Okta Workforce Checklist

GCA Technology Services | gca.net

1. Application Inventory Critical 1-2 weeks Governance

Count every application that needs SSO integration: OIN catalog apps, custom SAML/OIDC apps, SWA (Secure Web Authentication) legacy apps, and header-based apps. The number drives connector deployment,

2. Directory Architecture Critical 1-2 weeks Governance

Decide how Okta Universal Directory will integrate with existing directories: AD agent, LDAP agent, Azure AD/Entra ID sync, or flat-file import. Universal Directory is the authoritative source, but th

3. Okta Product Suite Selection Critical 1-2 weeks Governance

Determine which Okta products are in scope: SSO, Adaptive MFA, Universal Directory, Lifecycle Management, Governance, API Access Management, Advanced Server Access. Each product adds licensing cost an

4. Compliance Framework Mapping Critical 2-4 hours Governance

Identify which compliance frameworks govern your workforce identity: SOC 2, PCI-DSS Requirement 8, HIPAA, NIST SP 800-63, FedRAMP. Each framework has specific requirements for authentication strength,

5. SSO & Federation Strategy Critical 1-2 weeks Security

Define the SSO integration approach: Okta as IdP with SAML/OIDC, federation with existing IdPs (ADFS, PingFederate), or Okta as SP behind another IdP. The federation topology determines authentication

6. MFA Policy Design Standard 1-2 weeks Security

Configure Okta Sign-On policies and MFA rules: which apps require MFA, which MFA factors are allowed (TOTP, push, FIDO2, SMS), and what risk-based signals trigger step-up authentication. Okta's Adapti

7. Group Strategy & RBAC Standard 1-2 weeks Security

Design group structures in Universal Directory: mapped groups from AD, Okta-managed groups, group rules for automated membership, and app assignment groups. Groups drive SSO assignments and provisioni

8. Provisioning & Deprovisioning Standard 1-2 weeks Security

Configure SCIM provisioning for target applications: just-in-time provisioning, push provisioning, and deprovisioning on user lifecycle events. Deprovisioning speed directly impacts security posture w

9. Phased Rollout Strategy Standard 1-2 weeks Operations

Plan the rollout sequence: start with a pilot group (e.g., IT department), validate SSO and MFA workflows, then expand to additional departments. Okta rollouts affect employee productivity and require

10. Device & Endpoint Trust Standard 1-2 weeks Security

Configure Okta Device Trust and device posture policies: managed device detection, device certificates, and conditional access rules that enforce device compliance before granting application access.

11. Monitoring & Reporting Standard 1-2 weeks Operations

Configure Okta System Log integration with SIEM, authentication dashboards, and anomaly detection. Okta provides rich audit logs that require integration with security operations for actionable alerti

12. Operational Handoff Standard 1-2 weeks Operations

Decide who operates Okta after go-live: internal team, GCA managed services, or hybrid. Okta requires ongoing policy management, application integration maintenance, directory sync monitoring, and pla

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