publication) Requirements

Total Failed controls by Criticality

Total Failed controls by QDS Score

Asset Landscape

Asset Criticality

04

Appendix

NIST 800-53 (Special Publication) requirements

Top Mitre Tactics

Top 5 failing Controls

Top 5 Failing Ransomware Controls

Top 5 failing MITRE Controls

Scope of Report

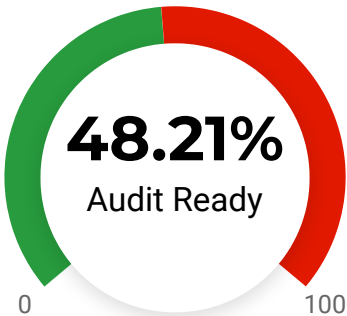
SCA vs Policy Audit

The purpose of the Audit Readiness Summary report is to present an overview of the organization's audit status and preparedness. It highlights alignment with various compliance frameworks, control requirements, and internal policies while identifying potential audit gaps. Each section provides a clear summary of key findings, audit requirements, gap analysis, relevant metrics, and actionable recommendations to strengthen audit readiness and close identified gaps.

Audit Readiness for NIST 800-53 (Special Publication)

Selected Asset Tags:

- Internet Facing Assets
- PCD_Tomcat
- Cloud Public IP
- Type: Domain Controller
- Department: Finance





Total Assets
2267



Unique Controls
7613

 Audit Gaps

50.33%
1516.2k of 3012.3k
Total Audit Gaps

45.95%
696.7k of 1516.2k
Critical Audit Gaps

Critical

 Asset Summary

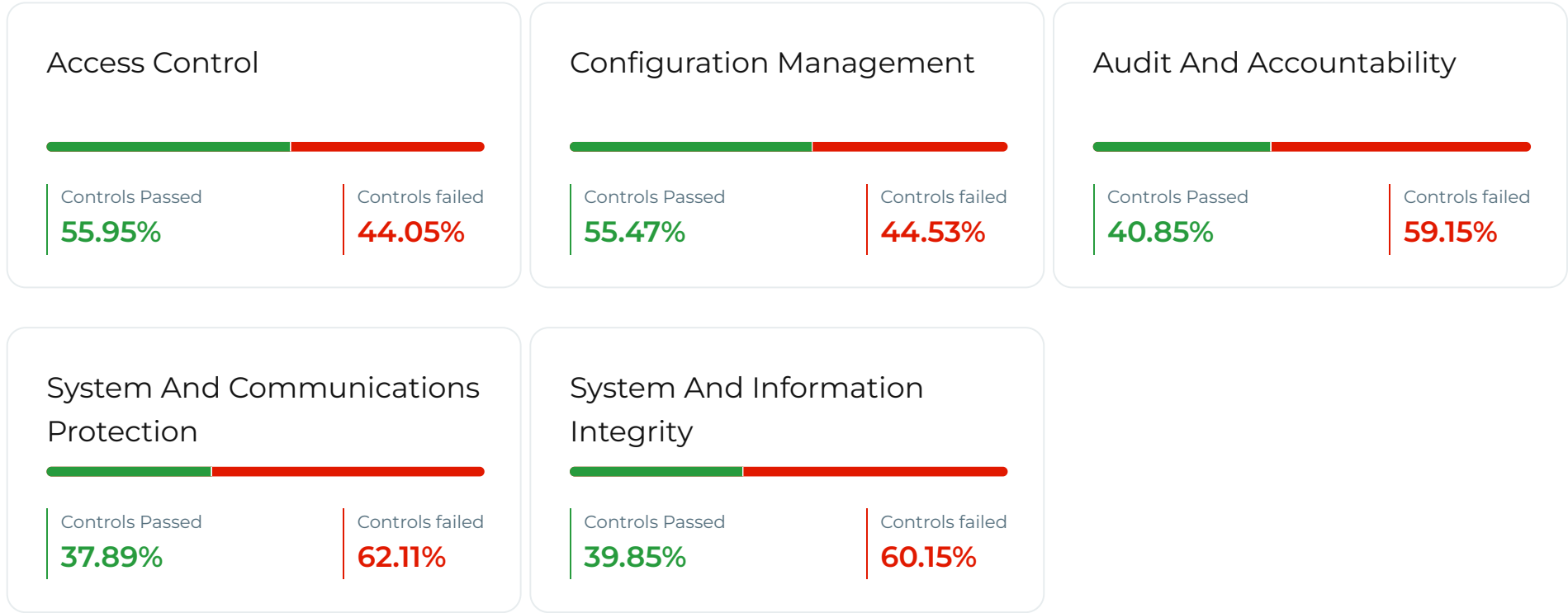
92.59%
2.1k of 2.3k
Assets with Audit Gaps

99.90%
2.1k of 2.1k
Assets with Critical Audit Gaps

Critical

Top 5 Failing NIST 800-53 (Special Publication) requirements

Requirements contributing to the audit readiness for NIST 800-53 (Special Publication)



Audit Insights : Top Failing Controls in NIST 800-53 (Special Publication) Requirements

Prioritise and eliminate the audit gaps by top failing NIST 800-53 (Special Publication) requirements

AC Access Control	CM Configuration Management	AU Audit And Accountability
<div>  2196 - Current list of Groups and User Accounts granted the 'Deny Access to this com... <div>1.6k Asset Instance</div> </div> <div>  2199 - Current list of Groups and User Accounts granted the 'Deny log on locally' right <div>1.6k Asset Instance</div> </div> <div>  2197 - Current list of Groups and User Accounts granted the 'Deny logon as a batch j... <div>1.6k Asset Instance</div> </div>	<div>  11281 - Status of the 'SMB v1' protocol for LanManServer services on Windows <div>1.6k Asset Instance</div> </div> <div>  9008 - Status of the 'Do not display network selection UI' setting <div>1.5k Asset Instance</div> </div> <div>  3919 - Status of the 'Turn off printing over HTTP' service <div>1k Asset Instance</div> </div>	<div>  4494 - Status of the audit setting 'Sensitive Privilege Use' (advanced audit setting) <div>1.6k Asset Instance</div> </div> <div>  4473 - Status of the audit setting 'IPsec Driver' (advanced audit setting) <div>1.6k Asset Instance</div> </div> <div>  4497 - Status of the audit setting 'Process Creation' (advanced audit setting) <div>1.6k Asset Instance</div> </div>

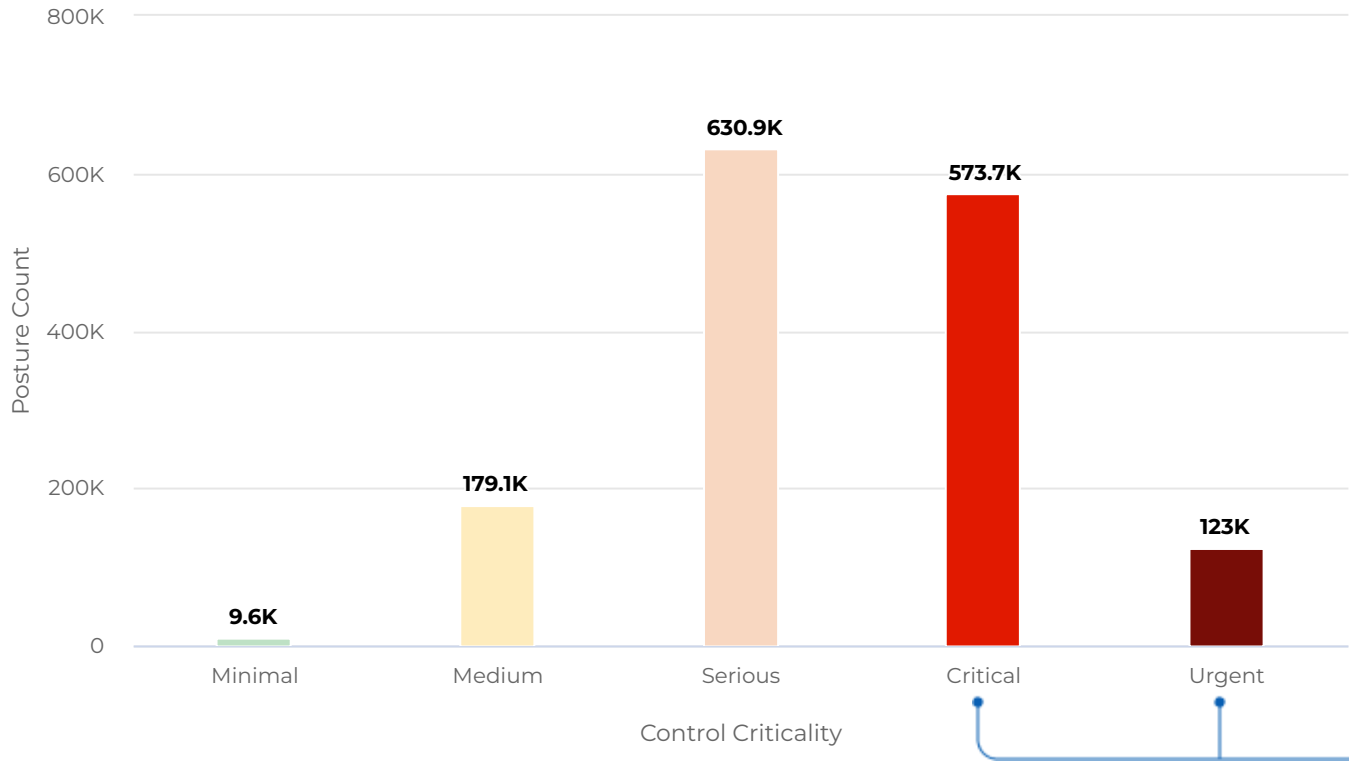


Pro Tip

Improve your **NIST 800-53 (Special Publication) audit readiness by 1%** by remediating the top failing controls!

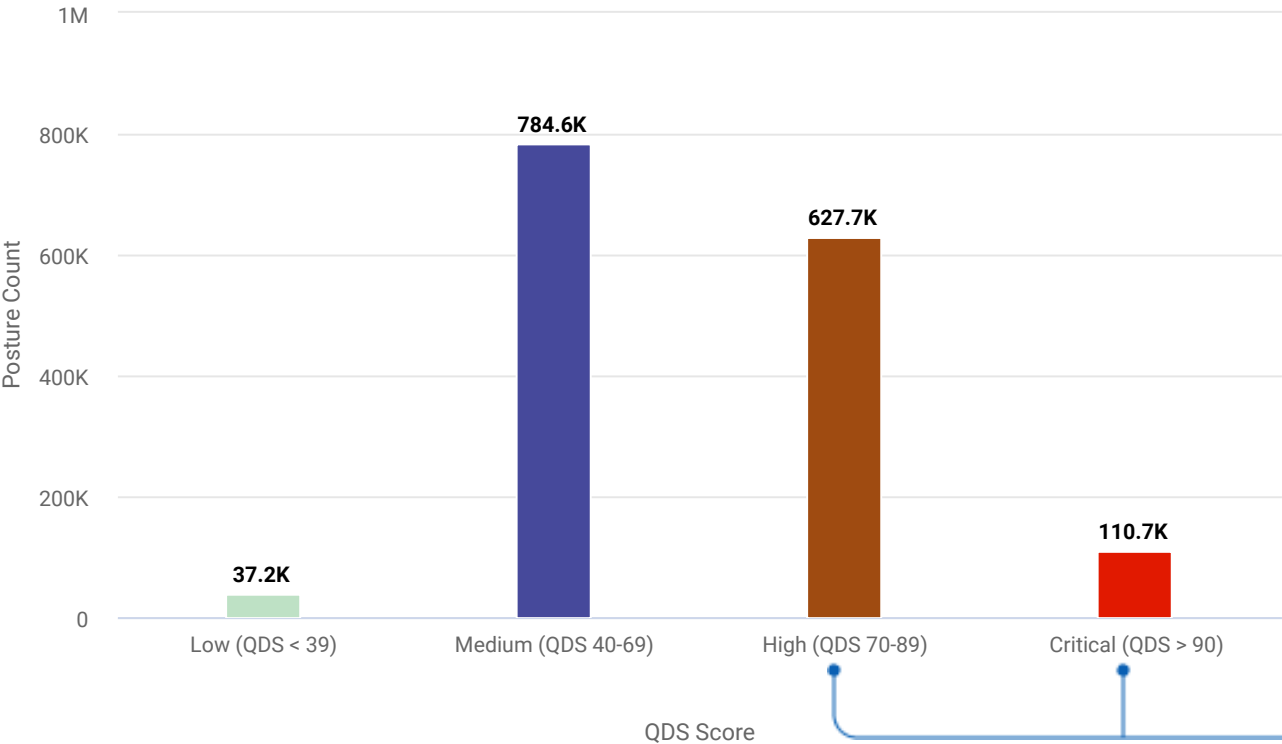
Audit Insights : Total Failed controls by Criticality

Prioritize and eliminate audit gaps by criticality for NIST 800-53 (Special Publication)



Total Failed controls by QDS Score

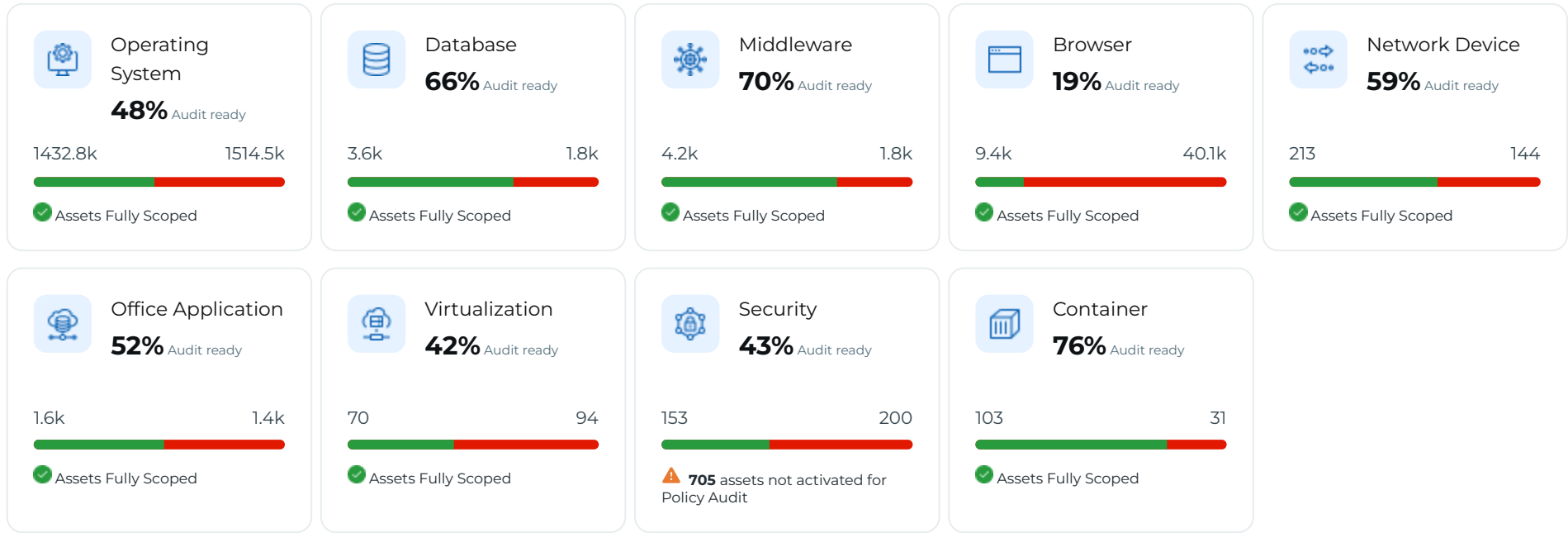
Audit readiness is at **48%** for NIST 800-53 (Special Publication)



Focus on **738.3k (24%)** misconfigurations by leveraging QDS instead of addressing all failures.

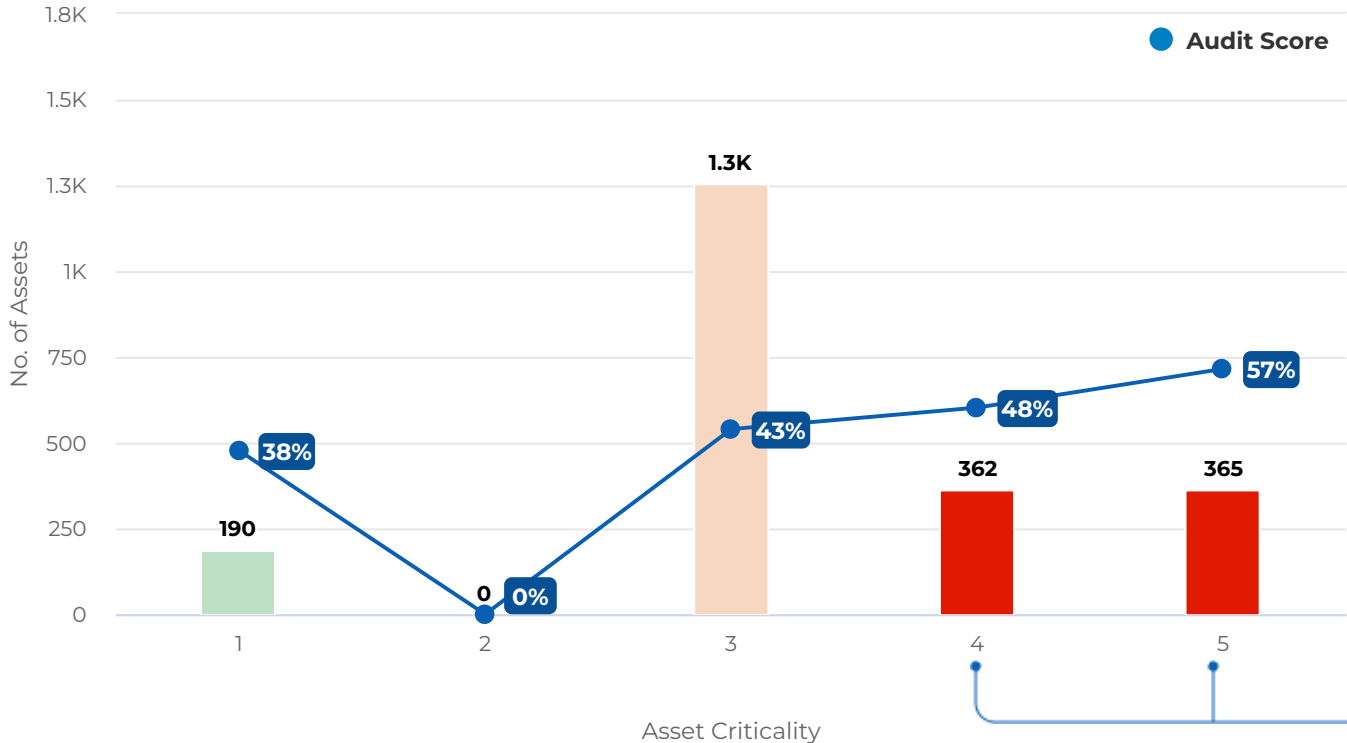
Audit Insights : Asset Landscape

Understand audit readiness across your asset inventory.



Audit Insights : Asset Criticality

Audit readiness is at **48%** for NIST 800-53 (Special Publication)




 Prioritize **727** critical assets when addressing misconfigurations to minimize exposure and protect key business functions.

Recommended remediation actions

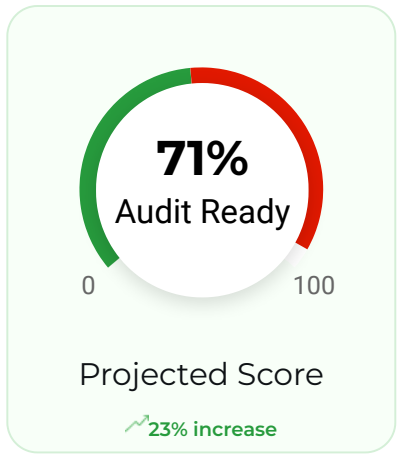
Audit readiness is at **48%** for NIST 800-53 (Special Publication)



- 

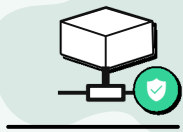
1%
NIST 800-53 (Special Publication) audit readiness boost can be achieved by remediating the **top failing controls** of NIST 800-53 (Special Publication) Requirements.
- 

23% 
boost in audit readiness can be achieved by prioritizing **718.2k critical and urgent** audit gaps.



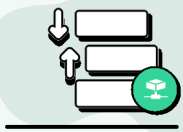
Risk Reduction Recommendations

Audit readiness is at **48%** for NIST 800-53 (Special Publication)



128.2k Assets

Are not activated for Policy Audit. As per NIST 800-53 (Special Publication) requirement, all in-scope assets should be continuously scanned to ensure audit readiness.



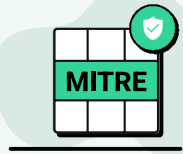
727 Critical Assets

To prioritize when addressing misconfigurations to minimize exposure and safeguard key business functions!



37.60% (586.7k out of 1560.2k)

Gaps are linked to ransomware-related risks. Prioritise these gaps to strengthen your security posture!

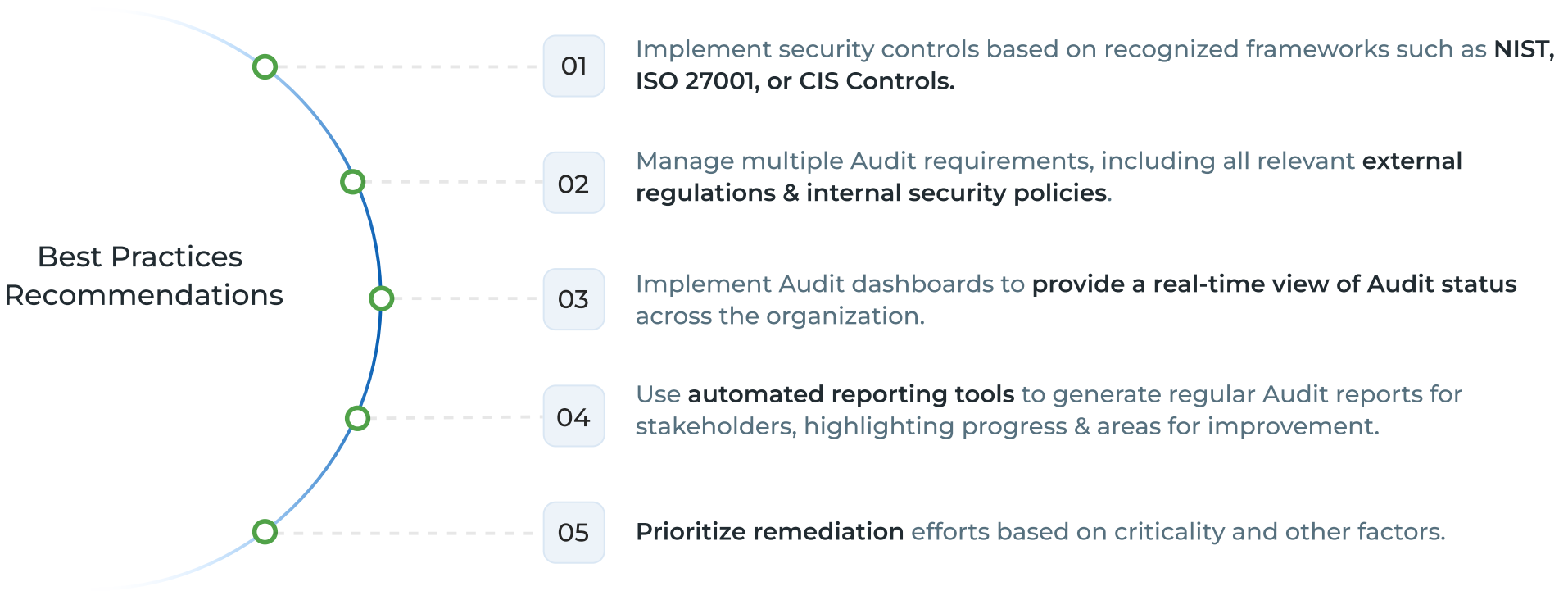


77.57% (1210.2k out of 1560.2k)

Gaps are mapped to the MITRE framework. Focusing on these can enhance your threat defence strategy!

Best Practices Recommendations

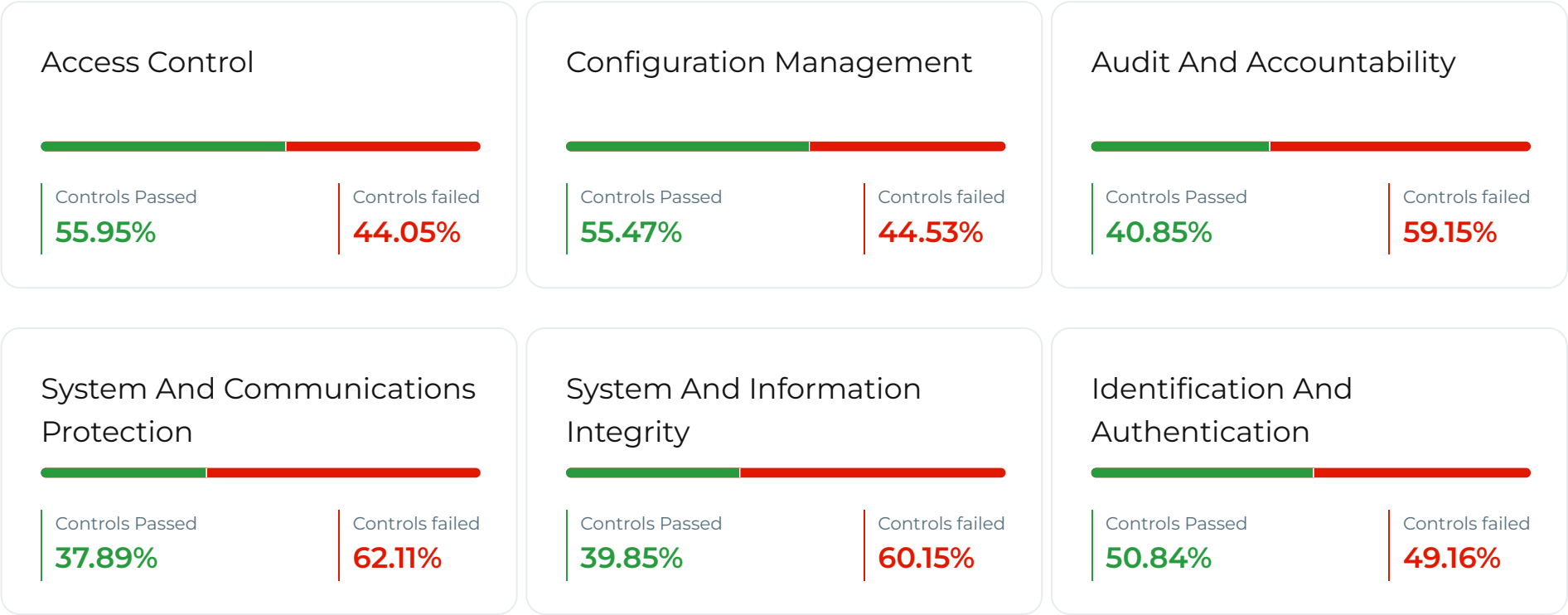
Here are some suggestions aligned with industry-wide best practices that you might consider implementing to enhance your Audit posture



Appendix

NIST 800-53 (Special Publication) requirements

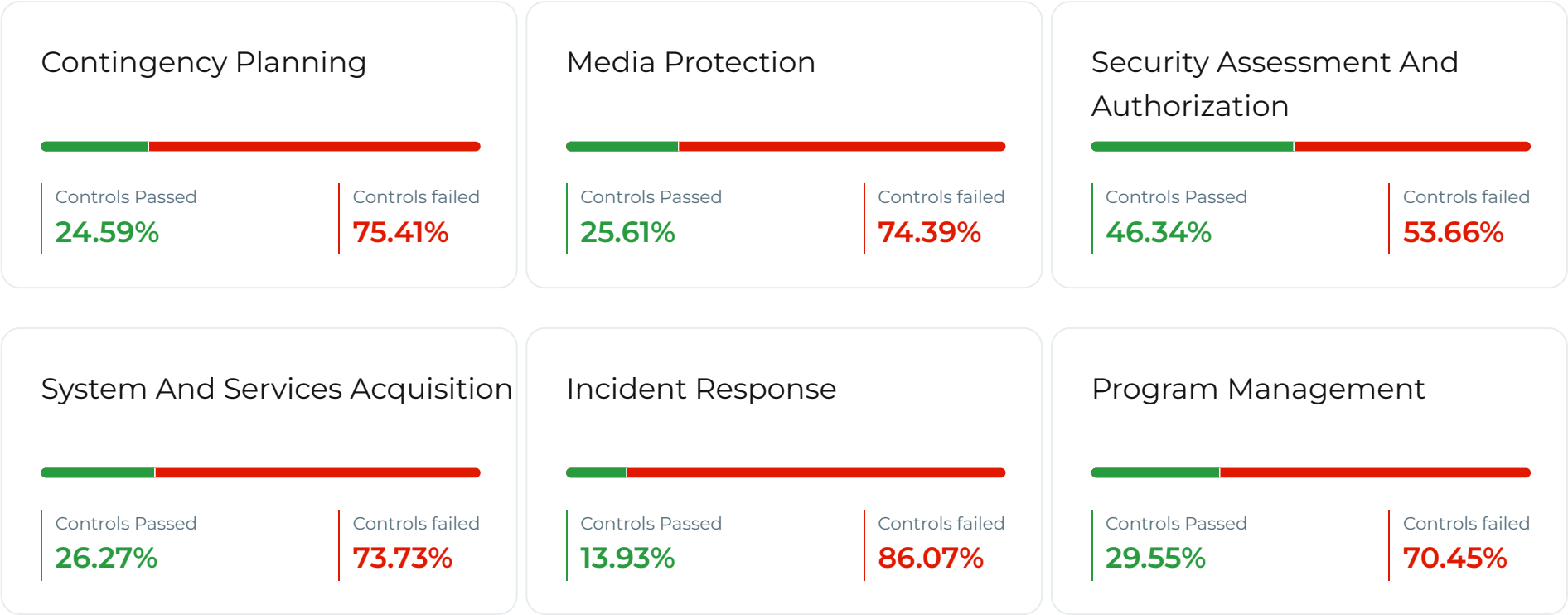
Audit readiness is at **48%** for NIST 800-53 (Special Publication)



Continued on next page

NIST 800-53 (Special Publication) requirements

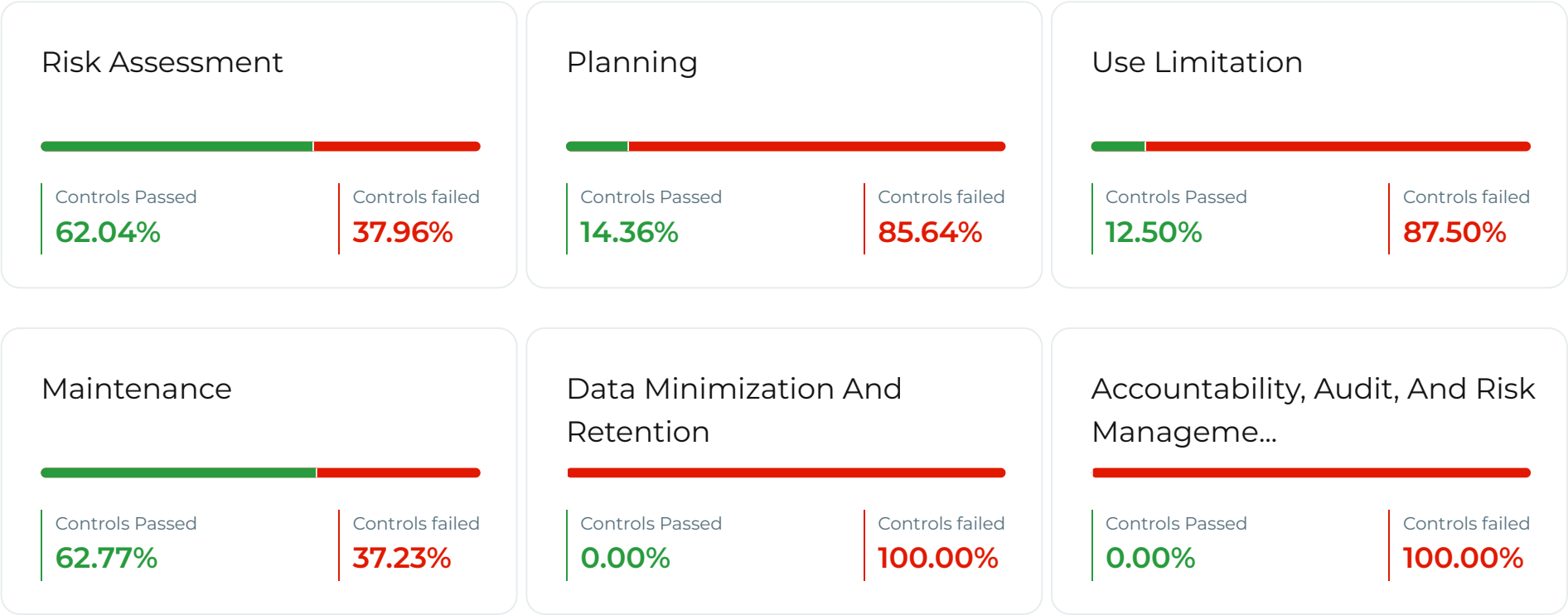
Audit readiness is at **48%** for NIST 800-53 (Special Publication)



Continued on next page

NIST 800-53 (Special Publication) requirements

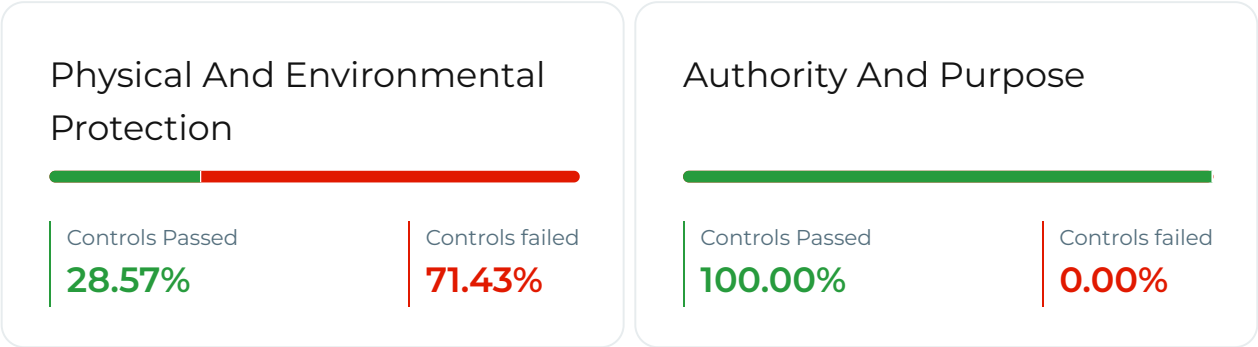
Audit readiness is at **48%** for NIST 800-53 (Special Publication)



Continued on next page

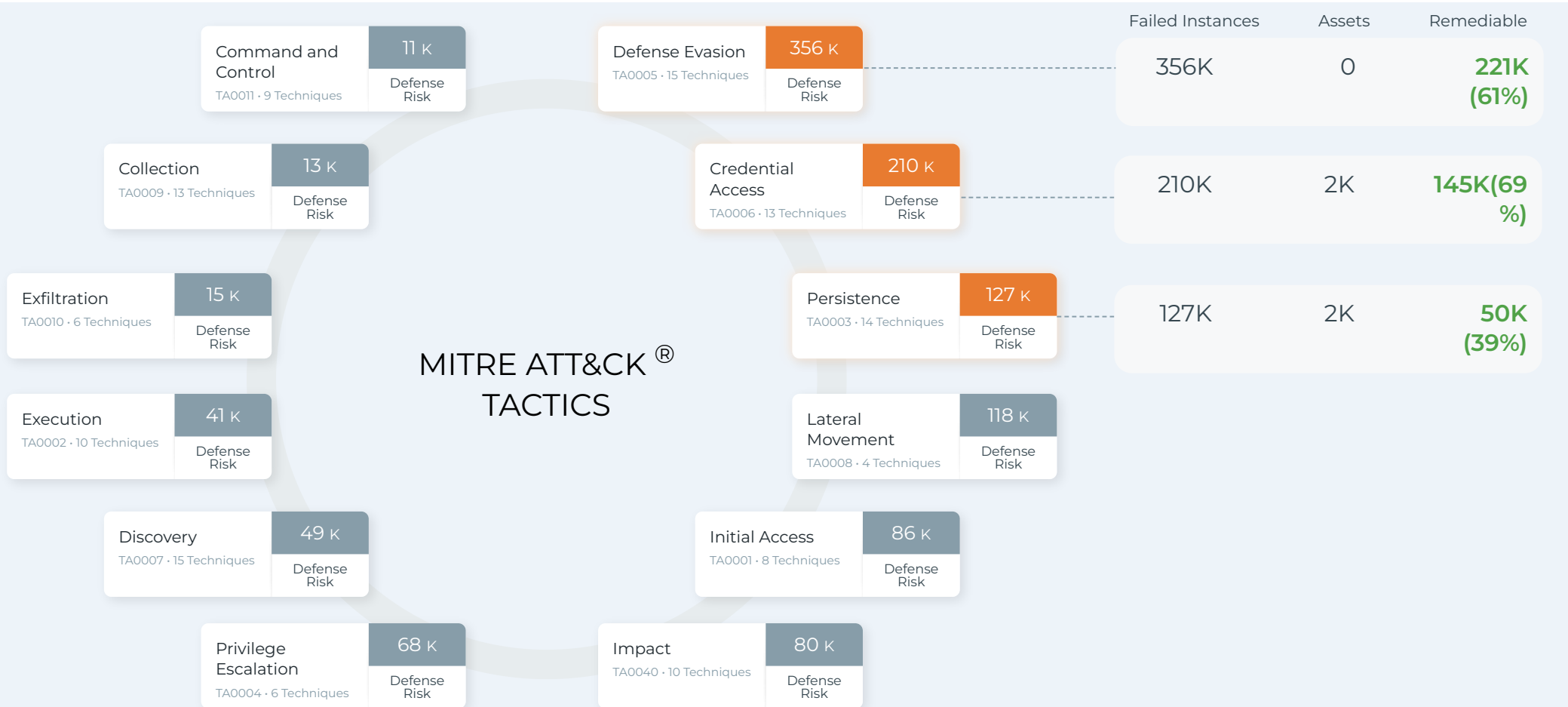
NIST 800-53 (Special Publication) requirements

Audit readiness is at **48%** for NIST 800-53 (Special Publication)



Top MITRE Tactics Mapped to NIST 800-53 (Special Publication)

Provides MITRE ATT&CK metrics view of all the misconfiguration detections in your organization.



Top 5 failing Controls

Audit readiness is at **48%** for NIST 800-53 (Special Publication)

CID	Statement	Criticality	QDS	Asset	Failed Instances ⌵	Audit Readiness
2196	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	CRITICAL	86	1.65K	6.07K	<div><div></div></div> 11%
2199	Current list of Groups and User Accounts granted the 'Deny log on locally' right	CRITICAL	86	1.64K	5.84K	<div><div></div></div> 10%
2197	Current list of Groups and User Accounts granted the 'Deny logon as a batch job' right	CRITICAL	86	1.65K	5.63K	<div><div></div></div> 11%
2391	Current list of Groups and User Accounts granted the 'Allow log on locally (SeInteractiveLogonRight)' right	URGENT	100	1.64K	5.49K	<div><div></div></div> 13%
2399	Current list of Groups and User Accounts granted the 'Restore files and directories (SeRestorePrivilege)' right	URGENT	100	1.63K	5.36K	<div><div></div></div> 12%

Top 5 Failing Ransomware Controls

Audit readiness is at **48%** for NIST 800-53 (Special Publication)

CID	Statement	Criticality	QDS ↓	Asset	Audit Readiness	Qualys Remediable
2391	Current list of Groups and User Accounts granted the 'Allow log on locally (SeInteractiveLogonRight)' right	URGENT	100	1.64K	13%	✗
2399	Current list of Groups and User Accounts granted the 'Restore files and directories (SeRestorePrivilege)' right	URGENT	100	1.63K	12%	✗
2196	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	CRITICAL	86	1.65K	11%	✗
2199	Current list of Groups and User Accounts granted the 'Deny log on locally' right	CRITICAL	86	1.64K	10%	✗
2197	Current list of Groups and User Accounts granted the 'Deny logon as a batch job' right	CRITICAL	86	1.65K	11%	✗

Top 5 failing MITRE Controls

Audit readiness is at **48%** for NIST 800-53 (Special Publication)

CID	Statement	Criticality	QDS	MITRE Tactics & Techniques	Asset ↓	Audit Readiness
2196	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	CRITICAL	86	TA0008: T1021	1.65K	11%
2197	Current list of Groups and User Accounts granted the 'Deny logon as a batch job' right	CRITICAL	86	TA0002: T1053	1.65K	11%
2391	Current list of Groups and User Accounts granted the 'Allow log on locally (SeInteractiveLogonRight)' right	URGENT	100	TA0003: T1098	1.64K	13%
2199	Current list of Groups and User Accounts granted the 'Deny log on locally' right	CRITICAL	86	TA0005: T1562	1.64K	10%
2399	Current list of Groups and User Accounts granted the 'Restore files and directories (SeRestorePrivilege)' right	URGENT	100	TA0003: T1098	1.63K	12%

Included Policies

Audit readiness is at **48%** for NIST 800-53 (Special Publication)

10 of 387 policies displayed (+377 more)

Title	Created by	Created on	Evaluated on ↓
PCD_DISA Security Technical Implementation Guide (STIG) for Windows Server 2016 DC, V1R12 v.3.0	Anu Kapil - CORP-Demo	02/09/2021	10/08/2026
SB_AuditFix_CIS Benchmark for Microsoft Windows Server 2022, v5.1.0 [Automated and Manual, Level 1 - Member Server, Level 2 - Member Server, Next Generation Windows Security - Member Server]	Shahista Baig - CORP-Demo	09/29/2026	10/08/2026
Minimum Security Hygiene for Windows Remote Endpoints v.2.0	Qualys MAIN PM-SETUP ACCOUNT	04/09/2020	10/08/2026
PCD_DISA Security Technical Implementation Guide (STIG) for Windows Server 2019 MS, V1R5 v.2.0	Anu Kapil - CORP-Demo	02/09/2021	10/08/2026
NERC Critical Infrastructure Protection (CIP)	Mohammad Arif Baig - CORP-Demo	06/10/2026	10/08/2026
Royal Decree 311/2022 - Annex II (HIGH) Policy for Windows	Shekhar Rana CORP-Demo	07/29/2025	10/08/2026
PC Demo CIS Benchmark for Microsoft IIS 10, v1.1.1 [Scored and Not Scored, Level 1 and Level 2] v.2.0	Corey Smith - CORP-Demo	08/20/2020	10/08/2026
CIS Benchmark for Azure Compute Microsoft Windows Server 2022 v1.0.0 [Automated and Manual, Level 1 Domain Controller] demo	Shekhar Rana CORP-Demo	04/09/2025	10/08/2026
CIS Benchmark for Microsoft Windows Server 2022, v3.0.0, [Automated and Manual, Level 1 - Member Server, Level 2 - Member Server] - Infy	Shekhar Rana CORP-Demo	04/30/2025	10/08/2026
PCD_Security Hygiene Controls for Reducing Risk of SolarWinds Orion Compromise (SUNBURST/Solorigate) v.1.0	Anu Kapil - CORP-Demo	02/11/2021	10/08/2026

Scope of Report

Audit readiness is at **48%** for NIST 800-53 (Special Publication)

Selected Asset Tags (30 of 637 tags displayed)

Internet Facing Assets

PCD_Tomcat

Cloud Public IP

Type: Domain Controller

Department: Finance

BusinessApp: Sales Portal

BusinessApp: App007

BusinessApp: Imaging Data

BusinessApp: Customer Support Portal

BusinessApp: Service Catalog

Production PCI Assets

Network LBs

WYQ_Demo

IP_Tag

RegreSSHion - all QIDs

PCI

LinuxHostname

BusinessApp: E-Commerce

BusinessApp: Finance

BusinessApp: Accounts Receivables

BusinessApp: Website1

ALL_IFA

Eliminate_Tag

critical_assets

DJ - Assets

Finance

BusinessApp: Reporting Services

BusinessApp: Spotlrix

Critical Privilege Assets

code2cloud

SCA vs Policy Audit

Choose the right security solution for your needs

Feature	SCA Free	Policy Audit Recommended
Compliance Assessments	⚠ Basic CIS configuration checks	✓ Advanced Compliance with 1200 policies & 20K controls
Onboarding and Operationalization	✗ Manual setup required	✓ Quick automated setup
Processes and Remediation	⚠ Manual processes, ticketing, remediation	✓ Automated remediation with out-of-the-box policies
Compliance Reporting	✗ No customisation	✓ Flexible and customisation
Auto-Discovery	✗ No auto-discovery	✓ Automated discovery & OCA coverage
Framework Reporting	✗ No frameworks reports	✓ Detailed mandate-based reporting (NIST, PCI DSS, ISO, FedRAMP)
Dashboard	⚠ Basic and non-customizable	✓ Real-time and customizable
TruRisk Integration	✗ Not integrated	✓ Integrated with Qualys TruRisk
Prioritization	✗ No risk based prioritization	✓ Prioritization based on QDS, MITRE tactics, and techniques
Time and Cost Efficiency	✗ High effort and cost	✓ 98% less time and cost

⚠ **Automated remediation** with the AuditFix add-on using out-of-the-box or custom-defined scripts across **SCA** and **Policy Audit**.

Powered By



The purpose of the Audit Readiness Summary report is to present an overview of the organization's audit status and preparedness. It highlights alignment with various compliance frameworks, control requirements, and internal policies while identifying potential audit gaps. Each section provides a clear summary of key findings, audit requirements, gap analysis, relevant metrics, and actionable recommendations to strengthen audit readiness and close identified gaps.

Copyright © 2026, Qualys and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Qualys is registered trademarks of Qualys and/or its affiliates. Other names may be trademarks of their respective owners.