HSE Incident Management & Reporting

Service Definition Document

Prepared by:	**OfficeLabs Ltd** Queensgate House 48 Queen Street Exeter, EX4 3SR +44 (0)1392 240365
Version:	Issued 1
Last revised:	10/01/2026
Version History:	1

1. SERVICE OVERVIEW

HSE Incident Management & Reporting is a cloud-based incident management service designed to support the structured reporting, management, and analysis of health, safety, cyber, and business continuity incidents within organisations.

The service enables organisations to capture incidents consistently, assess regulatory reporting requirements such as RIDDOR, manage follow-up actions, and maintain an auditable record of incidents and outcomes. It is typically used to replace paper-based or fragmented reporting processes with a single, governed system aligned to organisational and legal obligations.

The service is designed for organisations that require a controlled, auditable approach to incident management and regulatory reporting. It can be used independently or alongside broader information governance, reporting, and assurance services delivered under separate engagements.

2. PRODUCT CAPABILITIES

The service provides the following core capabilities:

- Structured capture and management of health, safety, cyber, and business continuity incidents
- Assessment of incidents against RIDDOR reporting criteria
- Centralised incident registers with status tracking and ownership
- Configurable incident forms, classifications, and follow-up actions
- Storage of supporting evidence, documents, and images
- Audit and reporting features to support compliance and assurance
- Management information and analytics to identify trends and risks

The service focuses on consistent reporting, regulatory awareness, and auditability, rather than informal or ad hoc incident logging.

3. DEPLOYMENT AND OPERATION

HSE Incident Management & Reporting is delivered as a multi-tenant SaaS service hosted in the public cloud, with logical separation between customer environments.

Customers access the service via a secure web interface. No client-side software installation is required. The service operates within supported Microsoft 365 environments, using configuration and permissions provided by the customer.

The platform leverages the resilience, monitoring, and recovery capabilities of the underlying cloud infrastructure. Operational management of the service is handled by OfficeLabs.

4. CONFIGURATION AND CUSTOMISATION

The service is configured through administrative settings rather than bespoke development.

Customers can configure incident types, reporting forms, classifications, workflows, notifications, roles, permissions, and reporting views within defined parameters. The core platform is not custom-built per customer, and no custom code is required for standard operation.

This configuration approach supports consistent incident handling and predictable reporting across the organisation.

5. ONBOARDING AND USE

Customers typically begin by defining incident categories, reporting requirements, and internal responsibilities.

Onboarding focuses on configuring reporting forms, validating RIDDOR assessment logic, and confirming workflows for review and follow-up. Time to initial operational use varies depending on organisational complexity and readiness.

Optional onboarding assistance, configuration support, and advisory services are available under separate Cloud Support service listings.

6. SUPPORT AND ASSURANCE MODEL

Standard SaaS support is included with the service subscription and covers incident logging, investigation, and resolution of software-related issues.

Enhanced support options, onboarding assistance, advisory services, and ongoing managed support are available separately under OfficeLabs Cloud Support service listings. These services are not included as part of the standard SaaS product.

7. SECURITY, AVAILABILITY, AND COMPLIANCE

The service operates within an ISO/IEC 27001–aligned information security management framework. Data is protected using industry-standard security controls, including encryption in transit and appropriate access controls.

Availability and resilience are provided through the underlying cloud hosting platform. No formal uptime service level agreement is included as part of the standard service.

Detailed security, compliance, and assurance controls are described in the Digital Marketplace listing and supporting assurance documentation.

8. DATA, EXIT AND COMMERCIAL NOTES

Customers retain ownership of their data at all times. Incident records, reports, and supporting metadata can be exported using supported formats prior to contract termination.

At the end of the contract, access to the service is withdrawn in line with agreed notice periods. No automatic data migration or remediation is included as part of the service.

Pricing, contract terms, and any trial or assessment arrangements are defined in the Digital Marketplace listing and associated commercial documentation.

9. RELATIONSHIP TO OTHER SERVICES

HSE Incident Management & Reporting is commonly used alongside information governance, reporting, assurance, and compliance support services. These services are optional and are delivered under separate contracts or service listings where required.