

astra

The Ultimate Security Readiness Testing Checklist



Security Readiness Checklist

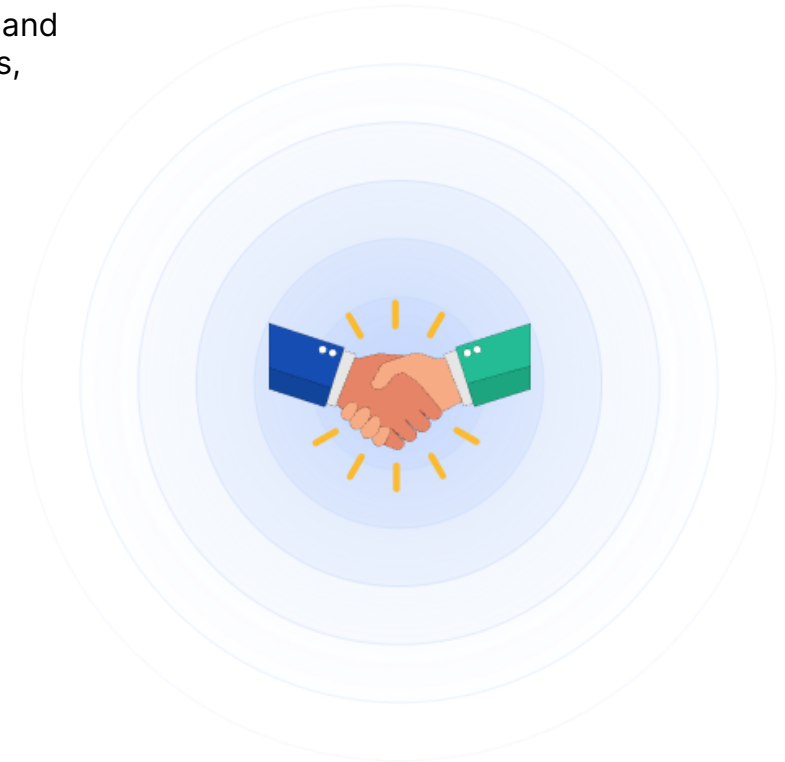
Buyers want proof, not promises. This checklist helps you organize the key security and compliance details your buyers and partners typically request including certifications, pen test results, data handling policies, access controls and more.

1. Basic Corporate & Contact Info

- ☐ Public security policy link
- ☐ Responsible disclosure / vulnerability reporting contact (email or process)
- ☐ Data processing / privacy policy link
- ☐ Dedicated contact for security / compliance matters

2. Compliance, Certifications, and Assessments

- ☐ List of all current certifications (e.g. SOC 2, ISO 27001, PCI-DSS, HIPAA, GDPR, etc.)
- ☐ Expiry or renewal dates for each certificate
- ☐ Audit / assessment reports (or attestation letters)
- ☐ Manual penetration test results & summary
- ☐ Automated vulnerability scanning results (especially recent ones)



3. Infrastructure & Security Controls

- ☐ Hosting environment details (platforms, cloud provider)
- ☐ [Secure DevOps integration](#) / how security is embedded in CI/CD
- ☐ Vulnerability management: frequency of scans, how you track & remediate (including for known CVEs)
- ☐ OWASP/SANS Top 10 or similar known checks coverage

4. Privacy & Data Handling

- ☐ Data classification (what is “sensitive”, what is “internal” etc.)
- ☐ [Encryption in transit & at rest policies](#)
- ☐ Data retention and deletion policies
- ☐ List of sub-processors (if any), with location and functions
- ☐ Mapping / flow of data, especially cross border



5. Access & Identity Controls

- ☐ Role-based access control (RBAC) setup
- ☐ Multi-factor authentication requirement (MFA)
- ☐ Onboarding / offboarding process for employees, contractors, etc.
- ☐ Logging & audit trails of access

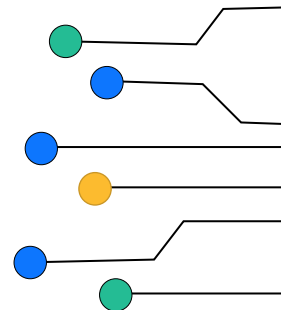


6. Monitoring, Incident Response & Compliance Violation Detection

- ☐ Real time or periodic security posture monitoring (how you observe infra, logs, etc.)
- ☐ Incident response plan: who is responsible, how you communicate, prior incidents if publicly disclosable
- ☐ Compliance violation detection (how you identify gaps versus the compliance frameworks such as SOC, GDPR etc.)

7. Document Management & Versioning

- ☐ Repository for all documents: reports, policies, certificates
- ☐ Version control and audit trail (who edited what & when)
- ☐ Metadata and searchability (tags, categories) so documents are easy to find
- ☐ Document expiry tracking / reminders



8. Review & Update Schedule

- ☐ Owners assigned for each document / policy
- ☐ Frequency of review for major items (e.g. certificates annually; scanning / compliance checks quarterly; policies maybe semi-annual or annual)
- ☐ Internal audit or check to ensure everything is up-to-date

9. Presentation & Accessibility

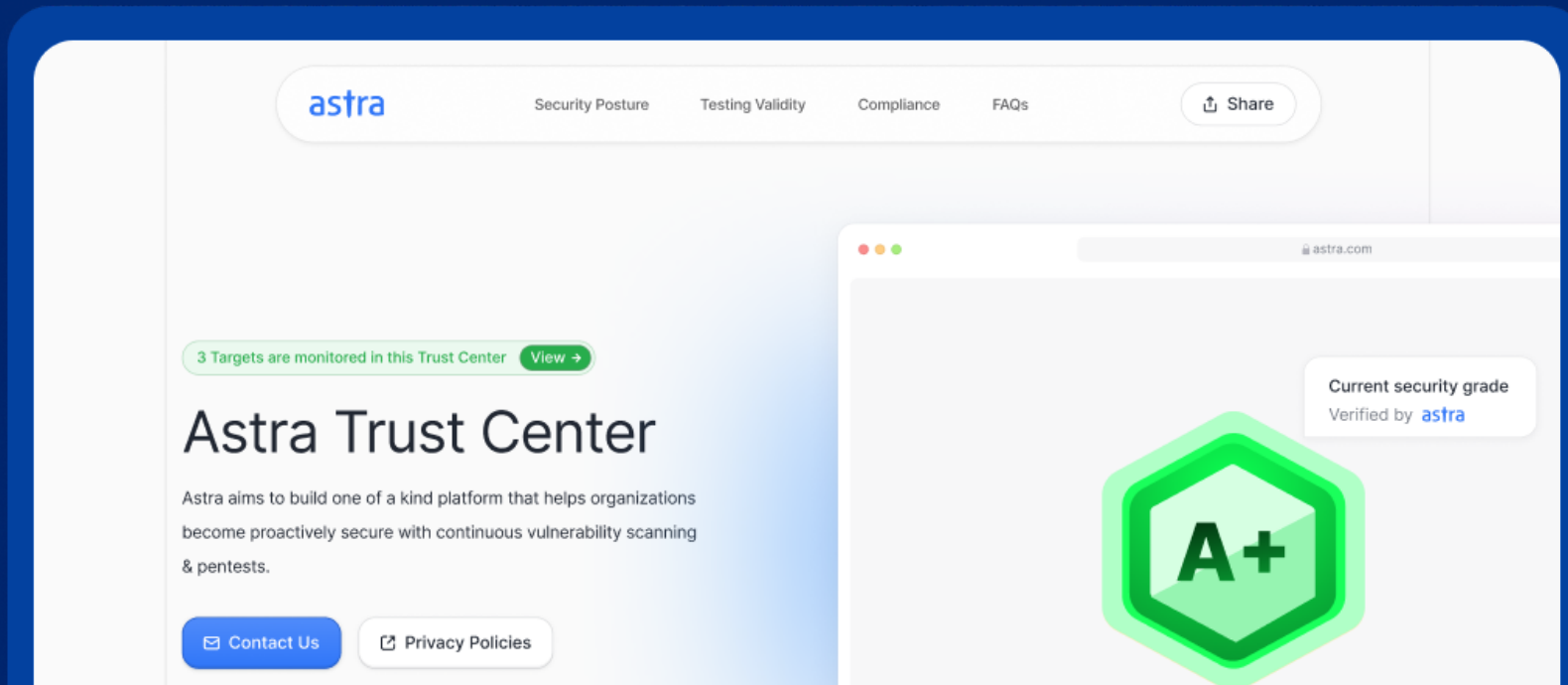
- ☐ Owners assigned for each document / policy
- ☐ Frequency of review for major items (e.g. certificates annually; scanning / compliance checks quarterly; policies maybe semi-annual or annual)
- ☐ Internal audit or check to ensure everything is up-to-date





When you're ready to move from scattered documents and time consuming requests to a single live and branded hub, Set up your Astra Trust Center.

It's built to help you publish all this information securely in one place, brand it as yours, and share it effortlessly with a single link.



Get Started



hello@getastra.com



www.getastra.com



Schedule a call



LinkedIn