Business Requirement document (BRD) – version 1.0 CyberArk program – December 2025	
The current Business problem	**1. Ineffective Onboarding process for privileged accounts** **1.1. Operational inefficiency** The onboarding is done manually and takes in average 3 days per account. That results in a 20% error rate in privilege assignments, delaying IT operations and disrupting workflows. For example, in 2024, configuration errors delayed critical application deployments by 48 hours. **2. Generic & unmanaged accounts** Most privileged business and IT users rely on a single account for all operations. An audit in 2024 identified 150 shared "admin" accounts and forgotten system accounts, leading to untraceable actions and increased security risks. **2.1. A rising of credential theft** Over the past two years, phishing and credential stuffing attacks caused a 30% increase in compromised administrator credentials, enabling attackers to bypass security controls. **3. Lack of Access Control Processes** **3.1. An increase in sensitive data leaks** The absence of granular access controls has led to a 25% increase in sensitive data leaks over the past three years. For instance, in 2023, a contractor with excessive privileges exposed 10,000 customer records, both inadvertently and maliciously. **3.2. Frequent critical system outages** Misconfigured privileges caused 10 major outages in critical Windows and Unix servers in 2024, resulting in an average downtime of 6 hours per incident and significant operational disruptions. **4. Lack of action's traceability of privileged accounts** **4.1. Financial fraud** In 2024, a compromised administrator account led to €500,000 in financial fraud due to unmonitored privileged access, used to divert funds. **4.2. Malware propagation into critical servers** Unmonitored accounts facilitated ransomware attacks, with 30% of critical servers infected in 2024, causing operational disruptions. **4.3. Compliance violations** In 2025, the organization incurred a €250,000 fine for non-compliance with GDPR, NIS2, and ISO27001 due to inadequate oversight and audit trails for privileged accounts.

<table>
<tr><td>Root cause analysis</td><td>This initial analysis, derived from historical incident reports, preliminary stakeholder interviews, and internal audits, identifies potential root causes. A detailed investigation will follow BRD approval during dedicated workshops.

1. Ineffective Onboarding Process
• Lack of standardized policies for account creation, leading to manual errors (observed in 20% of audited cases in 2024).
• Insufficient integration between HR systems and IT directories, causing delays and unverified privileges.
• Limited training for IT administrators on secure practices, exacerbating rushed processes.
2. Lack of Authorization and Access Control Processes
• Absence of least privilege enforcement in access policies, allowing over-provisioning.
• No regular access review mechanisms, resulting in accumulated unused privileges.
3. Inefficient Monitoring of Privileged Accounts
• Missing real-time monitoring tools, preventing anomaly detection.
• Inadequate audit logging standards, failing regulatory requirements like GDPR.</td></tr>
<tr><td>Proposed solutions (overview)</td><td>The company decided to implement CyberArk Entreprise to close to close the three highest privileged access risks:

<table>
<tr><th>Business Requirement</th><th>Description</th><th>Target state</th></tr>
<tr><td>BR – 01: Semi-Automated Onboarding of Privileged Accounts with Identity Segregation</td><td>Replace 3-day manual process and shared/orphan accounts with discovery → pending → safe → auto-rotation</td><td><4 h onboarding, 0 shared/orphan accounts in production safes, 100 % ownership assigned</td></tr>
<tr><td>BR – 02: Just-In-Time Elevation with Dual Approval & Password Rotation</td><td>Replace permanent elevated rights and e-mail approvals with time-boxed, dual-approved access</td><td>100 % of privileged sessions via JIT (max 8 h), automatic revocation, SoD enforced</td></tr>
<tr><td>BR – 03: Privileged Session Recording & Isolation</td><td>Replace zero traceability with mandatory PSM recording and real-time export to Splunk</td><td>100 % of privileged sessions recorded, indexed and searchable in Splunk <5 min, 1-year retention</td></tr>
</table>

BR -00: Discovery & Clean-up is the mandatory prerequisite (see section 1_Discovery_and_Clean_Up for inventory, data quality, SoD matrix and ownership assignment).</td></tr>
</table>

Impacted Systems

System	Role in the program
Workday	Source of truth → employee attributes
SailPoint IdentityNow	IGA → metadata & termination events to CyberArk
Active Directory + Entra ID	Directory + IDP (SSO/MFA for PVWA)
CyberArk PAM	Core platform (EPV, CPM, PSM, PVWA)
Windows + Unix servers	Wave 1
Oracle + SQL Server DB	Wave 2
AWS + Azure consoles	Wave 3
Microsoft 365 + Salesforce	Wave 4
OT/SCADA pilot (250 devices)	Pilot
Splunk (primary) + Sentinel	SIEM & evidence

Out of scope current programme (deferred to Phase 3 or separate initiative):

- Full GCP console access
- Full IoT / non-human identities fleet
- AI-based behavioural detection

Assumptions & dependencies

As the IAM Business Analyst, I record the following assumptions and external dependencies identified during the kick-off. Their validity will be checked through a short set of environment readiness checks before UAT execution for BR-01/02/03. Outcomes and evidence will be filed in the Evidence & Data Pack and referenced in the Go/No-Go decision.

- **Supported connectors:** Connectors and methods exist for the in-scope platforms (Windows/Unix, Oracle/SQL Server, AWS/Azure) and cover onboarding, rotation and, where applicable, PSM proxy.
- **Time synchronization:** PAM, IDP, SIEM and target systems are NTP-synchronized with an acceptable skew threshold to ensure consistent timestamps.
- **Backup & retention:** Vault/PVWA backup cadence and retention (≥ 1 year) are defined. Restore testing is scheduled on pre-prod.
- **Monitoring & evidence path:** PAM telemetry can be exported to the SIEM (syslog or API) and retained as per compliance.
  A shared repository for evidence (screenshots/exports/logs) is agreed for UAT/RTM.
- **Data readiness:** Phase-0 inventory and data-quality baseline are achievable (owners identified for Wave-1 privileged accounts, orphan, shared, stale patterns measurable).
- **Environments & stakeholders:** A pre-production environment mirrors production for testing key participants (approvers, PAM admins, SOC, DB/Cloud owners) are available during sprints and UAT windows.
- **Validation approach:** Each assumption above will be verified by a single, simple readiness check (e.g., SSO claim mapping note, port/protocol matrix, sample PAM log format, backup/retention note, NTP timestamp table, delta payload example, connector matrix, evidence index).
  All readiness checks must be **PASS** before UAT for BR-01/02/03 starts; any

	FAIL pauses testing until the dependency is fixed or a documented workaround is approved. References to the detailed checks and the Evidence & Data Pack will be included in the BRD annexes and in the Go/No-Go checklist.
Business Requirements	**BR-00:** Discovery, Clean-up & Ownership Assignment 1. **Goal:** Establish a reliable privileged-account inventory and data quality baseline before PAM onboarding. 2. **Scope:** AD/Entra accounts and privileged groups, HR roster (Workday export), list of critical systems (application owners). 3. **Method (high level): Read only extract, staging SQL, reconciliation queries:** • Privileged group membership. • AD and HRIS match (orphans/terminated) • Generic/service accounts patterns • Stale accounts (>90 days no logon) 4. **Acceptance criteria** • ≥95% of privileged accounts identified for priority systems • 0 accounts without owner in wave 1 • Data quality baseline and remediation plan published (orphans, generic/shared, stale) • Onboarding waves v1 approved (systems, owners, dates) 5. **Evidence** • See annex: datasets, SQL, result screenshots, and exported tables.
	BR-01: Semi-Automated Onboarding of Privileged Accounts with Identity Segregation
	BR-02: Just-In-Time Elevation with Dual Approval & Password Rotation
	BR-03: Privileged Session Recording & Isolation