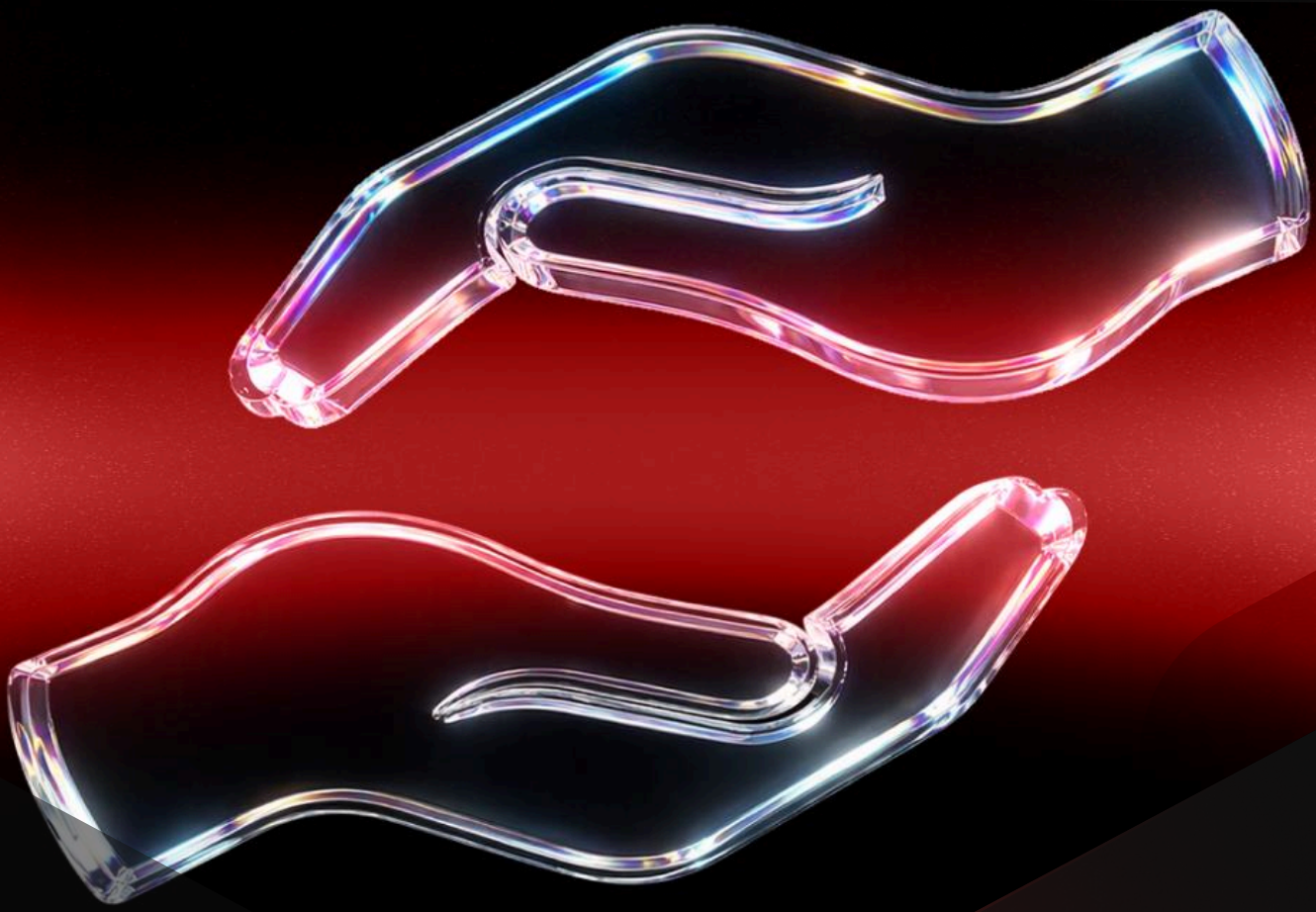
QBurst | A High AI-Q™ Company



Strengthening Governance and Data Protection for a Nonprofit Technology Division

Transforming informal security practices into a structured, ISO-aligned governance framework to safeguard distributed development environments and data.

Overview

We conducted a structured security and governance assessment to evaluate operational practices and strengthen compliance with **ISO 27001 and ISO 27701** principles.

- Provided clear insight into access governance, development workflows, and security practices across the technology division.
- Implemented remediation for access governance, endpoint protection, and formalized credential management.
- Advanced **Governance Maturity** from trust-based, manual oversight to a model of structured governance assurance with individualized, auditable access.

Client Profile

Based in the US, this prominent nonprofit technology division supports a global organization dedicated to healthcare certification. They manage a large-scale Salesforce ecosystem with a workforce of 19+ specialized personnel operating under a rigorous Agile delivery model.

Challenges: Governance and Data Protection Gaps

- **Shadow Access and Role Clarity:** Reliance on shared or temporary credentials weakened audit defensibility and individual accountability.
- **Absence of Endpoint Data Loss Prevention**: Lack of DLP controls and unrestricted USB permissions on workstations increased the risk of unauthorized data transfer.

- **Password Governance and Monitoring Oversight:** Manual credential tracking and a lack of structured log monitoring created reliance on informal documentation and external assumptions.

QBurst Solution: Security and Governance Assessment

We implemented a structured four-week assessment plan to establish total governance visibility and trigger corrective actions. Our approach moved the organization toward a high level of Governance Maturity Advancement by replacing trust-based practices with technical enforcement.

- **Week 1: Knowledge Transfer & Familiarization:** Reviewed system architecture, deployment pipelines (AutoRABIT), development workflows, and system dependencies.
- **Week 2: Policy & Security Practice Review:** Evaluated existing security controls and data handling procedures to identify early compliance gaps in role-based access.
- **Week 3: Awareness & Compliance Validation:** Conducted security awareness sessions and distributed comprehensive questionnaires to evaluate employee understanding of confidentiality.
- **Week 4: Gap Analysis & Reporting:** Prepared a detailed risk report mapping findings against ISO 27001 and ISO 27701 control objectives with prioritized remediation.

Implementation Highlights

- **Access Governance Normalization:** Provisioned individual credentials for all contributors to ensure 100% traceability and accountability.
- **Endpoint Data Protection Deployment:** Deployed DLP solutions and removed USB access permissions to mitigate data exfiltration risks.
- **Credential Management Enforcement:** Mandated bimonthly password resets and enforced validation through structured tracking mechanisms.

- **Active Security Awareness Validation:** Transitioned from passive policy acknowledgment to active validation through mandatory questionnaires and focused follow-up training.
- **Continuous Monitoring and Audits:** Introduced randomized weekly 1:1 security reviews to validate repository management and adherence to secure development guidelines.

Impact: Strengthened Governance and Data Protection

- **Individualized Access Accountability:** Eliminated 100% of shared credential risks, ensuring all actions are fully traceable and audit-ready.
- **Enhanced Endpoint Data Safeguards:** Strengthened protections against unauthorized data transfer through robust DLP deployment and restricted hardware access.
- **Reinforced Strategic Governance Principles:** Demonstrated that shared access undermines audit integrity, legal agreements require technical enforcement, and monitoring assumptions must be validated through oversight.
- **Validated Security Awareness:** Successfully transitioned the technology division toward a structured governance model that maintains operational continuity while meeting international standards.