



www.getastra.com

Compliance Mapping Report

The compliance standards for this PDF were:
SOC 2, GDPR, ISO 27001, PCI DSS, HIPAA, DORA

Userforge

Report Generated On **September 24, 2026**

About This Report

Astra assesses your applications and infrastructure for security vulnerabilities through a combination of manual penetration testing, automated dynamic scanning (web and API), cloud configuration review, and mobile application static analysis, depending on the scans included in this report.

Many of the vulnerability classes we identify map directly to specific technical controls within compliance frameworks such as SOC 2, ISO 27001, GDPR, HIPAA, PCI DSS, and DORA. This report lists each finding under the standards whose controls it touches, so you can see where your current technical posture intersects with your compliance obligations.

This report is not a certification, attestation, or audit of compliance with any standard listed. Only accredited auditors or qualified assessors can issue those. Astra maps technical findings from the scans included in this report to relevant controls, and it does not evaluate organizational, physical, or workforce controls (e.g., policies, training, vendor management, physical access), nor the design or operating effectiveness of the controls themselves.

Astra is a PCI Approved Scanning Vendor (ASV), CREST-accredited, and CERT-In empanelled. Reports issued under those accreditations are delivered separately and are not substituted by this document.

Assessment Duration and Dates

Scan Mode	Scan/Pentest Name	Name	Start At
Auto Pentest	Auto Pentest - 23 Sept 26	base44 (Website Pentest)	23rd Sep 2026

Control-Aligned Findings

SOC 2

SOC 2 reports are issued against the AICPA Trust Services Criteria by accredited CPA firms. The Common Criteria (CC series) cover security and form the baseline of every SOC 2 report.

We surface technical vulnerabilities that touch the logical-access and system-operations criteria such as authentication and authorization flaws, boundary-protection issues, transmission security gaps, and externally observable configuration weaknesses. Change management process, risk assessment, control environment, and other policy- and process-level criteria are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

Findings from this scan that map to SOC 2 controls:

No	Title	Severity	Status
1	Unauthenticated Full CRUD Access on Multiple Sensitive Entity Endpoints (Team, AuditLog, ApiToken, Invitation, ApprovalRequest)	Critical	Unsolved
2	Unauthenticated Privilege Escalation via Invitation Creation with Superadmin Role	Critical	Unsolved
3	Unauthenticated Approval Workflow Bypass via Direct Status Manipulation	Critical	Unsolved
4	Unauthenticated CRUD Operations on Profile Entity Allows Superadmin Account Creation	Critical	Unsolved
5	Unauthenticated User Creation with Arbitrary Roles via Entity API Bypassing Registration Flow	Critical	Unsolved
6	Broken Access Control - Unauthenticated Entity API Read/Write Access	High	Unsolved
7	NoSQL Injection via q Parameter on Profile Entity Endpoint	High	Unsolved
8	Unauthenticated Profile Entity Exposes User PII Bypassing User Entity Auth Protection	High	Unsolved
9	Unauthenticated Password Change Endpoint Bypasses Session Authentication	High	Unsolved
10	Unauthenticated Audit Log Injection via Mass Assignment	High	Unsolved
11	OTP Brute-Force via Attempt Counter Reset on Resend Enables Account Verification Bypass	High	Unsolved
12	Mass Assignment on Profile Role Field Enables Unauthenticated Privilege Escalation	High	Unsolved
13	Unauthenticated Entity Write Access via CORS Wildcard Enables Cross-Origin Data Tampering	High	Unsolved
14	Unauthenticated CRUD Access to AuditLog API	High	Unsolved
15	Unauthenticated PII Exposure via Entity API - Invitation and Team Listings	High	Unsolved
16	Unauthenticated Record Deletion on ApprovalRequest Entity	High	Unsolved
17	Unauthenticated Mass Assignment on User Entity - Admin Role Injection	High	Unsolved
18	Unauthenticated User Creation with Role Mass Assignment via Entity API	High	Unsolved
19	Unauthenticated Mass Data Exposure on ApprovalRequest Entity	High	Unsolved

No	Title	Severity	Status
20	Unauthenticated Cross-Origin Data Exfiltration via CORS Wildcard and Missing Authentication	High	Unsolved
21	Unauthenticated Invitation Record Modification and Deletion	High	Unsolved
22	Race Condition TOCTOU on Concurrent Approval Request Processing	High	Unsolved
23	Unauthenticated Audit Log Tampering Enables Evidence Destruction and False Trail Planting	High	Unsolved
24	Stored XSS via Team Name and Description Fields	High	Unsolved
25	Unauthenticated Entity CRUD with Role Mass Assignment on Profile Entity	High	Unsolved
26	Stored XSS via Invitation Entity email Field with JWT Exfiltration Chain	High	Unsolved
27	Unauthenticated WebhookConfig Endpoint Exposes 83 Configurations Including Internal Infrastructure URLs	High	Unsolved
28	OTP Attempt Limit Bypass via Race Condition (TOCTOU) on Verify-OTP Endpoint	High	Unsolved
29	Broken Access Control - Unauthenticated CRUD on SecurityAlert Entity API	Medium	Unsolved
30	Wildcard CORS Configuration Allows Any Origin to Access Sensitive API Endpoints	Medium	Unsolved
31	Mass Assignment Enables Unauthenticated Superadmin Role Escalation	Medium	Unsolved
32	Unauthenticated Cross-Origin Analytics Log Injection via IDOR on App-ID	Medium	Unsolved
33	User Enumeration via Differential Error Messages on Login Endpoint	Medium	Unsolved
34	X-Frame-Options Header Not Set	Medium	Unsolved
35	Wildcard CORS Policy Enables Cross-Origin Audit Log Manipulation	Medium	Unsolved
36	Missing Rate Limiting on Write Operations (POST/PUT)	Medium	Unsolved
37	Race Condition - Duplicate Team Resource Creation via Concurrent Requests	Medium	Unsolved
38	Stored XSS via Unvalidated AuditLog Entity Fields	Medium	Unsolved
39	Wildcard CORS Policy on Entity API Enables Cross-Origin Exploitation	Medium	Unsolved
40	Insecure JWT Token Storage in localStorage	Medium	Unsolved
41	No Rate Limiting or Uniqueness Constraints Enables Unlimited Duplicate Entity Creation	Medium	Unsolved
42	Unauthenticated Analytics Event Injection with No Input Sanitization	Medium	Unsolved
43	Mass Assignment - Arbitrary member_count Manipulation on Team Entity	Medium	Unsolved
44	User Enumeration via Login Timing Side-Channel and Registration ID Reuse	Medium	Unsolved
45	Open Redirect via from_url Parameter in OAuth Login Flow	Medium	Unsolved
46	Stored CSV Formula Injection via Unauthenticated Entity Creation	Medium	Unsolved
47	IDOR via Unauthenticated App-Log ID Enumeration on Login Endpoint	Medium	Unsolved
48	Lack of Account Lockout Enables Credential Brute-Force	Medium	Unsolved
49	Unauthenticated CRUD Access on SecurityAlert Entity	Medium	Unsolved
50	User Enumeration via Verify-OTP Endpoint	Medium	Unsolved
51	Broken Object-Level Authorization - Unauthenticated Profile Entity CRUD	Medium	Unsolved
52	Wildcard CORS Policy Enables Cross-Origin Data Theft and Modification on Entity APIs	Medium	Unsolved
53	Unauthenticated PII Exposure of Internal Employee Email Addresses	Medium	Unsolved
54	Timing-Based User Enumeration via Registration Endpoint	Low	Unsolved

No	Title	Severity	Status
55	Sensitive Data Exposure via Missing Cache-Control Headers on /teams Page and API	Low	Unsolved
56	Server Technology Stack Fingerprinting via Response Headers	Low	Unsolved
57	Missing Content-Security-Policy Header Enables Unrestricted Script Execution	Low	Unsolved
58	Weak Password Policy Accepts Simple Passwords Without Complexity Requirements	Low	Unsolved
59	Unauthenticated Build Metadata Disclosure via Health Endpoint	Low	Unsolved
60	Full Platform API Specification Exposed on App Subdomain Without Authentication	Low	Unsolved
61	Missing Authentication on Page View Logging Endpoint	Low	Unsolved
62	PII Disclosure	Low	Unsolved
63	Missing Content-Security-Policy Header	Low	Unsolved
64	CORS Wildcard Misconfiguration on /api/app-logs/ Endpoints	Low	Unsolved
65	Missing X-Frame-Options and Content-Security-Policy Headers Enabling Clickjacking on Login Page	Low	Unsolved
66	Missing X-Frame-Options and CSP frame-ancestors Headers Enabling Iframe Embedding	Low	Unsolved
67	Potential User Info Leak - Multiple User Emails Found	Info	Unsolved

GDPR

The EU General Data Protection Regulation governs the processing of EU residents' personal data and requires appropriate technical and organisational measures to protect it.

We surface technical vulnerabilities that, depending on the data handled by the affected component, can result in personal-data exposure: broken access control on user-data routes, weak or missing transport encryption, PII leakage through verbose errors or debug endpoints, insecure cookie attributes on identity-bearing cookies, and cross-origin misconfigurations on endpoints serving user data. Lawful basis, consent management, data subject rights workflows, and other organisational requirements are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

Findings from this scan that map to GDPR controls:

No	Title	Severity	Status
1	Unauthenticated CRUD Operations on Profile Entity Allows Superadmin Account Creation	Critical	Unsolved
2	Broken Access Control - Unauthenticated Entity API Read/Write Access	High	Unsolved
3	NoSQL Injection via q Parameter on Profile Entity Endpoint	High	Unsolved
4	Mass Assignment on Profile Role Field Enables Unauthenticated Privilege Escalation	High	Unsolved
5	Unauthenticated PII Exposure via Entity API - Invitation and Team Listings	High	Unsolved
6	Unauthenticated Mass Assignment on User Entity - Admin Role Injection	High	Unsolved
7	Unauthenticated Mass Data Exposure on ApprovalRequest Entity	High	Unsolved
8	Unauthenticated Cross-Origin Data Exfiltration via CORS Wildcard and Missing Authentication	High	Unsolved
9	Unauthenticated Invitation Record Modification and Deletion	High	Unsolved
10	Unauthenticated Entity CRUD with Role Mass Assignment on Profile Entity	High	Unsolved
11	Broken Access Control - Unauthenticated CRUD on SecurityAlert Entity API	Medium	Unsolved
12	X-Frame-Options Header Not Set	Medium	Unsolved
13	User Enumeration via Verify-OTP Endpoint	Medium	Unsolved
14	Broken Object-Level Authorization - Unauthenticated Profile Entity CRUD	Medium	Unsolved
15	Unauthenticated PII Exposure of Internal Employee Email Addresses	Medium	Unsolved
16	Sensitive Data Exposure via Missing Cache-Control Headers on /teams Page and API	Low	Unsolved
17	PII Disclosure	Low	Unsolved

ISO 27001

The international standard for an Information Security Management System (ISMS). Its Annex A enumerates security controls spanning organizational, people, physical, and technological domains.

We surface technical vulnerabilities that intersect with the technological controls in Annex A, primarily those concerning secure authentication, configuration hardening, cryptography, application security, and management of technical vulnerabilities. Organizational, people, and physical controls are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

Findings from this scan that map to ISO 27001 controls:

No	Title	Severity	Status
1	Unauthenticated Full CRUD Access on Multiple Sensitive Entity Endpoints (Team, AuditLog, ApiToken, Invitation, ApprovalRequest)	Critical	Unsolved
2	Unauthenticated Privilege Escalation via Invitation Creation with Superadmin Role	Critical	Unsolved
3	Unauthenticated Approval Workflow Bypass via Direct Status Manipulation	Critical	Unsolved
4	Unauthenticated CRUD Operations on Profile Entity Allows Superadmin Account Creation	Critical	Unsolved
5	Unauthenticated User Creation with Arbitrary Roles via Entity API Bypassing Registration Flow	Critical	Unsolved
6	Broken Access Control - Unauthenticated Entity API Read/Write Access	High	Unsolved
7	NoSQL Injection via q Parameter on Profile Entity Endpoint	High	Unsolved
8	Unauthenticated Profile Entity Exposes User PII Bypassing User Entity Auth Protection	High	Unsolved
9	Unauthenticated Password Change Endpoint Bypasses Session Authentication	High	Unsolved
10	Unauthenticated Audit Log Injection via Mass Assignment	High	Unsolved
11	OTP Brute-Force via Attempt Counter Reset on Resend Enables Account Verification Bypass	High	Unsolved
12	Mass Assignment on Profile Role Field Enables Unauthenticated Privilege Escalation	High	Unsolved
13	Unauthenticated Entity Write Access via CORS Wildcard Enables Cross-Origin Data Tampering	High	Unsolved
14	Unauthenticated CRUD Access to AuditLog API	High	Unsolved
15	Unauthenticated PII Exposure via Entity API - Invitation and Team Listings	High	Unsolved
16	Unauthenticated Record Deletion on ApprovalRequest Entity	High	Unsolved
17	Unauthenticated Mass Assignment on User Entity - Admin Role Injection	High	Unsolved
18	Unauthenticated User Creation with Role Mass Assignment via Entity API	High	Unsolved
19	Unauthenticated Mass Data Exposure on ApprovalRequest Entity	High	Unsolved
20	Unauthenticated Cross-Origin Data Exfiltration via CORS Wildcard and Missing Authentication	High	Unsolved
21	Unauthenticated Invitation Record Modification and Deletion	High	Unsolved
22	Race Condition TOCTOU on Concurrent Approval Request Processing	High	Unsolved

No	Title	Severity	Status
23	Unauthenticated Audit Log Tampering Enables Evidence Destruction and False Trail Planting	High	Unsolved
24	Stored XSS via Team Name and Description Fields	High	Unsolved
25	Unauthenticated Entity CRUD with Role Mass Assignment on Profile Entity	High	Unsolved
26	Stored XSS via Invitation Entity email Field with JWT Exfiltration Chain	High	Unsolved
27	Unauthenticated WebhookConfig Endpoint Exposes 83 Configurations Including Internal Infrastructure URLs	High	Unsolved
28	OTP Attempt Limit Bypass via Race Condition (TOCTOU) on Verify-OTP Endpoint	High	Unsolved
29	Broken Access Control - Unauthenticated CRUD on SecurityAlert Entity API	Medium	Unsolved
30	Wildcard CORS Configuration Allows Any Origin to Access Sensitive API Endpoints	Medium	Unsolved
31	Mass Assignment Enables Unauthenticated Superadmin Role Escalation	Medium	Unsolved
32	Unauthenticated Cross-Origin Analytics Log Injection via IDOR on App-ID	Medium	Unsolved
33	User Enumeration via Differential Error Messages on Login Endpoint	Medium	Unsolved
34	X-Content-Type-Options Header Missing	Medium	Unsolved
35	Wildcard CORS Policy Enables Cross-Origin Audit Log Manipulation	Medium	Unsolved
36	Missing Rate Limiting on Write Operations (POST/PUT)	Medium	Unsolved
37	Race Condition - Duplicate Team Resource Creation via Concurrent Requests	Medium	Unsolved
38	Stored XSS via Unvalidated AuditLog Entity Fields	Medium	Unsolved
39	Wildcard CORS Policy on Entity API Enables Cross-Origin Exploitation	Medium	Unsolved
40	Insecure JWT Token Storage in localStorage	Medium	Unsolved
41	No Rate Limiting or Uniqueness Constraints Enables Unlimited Duplicate Entity Creation	Medium	Unsolved
42	Unauthenticated Analytics Event Injection with No Input Sanitization	Medium	Unsolved
43	Mass Assignment - Arbitrary member_count Manipulation on Team Entity	Medium	Unsolved
44	User Enumeration via Login Timing Side-Channel and Registration ID Reuse	Medium	Unsolved
45	Open Redirect via from_url Parameter in OAuth Login Flow	Medium	Unsolved
46	Stored CSV Formula Injection via Unauthenticated Entity Creation	Medium	Unsolved
47	IDOR via Unauthenticated App-Log ID Enumeration on Login Endpoint	Medium	Unsolved
48	Lack of Account Lockout Enables Credential Brute-Force	Medium	Unsolved
49	Unauthenticated CRUD Access on SecurityAlert Entity	Medium	Unsolved
50	User Enumeration via Verify-OTP Endpoint	Medium	Unsolved
51	Broken Object-Level Authorization - Unauthenticated Profile Entity CRUD	Medium	Unsolved
52	Wildcard CORS Policy Enables Cross-Origin Data Theft and Modification on Entity APIs	Medium	Unsolved
53	Unauthenticated PII Exposure of Internal Employee Email Addresses	Medium	Unsolved
54	Timing-Based User Enumeration via Registration Endpoint	Low	Unsolved
55	Sensitive Data Exposure via Missing Cache-Control Headers on /teams Page and API	Low	Unsolved
56	Server Technology Stack Fingerprinting via Response Headers	Low	Unsolved
57	Missing Content-Security-Policy Header Enables Unrestricted Script Execution	Low	Unsolved

No	Title	Severity	Status
58	Weak Password Policy Accepts Simple Passwords Without Complexity Requirements	Low	Unsolved
59	Unauthenticated Build Metadata Disclosure via Health Endpoint	Low	Unsolved
60	Full Platform API Specification Exposed on App Subdomain Without Authentication	Low	Unsolved
61	Missing Authentication on Page View Logging Endpoint	Low	Unsolved
62	Content-Security-Policy Response Header not set	Low	Unsolved
63	PII Disclosure	Low	Unsolved
64	Missing Content-Security-Policy Header	Low	Unsolved
65	CORS Wildcard Misconfiguration on /api/app-logs/ Endpoints	Low	Unsolved
66	Missing X-Frame-Options and Content-Security-Policy Headers Enabling Clickjacking on Login Page	Low	Unsolved
67	Missing X-Frame-Options and CSP frame-ancestors Headers Enabling Iframe Embedding	Low	Unsolved

PCI DSS

The Payment Card Industry Data Security Standard governs systems that store, process, or transmit cardholder data.

We surface technical vulnerabilities in web and API components that map to PCI DSS's application-security and transmission-security expectations - including injection, broken access control, authentication weaknesses, transport encryption gaps, and exposure of sensitive data in responses. Penetration testing engagements additionally exercise scenarios aligned with PCI's external testing requirements. Whether a given system is part of the cardholder data environment (CDE) is a scope determination made by the customer or their QSA. Network segmentation testing, stored cardholder data handling, and operational controls outside the externally testable surface are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

Findings from this scan that map to PCI DSS controls:

No	Title	Severity	Status
1	X-Frame-Options Header Not Set	Medium	Unsolved
2	Content-Security-Policy Response Header not set	Low	Unsolved

HIPAA

The US Health Insurance Portability and Accountability Act sets safeguards for systems handling electronic Protected Health Information (ePHI). The HIPAA Security Rule covers administrative, physical, and technical safeguards.

We surface technical vulnerabilities relevant to the Security Rule's technical safeguards such as access control weaknesses, authentication gaps, transmission security issues, and integrity flaws that could result in ePHI exposure or tampering. Whether a given finding involves ePHI depends on the data handled by the affected endpoint. Administrative and physical safeguards are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

Findings from this scan that map to HIPAA controls:

No	Title	Severity	Status
1	Long expiration time in JSON Web Tokens (JWTs)	High	Unsolved
2	X-Content-Type-Options Header Missing	Medium	Unsolved
3	X-Frame-Options Header Not Set	Medium	Unsolved
4	Content-Security-Policy Response Header not set	Low	Unsolved

DORA

The EU Digital Operational Resilience Act sets ICT risk management and operational resilience requirements for financial entities operating in the EU.

We surface technical vulnerabilities in externally testable systems that increase ICT risk under DORA's risk management framework, including weak authentication on critical interfaces, unencrypted data flows, exposed management surfaces, and other issues that materially affect incident likelihood. Governance, third-party risk, incident reporting workflows, and resilience testing programs are out of scope for this report.

Auto Pentest - 23 Sept 26 - base44 (Web App)

No findings mapped to DORA controls in the scan of this target.