Business Requirement document V.01	
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.

Root cause analysis	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.
Proposed solutions (overview)	The company decided to implement CyberArk PAM solution to: • Enforce separation of standard and privileged identities (BR-01) • Replace ad-hoc e-mail approvals with JIT policy/SoD workflows (BR-02) • Proxy and record privileged sessions with PSM and SIEM export (BR-03) • The program is preceded by BR-00 (Data Discovery & reconciliation) to establish a reliable inventory and data-quality baseline. • Controls are aligned to ISO27001/NIS2/GDPR/DORA.
Impacted Systems	**1. Source of truth (Workday):** feeds identities/attributes to IGA (CSV/API) and downstream to directories/PAM.
	2. Identity Governance (IGA- SailPoint): Role/SoD policies. Provisioning via SCIM/REST, certification campaigns feeding PAM scope.
	3. Directory & Identity Provider (Microsoft Entra ID/Active Directory + IDP): Directory groups/attributes. Authentication context via SAML/OIDC (+MFA) for PVWA/portals.
	4. CyberArk PAM (Vault, PVWA, CPM, PSM): Central control plane for onboarding, rotation, JIT approvals, and session recording, APIs for automation.
	5. Databases (e.g., Oracle, SQL Server…): Privileged accounts onboarded to safes, rotation and proxied sessions via PSM, audit to SIEM.
	6. Cloud Platforms (AWS/Azure/GCP): Key/account onboarding (IAM roles, access keys), connectors, API-Based integrations where applicable.
	7. IoT/ non-human identities (devices, services, bots): Account discovery, ownership assignment, onboarding were feasible, policy-driven access, monitoring via SIEM.
	8. Security analytics (SIEM-Splunk): Centralized logs/alerts, correlation with PSM recordings, evidence retention.

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:** Data Discovery & reconciliation 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 for all accounts (executives, IoT), with separation.
	BR-02: Just-in-time approval with continuous verification and password rotation.
	BR-03: Session recording with AI detection, retained 1 year for GDPR/NIS2.