CYBERARK IMPLEMENTATION CHECKLIST

For security leaders implementing CyberArk PAM for the first time. 13 decision points that determine whether your privileged access management deployment succeeds or stalls. Estimated timeline: 12-20 weeks for full CyberArk deployment.

CyberArk is the market leader in privileged access management, but the platform is only as strong as the implementation behind it. A poorly designed vault topology, an untested break-glass procedure, or a CPM rotation policy that breaks application dependencies can turn CyberArk from a security asset into an operational liability. This checklist covers the 13 decision

points where GCA's CyberArk practice sees the most friction, the most rework, and the most avoidable risk.

These are not steps in a process. They are decisions that affect each other. A choice you make about vault architecture will reshape your session recording strategy. Check off the items you have completed to track your progress. Expand each item for details and common mistakes.

01

These four decisions define the scope and constraints of the entire engagement. Getting them wrong means rework later.

1

Privileged Account Inventory

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Count every privileged account that CyberArk will vault: domain admins, service accounts, shared accounts, database credentials, cloud root accounts, and emergency/break-glass accounts. The number drives vault sizing, CPM licensing, and connector deployment.

Common mistake: Counting only domain admin accounts and discovering mid-project that service accounts outnumber them 5:1.

2

Target System Scope

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Map every system that holds privileged credentials: Active Directory, databases (SQL Server, Oracle, MySQL), cloud platforms (AWS, Azure, GCP), network devices (firewalls, switches), and applications with embedded credentials. Each target system requires a connector and a rotation policy.

Common mistake: Starting with the "crown jewels" and discovering 200 additional systems during rollout that were never scoped.

3

Deployment Model

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Decide whether CyberArk will be deployed on-premises, in a private cloud, or as CyberArk Identity Security (SaaS). The decision depends on data residency requirements, existing infrastructure, and operational model. On-premises gives full control; SaaS reduces operational burden.

Common mistake: Choosing on-premises for compliance reasons without evaluating the operational cost of maintaining vault infrastructure.

4

Compliance Framework Mapping

CRITICAL 2-4 HOURS (SINGLE WORKSHOP) *Governance*

Identify which compliance frameworks govern your privileged access: PCI-DSS Requirement 8, SOX IT General Controls, HIPAA, NIST SP 800-53, NERC CIP. Each framework has specific requirements for credential rotation, session recording, and access review.

Common mistake: Deploying CyberArk without mapping controls to specific compliance requirements, then retrofitting evidence after audit.

02

These five decisions shape how the platform operates at scale. They are expensive to change after go-live.

5

Vault Architecture

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Design the vault topology: primary vault, DR vault, satellite vaults for distributed environments. Decide on HA configuration, replication strategy, and disaster recovery RPO/RTO targets. The vault is the foundation of the entire CyberArk deployment.

Common mistake: Deploying a single vault without DR replication, then discovering during an outage that all privileged credentials are unavailable.

6

CPM Strategy (Credential Provider Manager)

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Decide which credentials to onboard for automatic rotation via CPM, which to vault-only, and which to leave outside CyberArk entirely. Not every credential benefits from automated rotation. Service accounts with application dependencies may break if rotated unexpectedly. CPM supports rotation for most standard credential types (AD, SQL Server, Oracle, network devices), but complex database credentials with stored procedures, mainframe accounts, and some cloud API keys with rotation restrictions may require manual rotation or custom CPM scripts. GCA maps each credential type to its rotation method during the onboarding phase.

Common mistake: Enabling auto-rotation on all accounts without testing application dependencies, causing service outages.

7

Session Recording Scope

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Decide which privileged sessions to record via PSM: RDP, SSH, database connections, web applications. Recording every session produces massive storage requirements. Recording too few creates compliance gaps.

> **Common mistake:** Recording all sessions by default, then running out of storage within 6 months because nobody defined retention policies.

8

Integration Mapping

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Map the integrations between CyberArk and adjacent platforms: SIEM (Splunk, Sentinel) for alert forwarding, ITSM (ServiceNow) for access request workflows, AD for authentication, cloud platforms for workload identity. Each integration has authentication and data flow requirements. CyberArk maintains a marketplace of 100+ pre-built connectors for target systems. GCA leverages marketplace connectors where available and builds custom integrations via the CyberArk SDK when the target system requires it, reducing connector development time and maintaining upgrade compatibility.

> **Common mistake:** Treating SIEM integration as Phase 2 work, then discovering at audit time that privileged access alerts are not reaching the SOC.

9

Secrets Management & Endpoint Privilege (Conjur / EPM)

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Decide whether to extend CyberArk beyond credential vaulting into DevOps secrets management (Conjur) and endpoint privilege management (EPM). Conjur injects secrets into CI/CD pipelines and application workloads. EPM removes local admin rights from endpoints. Both extend CyberArk's value but add deployment complexity.

Common mistake: Deploying CyberArk for credential vaulting only, then discovering that DevOps teams are still using hardcoded secrets in application code and CI/CD pipelines.

03

These four decisions determine whether your CyberArk deployment produces operational value or operational overhead. A vault without tested break-glass procedures is a single point of failure. A CPM without rotation monitoring is a silent security gap.

10

Onboarding Phasing

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Decide the order in which privileged accounts are onboarded to CyberArk: start with a pilot group (e.g., IT admin accounts), validate rotation and access workflows, then expand to production accounts.

Common mistake: Attempting to onboard all privileged accounts simultaneously, overwhelming the CPM and causing rotation failures across the environment.

11

Break-Glass Procedures

CRITICAL 2-4 HOURS (SINGLE WORKSHOP) *Security*

Define what happens when CyberArk is unavailable: how do administrators access privileged credentials during a vault outage? Break-glass procedures must be documented, tested, and auditable.

Common mistake: Deploying CyberArk without a break-glass plan, then discovering during a vault failure that nobody can access domain admin credentials.

12

PTA Configuration (Privileged Threat Analytics)

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Decide whether to deploy PTA for behavioral analytics on privileged sessions. PTA detects anomalous privileged behavior but requires tuning to avoid false positives.

Common mistake: Deploying PTA with default thresholds, then getting flooded with alerts that the SOC ignores, defeating the purpose of behavioral detection.

13

Operational Handoff

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Operations*

Decide who operates CyberArk after go-live: internal team, GCA managed services, or hybrid. CyberArk requires ongoing vault health monitoring, CPM management, connector maintenance, and platform upgrades.

Common mistake: Treating go-live as the finish line, then discovering three months later that nobody is monitoring vault replication or CPM rotation failures.

These 13 decisions are CyberArk-specific in execution. When GCA is involved, here is how we approach them differently.

We scope the vault architecture against your privileged account population, target system landscape, and compliance requirements before any deployment begins. Our CyberArk practice covers EPV, PSM, PTA, Conjur, and the full platform lifecycle from architecture through managed operations. GCA is rated 4.8 / 5.0 on Gartner Peer Insights based on 32 verified reviews. See our full privileged access management practice for the broader PAM landscape beyond CyberArk.

DOWNLOAD CYBERARK CHECKLIST (PDF)

CYBERARK PARTNER PAGE

BOOK A CONSULTATION

Need help with your CyberArk Implementation Checklist?

GCA Technology Services — gca.net — Book a consultation: gca.net/book-a-consultation

MANAGING YOUR DIGITAL IDENTITIES

SERVICES

- Managed IAM
- Implementation
- Assessment & Strategy
- General IAM

SOLUTIONS

- Identity Management
- Web Access Management
- Identity Governance
- Privileged Access

PARTNERS

SailPoint

Microsoft Entra

Okta

OpenText

Netwrix

Ping Identity

COMPANY

About GCA

Careers

Contact Us

Privacy Policy

MANAGING **YOUR** DIGITAL IDENTITIES