



TECHNICAL WHITEPAPER

A Distributed, Audited Decision-Support Platform for Public-Sector Organisations

Abstract

Public-sector organisations face increasing pressure to demonstrate transparent, defensible decision-making while complying with stringent data-sovereignty and GDPR Right-to-Be-Forgotten requirements. Existing tooling provides limited support for weighted decision forms, auditable policy workflows, or tamper-proof historical records. This whitepaper presents a distributed cloud application that enables organisations to design, execute, and audit complex decision processes using a secure, multi-region architecture, cryptographically assured audit DAGs, least-trust managed identities, and deterministic CI/CD deployment pipelines.

1. Introduction

Public-sector decision-making often relies on structured forms, policy checklists, and multi-stage assessments. However, most organisations lack software capable of capturing *why* a decision was made, *how* it was evaluated, and *what evidence* contributed to the outcome. Traditional systems store only the latest edit, provide no weighting model for policy scoring, and cannot guarantee tamper-proof audit trails.

This application addresses these gaps by providing a secure, distributed, fully audited platform for creating weighted decision forms and capturing complete versioned histories of policy evaluations. It is designed for transparency, compliance, and operational resilience across UK and EU data jurisdictions.

2. Architecture Overview

The platform is deployed as two identical Azure stacks - one in the UK, one in the EU - ensuring strict data-sovereignty compliance. Each stack is deployed deterministically via CI/CD pipelines, ensuring that every environment is reproducible, configuration-consistent, and free from manual operator drift.

Each stack consists of:

- **Secure Web Front End** Authenticated via Microsoft Entra ID using on-behalf-of flows, ensuring identity continuity from the client through all backend layers.
- **Two Backend Services** Responsible for form template management, decision-instance creation, and scoring logic.

- **Asynchronous Worker Daemon** Monitors Cosmos DB change feed events and updates the Directed Acyclic Graph (DAG) audit index, ensuring every modification is captured as a new immutable node.
- **Azure Blob Storage** Stores encrypted versioned snapshots of form templates and decision instances. No historical versions are stored in the database itself.
- **Azure Key Vault** Manages rotating per-tenant encryption keys, refreshed every 30 days.

This architecture provides isolation, resilience, and cryptographic assurance across all layers.

3. Core Technical Concepts

Weighted Decision Templates

Users define custom form templates containing questions, answer sets, and weighted scoring models. Each answer can be assigned a positive, neutral, or negative weighting, enabling structured evaluation against policy matrices (e.g., “Good”, “Neutral”, “Bad”). This creates a consistent, repeatable framework for assessing complex public-sector decisions.

Decision Instances & Visualisation Engine

Templates are instantiated for specific decision points - such as planning applications - allowing consistent evaluation across cases while preserving full historical context. Once completed, each decision instance can be rendered through a flexible visualisation engine supporting multiple analytical styles, including:

- Bar charts
- Sunburst diagrams
- Radial charts
- Doughnut Economics Action Lab–style doughnut charts

These visualisations provide intuitive, multi-dimensional insight into weighted scores, section-level impacts, and overall policy alignment. They support both internal review and public transparency by presenting complex decision data in clear, interpretable formats.

PDF Export with Embedded Visualisations

Completed forms - including all visualisations - can be exported as a PDF. This ensures that decision records are portable, archivable, and suitable for inclusion in case files, committee packs, or public-facing documentation. The export process preserves the

audit lineage and scoring context, providing a complete, immutable snapshot of the decision at the time it was made.

Directed Acyclic Graph Audit Model

Every change to a template or decision instance generates a new DAG node. This ensures:

- Full version history
- Immutable audit lineage
- Tamper-proof change tracking
- Transparent decision evolution

The DAG is updated asynchronously via the worker daemon, guaranteeing audit consistency even under high load.

Encrypted Version Snapshots

Historical versions are stored as encrypted blobs rather than database records. Each audit entry carries a unique encryption vector, combined with the tenant's current key to decrypt the snapshot.

This design ensures:

- GDPR-compliant redaction
- Tenant-isolated cryptographic boundaries
- Zero leakage of historical data across jurisdictions

4. GDPR Right-to-Be-Forgotten Enforcement

The platform implements a cryptographically robust redaction mechanism:

1. Each audit entry includes a unique encryption vector.
2. Versioned snapshots are encrypted using the tenant's rotating Key Vault key + the vector.
3. To redact a historical version, the system removes the encryption vector from the audit index.
4. Without the vector, the snapshot becomes permanently unreadable - achieving irreversible crypto-shredding.

This approach ensures compliance without deleting audit structure, preserving the integrity of the DAG while rendering sensitive content inaccessible.

5. Security Model

Security is enforced end-to-end using a **least-trust identity and access model**:

- **Entra ID on-behalf-of flows** maintain identity context across all layers.
- **Least-trust RBAC boundaries** ensure every managed identity is scoped only to the minimum required permissions.
- **Azure Managed Identities** are configured so that even Azure Global Administrators cannot access live data, ensuring operational separation and preventing privilege escalation.
- **Managed identities** isolate service-to-service communication.
- **Per-tenant encryption keys** prevent cross-tenant data exposure.
- **Multi-region deployment** ensures data remains within its legal jurisdiction.

This model ensures that no human operator - regardless of administrative role - can directly access production data, aligning with modern zero-trust principles.

6. Deterministic CI/CD Deployment

All infrastructure, configuration, and application components are deployed via deterministic CI/CD pipelines. This ensures:

- Reproducible environments
- Immutable infrastructure definitions
- No manual configuration drift
- Full auditability of deployment changes
- Predictable, testable release workflows

The system can be redeployed from source with identical behaviour, supporting long-term maintainability and compliance verification.

7. Performance & Scalability

The architecture scales horizontally across:

- Cosmos DB partitions
- Worker daemon throughput
- Blob storage capacity
- Stateless backend services

The DAG audit model is optimised for append-only operations, enabling high-volume decision workflows without compromising audit integrity.

8. Extensibility & Future Work

The platform is designed for extension into:

- Additional data-sovereignty regions
- More complex scoring matrices
- Policy-specific workflow engines
- Public-facing transparency dashboards
- Automated compliance reporting

9. Conclusion

This application provides a secure, transparent, and fully auditable foundation for public-sector decision-making. By combining distributed cloud deployment, cryptographically assured audit DAGs, weighted decision templates, least-trust managed identities, deterministic CI/CD pipelines, and GDPR-compliant redaction mechanisms, it delivers a modern, defensible approach to policy evaluation across UK and EU jurisdictions.