60-SECOND ASSESSMENT

PKI Readiness Assessment

Evaluate your organization's preparedness across organizational, technical, compliance, and operational dimensions.

1 = Strongly disagree **3** = Partially true **5** = Strongly agree

Organizational Readiness (40% of score)

Governance, sponsorship, and team capacity

0/40

1 We have clearly defined RACI (Responsible, Accountable, Consulted, Informed) for certificate management across teams.

- ○ 1 - No RACI defined, ownership unclear
- ○ 2 - Some ownership discussion, nothing documented
- ○ 3 - RACI exists but not consistently followed
- ○ 4 - RACI documented and mostly followed
- ○ 5 - RACI clearly defined, universally understood and followed

2 We have executive sponsorship with actual authority to break organizational deadlocks and approve budget.

- ○ 1 - No executive sponsor identified
- ○ 2 - Executive "supports" project but no authority
- ○ 3 - Executive sponsor exists but engagement varies
- ○ 4 - Executive sponsor actively engaged with budget authority
- ○ 5 - Executive sponsor has authority, actively removes blockers

3 We have a formal change management process that works (doesn't require CEO escalation for routine changes).

- ○ 1 - No formal process, ad-hoc approvals
- ○ 2 - Process exists but frequently bypassed
- ○ 3 - Process works but very slow (30+ days)
- ○ 4 - Process works reasonably well (10-20 days)
- ○ 5 - Streamlined process with appropriate approvals (< 10 days)

4 Infrastructure, security, and development teams actively collaborate (not just in crisis).

- ○ 1 - Teams operate in silos, minimal collaboration
- ○ 2 - Collaboration happens only when forced
- ○ 3 - Some collaboration on major projects
- ○ 4 - Regular collaboration, established patterns
- ○ 5 - Deep collaboration, shared objectives and metrics

5 We can dedicate a team to PKI implementation (not everyone working "part time").

- ○ 1 - No dedicated team possible
- ○ 2 - Part-time from multiple people (< 0.5 FTE total)
- ○ 3 - 1-2 people part-time (0.5-1 FTE total)
- ○ 4 - 2-3 people dedicated (1.5-2.5 FTE)
- ○ 5 - Full dedicated team (3+ FTE)

6 We have successfully completed similar infrastructure transformation projects in past 2 years.

- ◯ 1 - No major infrastructure projects, or all failed
- ◯ 2 - Attempted projects that stalled or were abandoned
- ◯ 3 - Completed projects but massively over timeline/budget
- ◯ 4 - Completed projects mostly on time/budget
- ◯ 5 - Strong track record of successful infrastructure change

7 We understand our organizational capacity for simultaneous change (not attempting 5 major projects at once).

- ◯ 1 - 5+ major projects in flight, resources stretched
- ◯ 2 - 4 major projects, competing for resources
- ◯ 3 - 3 major projects, manageable but tight
- ◯ 4 - 2 major projects, capacity exists
- ◯ 5 - <2 major projects, or PKI is top priority

8 We have realistic timeline expectations (not "must be done by Q2" without basis).

- ◯ 1 - Arbitrary deadline imposed from above
- ◯ 2 - Timeline based on wishful thinking
- ◯ 3 - Timeline based on vendor estimates
- ◯ 4 - Timeline based on similar projects + buffer
- ◯ 5 - Timeline based on organizational capacity assessment

Technical Readiness (30% of score)

Infrastructure, tooling, and expertise

0/30

9 We know how many certificates we currently manage (± 20% accuracy).

- ◯ 1 - No idea ("thousands?")
- ◯ 2 - Rough guess (order of magnitude)
- ◯ 3 - CMDB count but known to be incomplete
- ◯ 4 - Recent inventory (within 6 months)
- ◯ 5 - Continuous discovery, live accurate count

10 We know where our certificates are deployed and who owns the applications using them.

- ◯ 1 - Unknown certificate distribution
- ◯ 2 - Know some high-profile applications
- ◯ 3 - 50-70% of certificates mapped to owners
- ◯ 4 - 70-90% mapped to owners
- ◯ 5 - Complete mapping, kept current

11 We have documented our current certificate issuance processes and approval workflows.

- ◯ 1 - No documentation, tribal knowledge
- ◯ 2 - Partial documentation, outdated
- ◯ 3 - Documentation exists but not followed
- ◯ 4 - Accurate documentation, mostly followed
- ◯ 5 - Living documentation, automation aligned

12 Our IT infrastructure is modern enough to support automation (APIs, CMDB integration possible).

- ◯ 1 - Legacy systems, no APIs, manual processes
- ◯ 2 - Mix of legacy and modern, limited APIs
- ◯ 3 - Mostly modern, some legacy holdouts
- ◯ 4 - Modern infrastructure, APIs available
- ◯ 5 - Cloud-native or modern infrastructure with robust APIs

13 We have monitoring and logging infrastructure to support PKI operations.

- ○ 1 - No centralized monitoring/logging
- ○ 2 - Basic monitoring, no PKI-specific visibility
- ○ 3 - Good monitoring, limited PKI visibility
- ○ 4 - PKI-aware monitoring for some certificates
- ○ 5 - Comprehensive PKI monitoring and alerting

14 We have in-house PKI/cryptography expertise (not just general sysadmin knowledge).

- ○ 1 - No PKI expertise on team
- ○ 2 - General understanding, no specialists
- ○ 3 - 1 person with PKI experience
- ○ 4 - 2-3 people with PKI experience
- ○ 5 - Deep bench of PKI expertise (5+ people)

Compliance & Risk Readiness (20% of score)

Regulatory requirements and risk management

0/20

15 We understand our compliance requirements for certificate management (SOC 2, PCI DSS, HIPAA, etc.).

- ○ 1 - Don't know what applies to us
- ○ 2 - Know some requirements, unclear on specifics
- ○ 3 - Know requirements, unclear how to implement
- ○ 4 - Requirements documented, implementation path unclear
- ○ 5 - Requirements fully mapped to technical controls

16 GRC/audit teams are engaged early in PKI planning (not surprised at go-live).

- ○ 1 - GRC not aware of PKI project
- ○ 2 - GRC aware but not engaged
- ○ 3 - GRC consulted occasionally
- ○ 4 - GRC participating in planning
- ○ 5 - GRC integrated from architecture phase

17 We have documented our risk tolerance for outages during migration.

- ○ 1 - Never discussed
- ○ 2 - Vague expectations ("no outages")
- ○ 3 - General risk tolerance discussed
- ○ 4 - Risk tolerance by application tier
- ○ 5 - Documented risk tolerance with SLA-backed decisions

18 We understand data sovereignty and compliance implications of PKI vendor choices.

- ○ 1 - Haven't considered this
- ○ 2 - Aware it might matter, no analysis
- ○ 3 - Some analysis, unclear on implications
- ○ 4 - Clear understanding, documented requirements
- ○ 5 - Requirements mapped to architectural constraints

Operational Readiness (10% of score)

Incident response and support capabilities

0/10

19 We have runbooks and escalation procedures for certificate-related incidents.

- ○ 1 - No documented procedures
- ○ 2 - Informal procedures, tribal knowledge
- ○ 3 - Some documentation, not current
- ○ 4 - Good documentation, regularly updated
- ○ 5 - Comprehensive runbooks, regularly tested

20 We have capacity to support 24/7 operations if certificate issues arise.

- ○ 1 - No on-call, business hours only
- ○ 2 - On-call exists but not PKI-trained
- ○ 3 - On-call with basic PKI knowledge
- ○ 4 - Dedicated security on-call, PKI-aware
- ○ 5 - Follow-the-sun coverage, PKI experts available

Total Readiness Score

0/100

S1: 0/40
S2: 0/30
S3: 0/20
S4: 0/10

Interpretation

Complete all 20 questions and visit axonshield.com/business/pki-readiness-assessment