Intelligent Spaces, Sustainable Futures.

D-XPERT: Automated ESG & Compliance Reporting Engine

Service Definition Document

G-Cloud 15 Framework Agreement

Document Title	Service Definition Document – Automated ESG & Compliance Reporting Engine
Service Type	Software as a Service (SaaS)
Supplier	DIREK LTD
Version	1.0
Status	For publication on the Digital Marketplace
Effective Date	January 2026

Table of Contents

1. Service Overview

The Automated ESG & Compliance Reporting Engine is a cloud-based reporting platform that converts building, portfolio, and operational datasets into audit-ready evidence packs and structured disclosures for Environmental, Social, and Governance (ESG) and compliance use cases.

The Service generates:

- Standards-aligned evidence packs (downloadable packages) suitable for certification audits and internal governance
- Role-specific summaries and performance narratives for non-technical stakeholders
- Traceable metric outputs with an auditable link between source data and reported results

1.1 Service Purpose

The Service automates the creation of traceable, defensible reports for:

- ESG disclosures (including configurable frameworks such as GRI and other buyer-defined disclosure formats)
- Built environment certifications and operational standards (for example BREEAM, WELL, ISO 50001, NABERS)
- Internal and external governance reporting cycles (monthly, quarterly, annual)

1.2 Data Sources

The Service supports building data sources including:

- IoT sensor datasets (for example indoor air quality, energy metering, occupancy-derived metrics where provided by the buyer)
- Building Management System (BMS) data via secure software gateway (D-XPERT Bridge) or supported API
- CSV and JSON uploads for supplementary datasets (for example asset registers, baseline consumption, audit logs)

1.3 Service Limitations

Important: The Service does not certify compliance. It provides evidence packs and analytics to support buyer audit processes and third-party assurance. Buyers remain responsible for selecting applicable reporting frameworks and ensuring organizational policies align with reported claims.

2. Core Functionality

2.1 Evidence Pack Generation

The Service generates evidence packs that include:

- Report scope definition (site, building, portfolio, timeframe, applicable standard or framework)
- Metric calculations with references to underlying source datasets
- Exceptions, anomalies, and completeness checks
- Attachments and supporting artefacts uploaded by authorized users (for example policy documents, commissioning notes)
- Export formats including PDF and structured data exports

2.2 Multi-Standard Alignment

The Service supports templates and mapping logic for multiple reporting frameworks:

- Global Reporting Initiative (GRI)
- BREEAM
- WELL Building Standard
- ISO 50001 (Energy Management Systems)
- NABERS (National Australian Built Environment Rating System)

Buyers can configure:

- Applicable standard version and scope
- Portfolio structure (site, building, floor, zone where relevant)
- Role-based reporting views and outputs

2.3 Traceable Data Lineage

The Service maintains an audit trail from source data to reported metric, including:

- Data source identifier, timestamp, and ingestion record
- Transformation steps (normalization, aggregation, unit conversion)
- Metric definition and calculation parameters
- Report versioning (who generated, when, and what changed)

2.4 AI-Powered Gap Analysis

The Service provides pre-audit readiness checks using AI analysis:

- Missing data detection (time gaps, sensor dropouts, incomplete registers)
- Coverage checks against the selected standard or template requirements
- Flagging of non-conformance risks based on thresholds and rule sets configured by the buyer

2.5 Generative Narratives

The Service produces narrative explanations to accompany metrics and charts:

- Trend interpretation (for example year-on-year comparison, seasonal patterns)
- Anomaly summaries (spikes, drops, missing data impacts)
- Plain-English executive summaries for non-technical audiences

Controls: Narrative outputs reference the underlying metric set and timeframe used. Users can export narratives with the corresponding evidence pack. The Service treats narrative text as supplementary to the traceable metric outputs.

2.6 Scheduled Generation

The Service can generate packs and reports automatically on configurable schedules:

- Monthly, quarterly, or annual schedules
- Per site, per building, or across a portfolio
- Per audience (Board, Facilities Management, Compliance/ESG teams)

2.7 Role-Based Views

The Service provides role-based access to dashboards and outputs:

- **Board and Senior Leadership:** Executive KPIs, risk flags, and narrative summaries
- **Compliance and ESG Teams:** Evidence packs, completeness checks, standards mapping
- **Facilities and Operations Teams:** Source data quality indicators, anomaly lists, corrective action tracking

3. Service Features

- Evidence pack generation with report versioning and audit trail
- Multi-standard reporting templates (configurable)
- Traceable data lineage from ingestion record to metric output
- AI-driven readiness and gap analysis
- Scheduled report generation and automated distribution workflows
- Generative narratives aligned to selected metrics and scopes
- Historical benchmarking against prior periods and baselines
- Export options: PDF for evidence packs, CSV and JSON for datasets and metric outputs
- API access for automated retrieval and downstream integration

4. Service Benefits

- Reduce manual effort in audit preparation through scheduled, repeatable evidence pack generation
- Improve audit readiness through completeness checks and gap analysis
- Reduce spreadsheet error risk by applying consistent calculation logic and traceable lineage
- Provide a single, controlled reporting process across multiple sites and reporting frameworks
- Support governance through role-based outputs and report versioning

5. Service Constraints and Assumptions

Buyer Responsibilities:

- Buyers must provide source datasets via supported APIs, protocols, or CSV and JSON import
- Buyers must provide required metadata (asset register, site and building hierarchy, reporting scope)
- Buyers must ensure accurate source datasets and required governance artefacts
- Buyers remain responsible for selecting applicable reporting frameworks and certification schemes
- Buyers must ensure organizational policies and controls align with reported claims and disclosures

Technical Requirements:

- The Service requires secure outbound internet connectivity from buyer environments where direct integrations are used
- Planned maintenance is scheduled outside core UK business hours with advance notice

6. How Users Access and Use the Service

6.1 Web Access

Access via supported web browsers:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Apple Safari

No client-side application installation is required.

6.2 User Roles

The Service supports role-based access control (RBAC):

- **Administrators:** Tenant configuration and access management
- **Report Authors:** Generate packs, configure schedules
- **Reviewers:** Approve and export packs
- **View-Only Users:** Consume dashboards and exported reports

7. Service Interfaces and Interoperability

7.1 APIs

The Service provides an HTTPS REST API for authorized use:

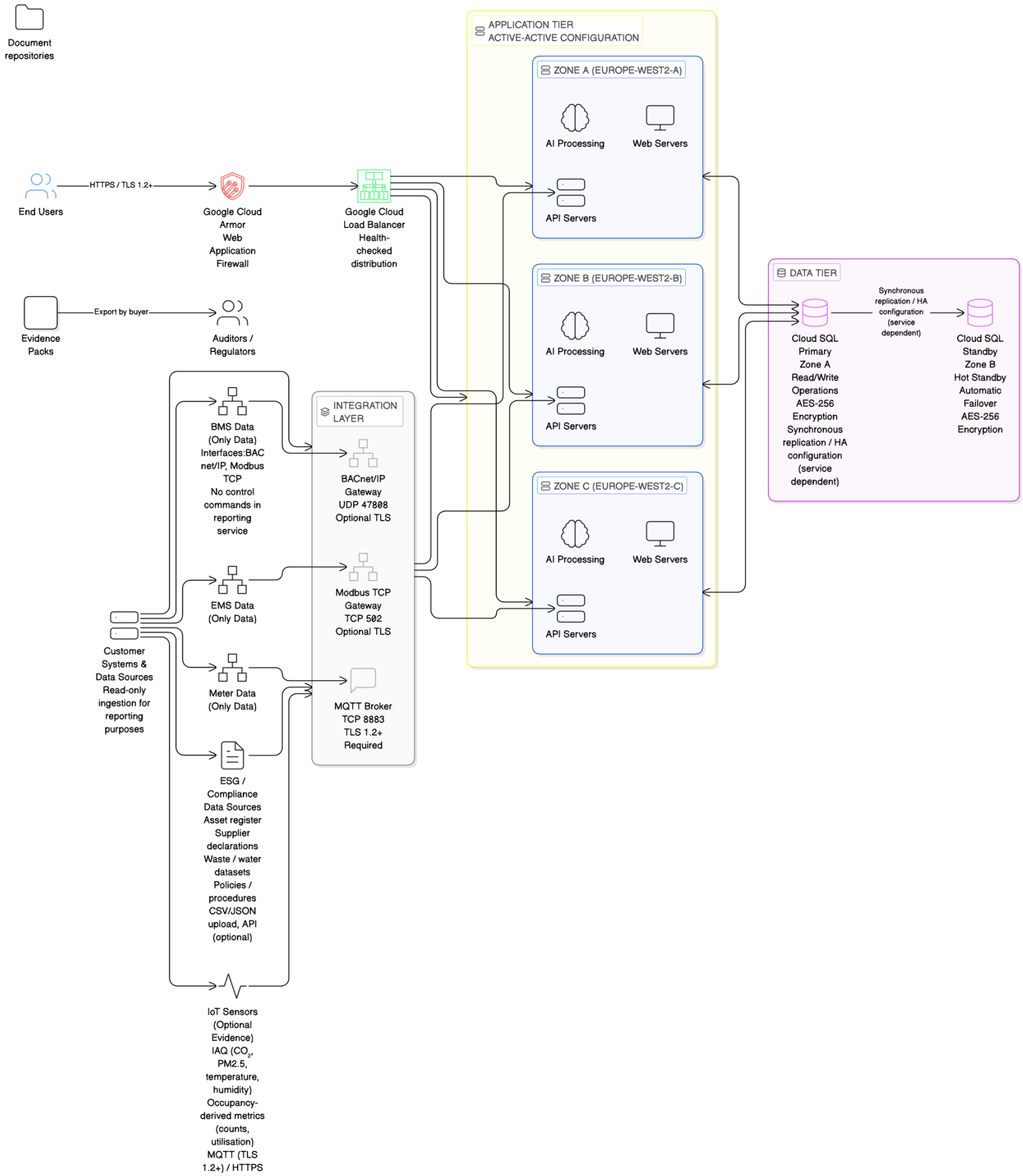
- Retrieve evidence packs and report metadata
- Retrieve metric outputs and source dataset references
- Configure report parameters and schedules (where enabled)
- Subscribe to alerts and events via webhooks (where configured)

The Service provides OpenAPI (Swagger) documentation and a sandbox test environment for integration development.

7.2 Data Import Interfaces

Supported import patterns include:

- API integrations with third-party systems (buyer-provided credentials and approvals)
- Secure streaming where required for near real-time datasets
- CSV and JSON imports for supplementary datasets (asset registers, baselines)


Document repositories
APPLICATION TIER
ACTIVE-ACTIVE CONFIGURATION
ZONE A (EUROPE-WEST2-A)
AI Processing
Web Servers
API Servers
ZONE B (EUROPE-WEST2-B)
AI Processing
Web Servers
API Servers
ZONE C (EUROPE-WEST2-C)
AI Processing
Web Servers
API Servers
DATA TIER
Synchronous replication / HA configuration (service dependent)
Cloud SQL Primary Zone A Read/Write Operations AES-256 Encryption Synchronous replication / HA configuration (service dependent)
Cloud SQL Standby Zone B Hot Standby Automatic Failover AES-256 Encryption
End Users
HTTPS / TLS 1.2+
Google Cloud Armor Web Application Firewall
Google Cloud Load Balancer Health-checked distribution
Evidence Packs
Export by buyer
Auditors / Regulators
INTEGRATION LAYER
BMS Data (Only Data) Interfaces:BACnet/IP, Modbus TCP No control commands in reporting service
BACnet/IP Gateway UDP 47808 Optional TLS
EMS Data (Only Data)
Modbus TCP Gateway TCP 502 Optional TLS
Meter Data (Only Data)
MQTT Broker TCP 8883 TLS 1.2+ Required
Customer Systems & Data Sources Read-only ingestion for reporting purposes
ESG / Compliance Data Sources Asset register Supplier declarations Waste / water datasets Policies / procedures CSV/JSON upload, API (optional)
IoT Sensors (Optional Evidence) IAQ (CO_2, PM2.5, temperature, humidity) Occupancy-derived metrics (counts, utilisation) MQTT (TLS 1.2+) / HTTPS

8. Data Management

8.1 Data Storage Location

All data storage and processing occurs within the United Kingdom.

8.2 Audit Logging and Retention

- User activity audit logs retained for at least 12 months
- System logs retained for at least 12 months

8.3 Data Export

Export formats include CSV and JSON for structured exports and PDF for evidence packs. Exports are available via the user interface and API.

8.4 End-of-Contract Data Extraction and Deletion

Buyers can export their datasets and generated reports prior to contract end using self-service export and API methods.

On contract termination:

- User access is revoked after the contract end date
- Data is retained for a defined grace period to support final extraction
- Data is then securely deleted in accordance with the supplier's sanitization and deletion processes

9. Security

9.1 Data in Transit

- TLS 1.2 or above between buyer and supplier networks
- TLS 1.2 or above within the supplier network

9.2 Data at Rest and Media Protection

The Service uses cloud data center controls including:

- Physical access controls aligned to recognized standards (for example CSA CCM v4.0, SSAE-18, ISAE 3402)
- Encryption of storage media
- Secure sanitization processes (cryptographic erasure, secure erase, and physical destruction as applicable)

9.3 Penetration Testing

Penetration testing occurs at least every 6 months using a CREST-approved provider (IT Health Check).

9.4 Identity and Access Management

- User authentication supports multi-factor authentication (MFA) and identity federation
- The Service applies least privilege access controls and records administrative actions for audit

9.5 Secure Development and Vulnerability Management

- Secure development practices include peer review, continuous integration and continuous deployment (CI/CD) controls, and environment segregation
- Vulnerability scanning and remediation timelines are based on severity, aligned to recognized guidance (including NCSC-aligned practices)

9.6 Incident Management

- Incident management follows an NCSC-aligned lifecycle with defined runbooks and post-incident review for significant events
- For personal data breaches, the Service supports notification processes aligned with GDPR timescales

10. Availability and Resilience

10.1 Availability Target

The supplier targets 99.9% monthly uptime for the production service, excluding planned maintenance and force majeure events.

10.2 Resilience Approach

- The Service is hosted in a UK cloud region using a multi-zone architecture to reduce single points of failure
- The platform uses load balancing and self-healing patterns to maintain service continuity during component failure

10.3 Outage Reporting

The supplier maintains a status page and provides incident updates through published channels.

11. Support

11.1 Support Channels

- Email helpdesk and online ticketing support
- Phone support and web chat support during UK business hours

11.2 Support Hours and Response Targets

Support Hours: 09:00 to 17:00 UK time, Monday to Friday (excluding public holidays)

Target Response Times:

Priority Level	Response Target
Priority 1 (Critical Outage)	Response within 1 hour
Priority 2 (Major Issue)	Response within 4 hours
Priority 3 (Minor/General)	Response within 1 business day

12. Onboarding, Training and Documentation

12.1 Onboarding

- Account provisioning via secure invitation and role assignment
- Data onboarding using standard templates and API tooling for metadata and historical imports

12.2 Training and Documentation

- Remote training options and webinars for user enablement
- Documentation provided in HTML and PDF formats

12.3 Accessibility

The Service aims to meet Web Content Accessibility Guidelines (WCAG) 2.2 Level AA for the web interface and support channels.

Accessibility testing includes screen reader compatibility and keyboard-only navigation for core user journeys.

13. Compliance and Audit Support

The Service Supports:

- Traceable reporting outputs with version history and audit trails
- Evidence pack exports suitable for third-party assurance processes
- Configurable reporting schedules aligned to internal and external deadlines

The Buyer Remains Responsible For:

- Selecting applicable reporting frameworks and certification schemes
- Providing accurate source datasets and required governance artefacts
- Ensuring organizational policies and controls align with reported claims and disclosures

— End of Service Definition Document —