Welford IAG®

# Welford Identity & Access Governance (IAG)

Service Definition

WELFORD® SYSTEMS

CfA Centre for Assessment ISO 27001 Information Security

UKAS MANAGEMENT SYSTEMS 0120

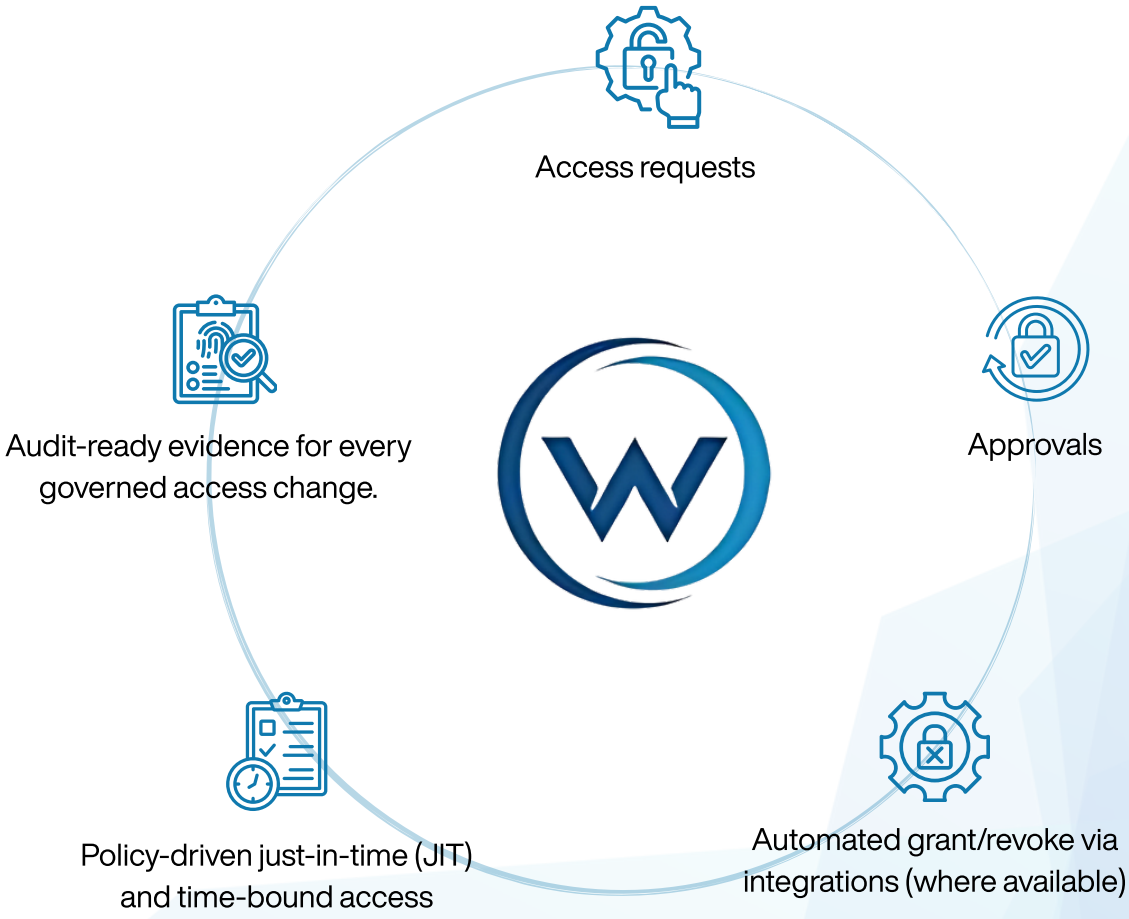
# Table of Contents



# 1. Service summary

Welford IAG is an Identity & Access Governance (IAG) platform that governs access end-to-end across the enterprise. It provides a central control point for access requests, approvals, policy-driven just-in-time (JIT) and time-bound access, automated grant/revoke via integrations (where available), and audit-ready evidence for every governed access change. Where direct automation is not available, Welford IAG orchestrates controlled fulfilment through ticketing while preserving governance and traceability.

Welford IAG includes Privileged Access Management (PAM) capabilities, focused on privileged credential governance (vaulting, controlled reveal, rotation and “no-human reveal” for non-human identities) and password-less Linux privileged access with optional command auditing for Linux sessions initiated through Welford IAG.



# 2. Intended users and common use cases

## 2.1. Intended audience

Welford IAG is for organisations that need to reduce cyber risk, strengthen cyber resilience, and meet compliance obligations by governing access across cloud, SaaS, databases, directory services and servers. It supports Zero Trust principles (least privilege, just-in-time access), segregation of duties (SoD), and audit-ready evidence for regulated environments. It is designed for:

Security, risk and compliance teams (Zero Trust, SoD, audit readiness, resilience)

IT operations and service management teams (controlled fulfilment, lifecycle governance)

Application, data and system owners (ownership, approvals, accountability)

Teams managing privileged access across Linux servers and databases

Employees, contractors and third parties who require governed access

## 2.2. Typical use cases

- Govern all access using time-bound/JIT approvals with automatic expiry and revoke
- Apply risk-based approval routes, including additional approvals for privileged access (e.g., line manager + InfoSec)
- Govern privileged credentials for Oracle databases and Linux privileged accounts (vault/reveal/rotate)
- Control supplier/third-party access with approvals, time limits, and auditable evidence
- Joiner/Mover/Leaver governance with automated deprovisioning; raise tickets when manual removal is required to reduce access drift
- Provide audit-ready evidence and point-in-time access views across connected systems
- Application/service account governance using “no-human reveal” (API-only secret retrieval from allowlisted IP ranges)

# 3. Service scope and delivery model

## 3.1. SaaS delivery

Welford IAG is delivered as a SaaS service accessed via supported web browsers and APIs over HTTPS. Each customer is provided a dedicated instance/tenant, deployed in a dedicated network segment (subnet). This provides strong isolation between customers.

Optional enhanced isolation: Where required, Welford can deploy the customer's dedicated instance within a dedicated cloud subscription for additional isolation (agreed in the Order Form/Call-Off Contract).

## 3.2. Integration-dependent automation

Automation and reconciliation depend on the buyer's target systems and permitted access, including:

- Target system capability (APIs/connectors/DB access)
- Buyer security policies, credentials, and network connectivity
- Agreed onboarding scope and integration configuration

Where direct automation is not available, Welford IAG supports ticket-orchestrated fulfilment (e.g., ServiceNow/Jira/Welford SM) while retaining end-to-end governance, traceability, and audit evidence.

## 3.3. Optional deployment in buyer-controlled environments

If a buyer requires, Welford IAG can be deployed in a buyer-controlled environment, such as the buyer's cloud subscription or on-premises infrastructure.

## 3.4. Optional managed service (operational support)

Welford can optionally provide a managed service to operate Welford IAG day-to-day (e.g., governance operations, onboarding/offboarding support, and integration monitoring), reducing the buyer's need for specialist resources. Scope and pricing are agreed separately.

# 4. Functional capabilities

## 4.1. Identity & Access Governance (IAG/IGA) capabilities

### 4.1.1 Access request and approval workflows

Welford IAG enables users to request access and routes approvals based on policy, ownership, and risk level.

- Request access to systems, roles, privileges and entitlements
- Configurable approval routing (e.g., line manager, system owner, data owner, InfoSec)
- Risk-based routing for privileged access (e.g., additional approvals for DBA/admin access)
- Policy-based controls and consistent governance rules
- Evidence captured for request details, justification, approvals and timestamps
- Segregation of duties controls, including prevention of self-approval (and additional SoD rules where configured)

### 4.1.2. Time-bound / JIT access governance

Welford IAG governs all access using just-in-time/time-bound approvals to reduce standing access and enforce least privilege.

- Just-in-time access for all governed access requests
- Time-bound access by policy (approve access for a defined window)
- Automatic expiry and revoke actions where integrated
- Early revoke when necessary
- Supports least privilege by reducing standing access

### 4.1.3. Joiner / Mover / Leaver (JML)

Welford IAG governs lifecycle access changes with controlled approvals and traceable evidence.

- Workflow support to govern onboarding, internal moves and offboarding
- Controlled approvals and evidence for lifecycle changes
- Deprovisioning workflows for leavers and role changes for movers

### 4.1.4. Entitlement catalogue and ownership

Welford IAG maintains an entitlement catalogue with ownership to support accountability and consistent approvals.

- Catalogue of governed entitlements (roles/privileges) as configured
- Ownership assignment for accountability and approval routing
- Multi-level approvers and approver substitution (where configured)

### 4.1.5. Audit and evidence (governance layer)

Welford IAG provides end-to-end traceability across requests, approvals, fulfilment, and expiry/revocation.

- Full audit trail for buyer user actions (requests, approvals, admin activity)
- Evidence linking approval decisions to implemented access and expiry/revocation

### 4.1.6. Access visibility

Welford IAG provides visibility into current and historical access for authorised stakeholders and auditors.

- Real-time visibility into who has what access and until when (including JIT/time-bound access)
- Point-in-time views to show what access a user had at a specified date/time, based on entitlement history and captured evidence (reconciliation improves accuracy where enabled)

## 4.2. Privileged Access Management (PAM) capabilities

Welford IAG includes PAM capabilities covering privileged credential governance and privileged session oversight where supported.

### 4.2.1. Privileged credential governance (vault/reveal/rotate)

Welford IAG governs privileged credentials for governed privileged accounts (e.g., Oracle privileged accounts and Linux privileged accounts).

- Credential vaulting: secure storage and governance of privileged credentials
- Controlled reveal: password reveal to authorised users, linked to approvals and time-bound/JIT access
- Rotation: scheduled rotation and/or rotation after use (policy dependent)
- Evidence: audit trail of requests, approvals, reveals, rotations and administrative changes

### 4.2.2. “No-human reveal” for non-human identities

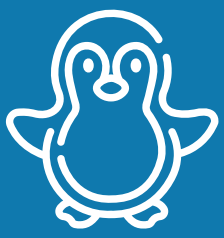
Welford IAG supports application/service account governance through API-only secret retrieval.

- Configure credentials as “no-human reveal” for application/service accounts
- API-only retrieval for authorised systems
- Retrieval restricted to allow-listed IP addresses/ranges
- Retrieval events are logged and auditable

### 4.2.3. Privileged session oversight and auditing (Linux)

When Linux access is initiated through Welford IAG, sessions can be governed and audited.

- Access is controlled and time-bound
- Commands executed during the session can be recorded for audit (subject to configuration and policy)
- Audit evidence links the access request and approval to the resulting session activity



Scope note: Session command auditing currently applies to Linux sessions initiated through Welford IAG. For password-revealed logins to other systems, Welford IAG audits credential lifecycle events (request/approval/reveal/rotation), but does not currently provide session command recording for those logins.

## 4.3. Linux Access Management (no standing credentials)

Welford IAG supports password-less Linux privileged access designed to reduce standing credential risk.

- No standing SSH keys/certificates left on user devices
- No shared privileged passwords distributed to users
- Access is time-bound and linked to approvals
- Automatic expiry/revocation and auditable evidence

## 4.4. Built-in Password Wallet

Welford IAG includes password wallet for individual users to securely store work passwords, reducing reliance on browser or local password stores.

- Secure, encrypted storage for user-owned credentials protected by access controls
- Users can retrieve stored passwords when needed, with access activity logged for audit
- Helps reduce credential exposure risk from browser-based saving and local device compromise

## 4.5. Automation coverage and integration approaches

Welford IAG supports multiple approaches to automation depending on target system type and buyer environment.

### 4.5.1. Integration methods

Welford IAG integrates using methods appropriate to each target system.

- REST API-based integrations where APIs are available
- Directory/IdP and application integrations where supported (e.g., role/group assignment, provisioning)
- Database integrations for controlled grant/revoke of roles/privileges where permitted
- Ticket orchestration to create/update tickets where direct automation is not feasible

### 4.5.2. What can be automated end-to-end (where integrated)

Where integrations are in place, Welford IAG can automate the access lifecycle end-to-end.

- Request → approval → grant → audit evidence
- Time-bound access → automatic expiry/revoke → evidence
- JML workflows with consistent approvals and controlled fulfilment
- Privileged credential governance workflows (where configured)

### 4.5.3. Coverage examples by subsystem type

Final automation coverage is confirmed during onboarding based on buyer systems, permissions and agreed scope.

- Identity/Directory: role/group assignment and revocation (where integrated)
- Cloud: role assignment/removal and reporting (where integrated)
- SaaS apps: provisioning/deprovisioning where supported by API/SCIM/DB connector
- Databases: grant/revoke roles/privileges and reconciliation where integrated
- Linux: password-less access and session audit (where enabled)
- ITSM/Ticketing: ticket creation/update and evidence linkage for manual fulfilment

# 5. Reporting, audit, and evidence

Welford IAG is designed to support audit readiness by producing traceable evidence for end-to-end access governance.

### Access requests and approvals

who approved what, when, and why

### Implemented access changes

automated fulfilment or ticket-orchestrated fulfilment

### Time-bound/JIT expiry and revocation events

including early revoke where applied

### Privileged credential governance events

reveal, rotation, API retrieval and no-human reveal activity

### Administrative actions within the platform

configuration changes and privileged actions

### Exportable reports and audit logs for audits and investigations

CSV/JSON; PDF reports where available

# 6. Service management and support

## 6.1. Support channels

Support is provided through standard channels, with options for enhanced coverage.

- Standard support via ticketing/email (web-based support management)
- Optional phone support for priority incidents as part of enhanced support (where agreed)

## 6.2. Support hours and response

Support is provided during UK business hours, with optional higher tiers available by agreement.

- Standard support: UK business hours (Mon–Fri)
- Enhanced support (optional): extended weekday hours (e.g., 08:00–20:00 UK) and phone for P1/P2
- 24x7 P1 incident response (optional): on-call coverage for P1 incidents; scope/limits defined in the Order Form

## 6.3. Incident reporting and communications

Buyers can report incidents via ticketing/email (and phone for priority incidents where included).

- Incident updates during investigation and response
- Written incident report on closure for significant incidents (timeline, impact, actions taken, corrective actions/CAPA, and any buyer actions required)

# 7. Onboarding and adoption

Welford IAG onboarding is typically delivered in phases to validate governance design, integrations, and operational readiness.

- Discovery: scope, target systems, governance model, policies and workflows
- Consulting and implementation (workflow/policy design, configuration, integrations, testing)
- Integration: APIs/connectors/databases/ticketing as agreed
- Pilot (optional): validate policies, automation/orchestration and reporting
- Rollout: phased onboarding of systems and identities into production
- Training and handover: admin training, operational handover documentation, and adoption support

# 8. Implementation, consulting, and managed service (optional)

Welford can provide end-to-end delivery services to support adoption at scale.

- Project management and delivery governance
- Consulting and implementation (workflow/policy design, configuration, integrations, testing)
- Training and adoption support
- Optional managed service to operate and administer the platform (e.g., onboarding/offboarding operations, governance operations, and integration monitoring), reducing the buyer's need for specialist resources

Scope and pricing are agreed in the Order Form/Call-Off Contract.

# 9. Data handling, export, and end-of-contract

## 9.1. Data export

Buyers can export data via the UI and/or API.

- Standard export formats include CSV/JSON (and PDF reports where available)
- A final export package can be provided on request (supplier-assisted export by agreement)

## 9.2. End-of-contract process

At contract end:

- Buyer performs data export (and/or requests supplier-assisted export)
- Access is disabled after the agreed end date
- Buyer data is securely deleted in line with retention/deletion policy and contractual requirements after export confirmation

# 10. Summary of differentiators

Welford IAG differentiators include:

- End-to-end IAG governance with audit-ready evidence
- JIT and time-bound access by policy across all governed access, reducing standing privileges
- PAM capabilities: vault/reveal/rotate privileged credentials plus no-human reveal for service accounts
- Password-less Linux privileged access with optional command auditing (Linux sessions initiated through Welford IAG)
- Built-in password wallet for user-owned work passwords
- Automation where possible; ticket orchestration where not—without losing governance evidence
- Optional implementation services and managed service for buyers lacking specialist resources
- Optional buyer-controlled/on-prem deployment

WELFORD® SYSTEMS

For more information, please contact us at +44 203 442 0741 (UK), +94 75 321 2303 (SL)
E-mail: info@welfordsystems.com
or visit us online at www.welfordsystems.com