PingOne Workforce Checklist

GCA Technology Services | gca.net

1. Application Inventory Critical 1-2 weeks Governance

Count every application that needs SSO integration: SAML 2.0, OIDC, WS-Federation, and legacy header-based apps. The number drives connector deployment, licensing, and phasing strategy.

2. Directory Source of Truth Critical 1-2 weeks Governance

Identify which directory serves as the authoritative identity source: PingOne Directory (cloud-native DaaS), Active Directory, Azure AD/Entra ID, LDAP, or a combination. For workforce deployments, HR

3. Deployment Model Critical 1-2 weeks Governance

Decide whether PingOne will be deployed as SaaS-only, hybrid with PingFederate on-premises, or as part of a broader PingOne suite deployment. The decision affects latency, data residency, and operatio

4. Compliance Framework Mapping Critical 2-4 hours Governance

Identify which compliance frameworks govern your workforce identity: SOX IT General Controls, HIPAA, PCI-DSS Requirement 8, NIST SP 800-63, NERC CIP. Each framework has specific requirements for authe

5. SSO Protocol Strategy Critical 1-2 weeks Security

Decide the workforce SSO protocol hierarchy: prioritize OIDC for modern cloud apps, SAML 2.0 for enterprise SaaS and on-premises apps, and WS-Federation for legacy Microsoft stacks. Enterprise applica

6. MFA Policy Design Standard 1-2 weeks Security

Design Adaptive MFA policies using PingOne Protect's risk engine: define which applications require MFA, which methods are permitted (TOTP, push, FIDO2/WebAuthn, biometric), and what risk signals trig

7. Directory Integration Architecture Standard 1-2 weeks Security

Design how PingOne connects to directory sources using PingOne Directory as a cloud-native Directory-as-a-Service: LDAP connector, AD connector, native Azure AD/Entra ID integration, or HR system conn

8. Token & Session Management Standard 1-2 weeks Security

Configure token lifetimes, refresh token policies, and single logout (SLO) behavior. Long-lived tokens reduce authentication prompts but increase security exposure. SLO requires application cooperatio

9. User Enrollment & Migration Standard 1-2 weeks Operations

Plan how employees migrate to PingOne: HR-driven bulk provisioning from your HRIS, self-service MFA enrollment, or phased rollout by department or location. MFA enrollment is the highest-friction migr

10. Identity Lifecycle Automation Standard 1-2 weeks Operations

Define automated workforce lifecycle workflows: joiner/mover/leaver automation triggered by HRIS events (new hire, transfer, termination), PingOne Directory group membership changes, and application p

11. Monitoring & Alerting Standard 1-2 weeks Operations

Configure PingOne Protect risk analytics, workforce-specific anomaly detection alerts, and SIEM integration for identity-focused threat detection. PingOne Protect provides real-time risk scoring for e

12. Operational Handoff Standard 1-2 weeks Operations

Decide who operates PingOne Workforce after go-live: internal team, GCA managed services, or hybrid. Workforce identity operations include ongoing PingOne Protect risk policy tuning, Adaptive MFA poli

Schedule a consultation: gca.net/book-a-consultation