Managed Data Loss Prevention Monitoring

G-Cloud 15 Service Definition

Table of Contents

Introduction

Ekco Cloud & Security is an ideal partner for public sector organisations seeking a **secure, compliant, and scalable provider** via G Cloud 15.

We make it easier for IT teams to innovate, scale, manage, troubleshoot and secure. Across cloud, business continuity, security and workspace solutions, we enable the growth our customers want with the team they already have.

Through our security-first approach, large specialist workforce, AI-enhanced operations, and proven delivery capability, we help organisations:

- Modernise securely
- Strengthen cyber resilience
- Reduce operational risk
- Improve service continuity
- Deliver safer, more reliable digital services for our customers and their stakeholders.

Ekco's end-to-end cloud and cyber services are well matched to **G Cloud purchasing needs and public sector transformation goals**.

Managed Data Loss Prevention (DLP) Service

Service Overview

Ekco's **Data Loss Prevention (DLP) Monitoring Service** helps organisations protect against the loss and misuse of sensitive data. Our team designs, implements, and configures data classification and DLP controls aligned to your organisation's risk profile and compliance needs, then continuously monitors DLP activity to detect potential data exposure, misuse, or policy violations.

This service combines three core capabilities:

- **Data classification and labeling** to ensure sensitive content is consistently identified.
- **DLP policy design and configuration** to prevent data leakage across email, endpoints, Teams/SharePoint/OneDrive, and other supported channels.
- **Ongoing monitoring and event response support** to maintain visibility into DLP alerts and trends and to help reduce the likelihood and impact of data loss incidents.

Features

The key features of the Managed Data Loss Prevention Service are:

Data Classification & Sensitivity Enablement

- Configuration of Microsoft Purview Information Protection components that support classification (e.g., sensitivity labels, label policies, and supporting settings).
- Enablement and tuning of Sensitive Information Types (SITs) and classification methods (built-in and custom where required).
- Guidance for aligning classification to business data categories (e.g., PII, PCI, PHI, confidential IP, regulated data).

DLP Policy Design & Implementation

- Creation and configuration of **DLP policies** to help reduce the risk of:
    - Inappropriate external sharing restrictions
    - Sensitive data in email and Teams messages
    - Sensitive files in SharePoint/OneDrive
    - Endpoint controls for copying to USB, printing, clipboard, browser uploads (where licensed/supported)

- Definition of **policy rules**, thresholds, conditions, and exceptions to reduce noise and support business workflows.
- Configuration of **user notifications, policy tips, and remediation actions** (block, restrict, warn, allow with justification, etc.).
- Phased rollout support (e.g., **audit mode → warn → block**) to minimize user disruption.

Monitoring, Alert Triage & Operational Oversight

- Continuous monitoring of **Purview DLP alerts and events** to identify suspicious or high-risk activity.
- Alert triage and categorization (e.g., true positive, false positive, needs tuning, training opportunity).
- Identification of trends (repeat offenders, risky channels, common false positives, emerging data types).
- Escalation recommendations and evidence gathering to support incident handling workflows.

Policy Tuning & Continuous Improvement

- Regular refinement of rules and exceptions based on observed events and business feedback.
- Optimization to reduce false positives and close policy gaps.
- Recommendations for expanding coverage (additional locations, new sensitive data types, improved labeling).

Reporting & Service Communications

- Regular operational reporting (volume of events, severity, top policies triggered, top data types, affected users/channels).
- Daily escalations of incidents to the client for HR or legal to action.
- Documentation of configured policies and classification standards (as-built view).

Benefits

The key Benefits of the Managed Data Loss Prevention Service are:

- Reduced Risk of Data Loss and Exposure
    - Prevents accidental or intentional leakage of sensitive data through common collaboration and sharing channels.

- Improves detection of risky behavior early, reducing the likelihood of major incidents.

- Consistent, Defensible Data Handling
  - Establishes repeatable, auditable controls for protecting regulated or confidential information.
  - Helps enforce policies aligned to compliance requirements and internal governance standards.
- Improved Visibility and Control
  - Centralized insight into where sensitive data is being shared, how it's moving, and which controls are most effective.
  - Ability to identify systemic issues (e.g., business process gaps, training needs, over-permissive access).

Service Outline

Service Option - Essentials

The ‘ **Essentials’** Service Level is an entry level Data Loss Prevention service aimed at small / medium sized organisations that require a basic level of DLP policies and monitoring. As part of the Essential service, Ekco will:

- Enable and configure Microsoft Data Classification with a “standard” sensitivity label schema.
- Enable and configure Microsoft DLP to monitor email for high-risk Data Loss events.
- Monitoring and alerting service for data loss events with daily escalations.
- Quarterly DLP reporting pack.
- Standard training and documentation for end-users on Data Classification and Data Loss Prevention.

The **Essentials** Service Level is an entry-level **Microsoft Purview Data Loss Prevention** service designed for small to medium-sized organisations that require a baseline level of DLP capability and monitoring. As part of the Essentials service, Ekco will:

- Enable and configure **Microsoft Purview Data Classification** using a **standard sensitivity label schema**.
- Enable and configure **Microsoft Purview DLP for Exchange Online** to monitor email for **high-risk data loss events**.
- Provide **monitoring and alerting** for data loss events, including **daily escalations**.
- Provide a **quarterly DLP reporting pack**.
- Provide **standard end-user training and documentation** covering Data Classification and Data Loss Prevention.

Service Option - Standard

The Standard Service Level builds on Essentials by tailoring classification to your organisation and extending DLP coverage beyond email to include Microsoft Teams and endpoints. As part of the Standard service, Ekco will:

- Design and implement customised sensitivity labels and classification schema aligned to your business data and handling requirements.

- Enable and configure Microsoft Purview DLP across:
    - Email
    - Microsoft Teams (chat and channel messages, where supported)
    - Endpoints (to monitor and help prevent risky user actions on managed devices, where supported)
- Provide monitoring and alerting for data loss events, including daily escalations.
- Provide regular DLP reporting covering email, Teams, and endpoint trends and policy effectiveness (cadence aligned to service governance).
- Provide tailored training and documentation to support adoption of the customised labels and extended DLP controls.

Project Implementation

Onboarding a client into their new contracted services requires a structured process to ensure a smooth transition and clear expectations. The following process provides a high-level overview of our bespoke implementation plan.

1. Pre-Implementation Preparation

Initiate internal communications with internal stakeholders, confirming contracted deliverables, and bespoke scope of works. Confirm dedicated resource across the business depending on function.

2. Client Engagement

Initiate communication with the customer's key stakeholders to discuss the onboarding process, timescales (including support go live date), expectations, and roles.

3. Business Intelligence Discovery

Conduct a thorough assessment of the client's internal processes, gather key information regarding end users, business requirements, 3rd party data, user account management and operational workflows.

4. Technical Deliverables

Complete a detailed assessment of the customer's existing IT infrastructure, cloud, network, applications, and systems. Identify different user roles and access requirements. Deploy and document toolsets. Develop a comprehensive knowledge base containing FAQs, troubleshooting guides, and best practices based on their current environment.

5. NOC and SOC Deliverables

Configure and deploy and contracted NOC and SOC toolsets, complete basic security checks such as MFA and password policies.

6. Points of Attention

Based on technical audits and client concerns, create a Points of Attention document with the assigned account manager to review with the client

7. Acceptance into Service

Schedule and complete the acceptance into service with the required internal departments.

8. "Go Live"

Handover to our required internal stakeholders and departments to take on the clients contracted deliverables. Implementation team to provide 2 weeks of enhanced support to our internal teams and the client, ensuring support, access and processes are running smoothly.

Why Ekco

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security

Security-First Cloud Services Aligned to Government Standards
Ekco Cloud & Security is a leading UK and European **security-first managed cloud provider**, delivering deep expertise across cyber security, identity, and cloud. Our services align with **NCSC guidance, the Cyber Assessment Framework (CAF), NHS DSPT**, and wider public sector assurance requirements.

Our proven **Assess → Protect → Detect → Respond** model supports secure-by-design digital transformation across hybrid and distributed environments—directly addressing public sector risk and resilience priorities.

End-to-End Capabilities Mapped to G Cloud 15
Public sector buyers need suppliers that can deliver migration, protection, management, and optimisation through a single, accountable partner. We provide a **fully integrated cloud and security portfolio**, including:

- Cloud migration and managed cloud operations
- Security and infrastructure management
- Identity security and privileged access management
- Secure modern architecture design
- Real-time threat detection and incident response

These services align directly with **G Cloud 15 lots and purchasing criteria**, enabling organisations to modernise securely while managing complex legacy estates.

Scalable Expertise and Sovereign Delivery
With **1,000+ cloud and security specialists across the UK and Europe**, we offer the scale, depth, and resilience required to support mission-critical public services. A dedicated **identity security practice** provides mature capability for access control and Zero Trust adoption—an increasingly critical requirement across government organisations.

Tailored Solutions for Resource-Constrained Organisations
Recognising the challenges faced by councils, NHS trusts, education, and blue-light services, we offer **cost-effective, scalable cloud and cyber security solutions** designed for organisations with limited internal capacity.

These services protect against phishing, ransomware, and social engineering while meeting G Cloud's expectations for solutions that are secure by default, rapidly deployable, and low overhead.
AI-Enhanced Security Operations
We embed **AI into daily security operations**, improving analyst productivity and response effectiveness. AI-assisted services accelerate:

- Incident triage and prioritisation
- Threat analysis and vulnerability summarisation
- Reporting accuracy and audit readiness

This enables faster outcomes and stronger protection for public bodies operating with limited staffing.

Public Sector-Focused Engagement Model

Our partnership-led approach aligns with government procurement expectations, offering:

- Dedicated, accountable delivery teams
- Transparent SLAs and service reporting
- 24/7 support with local expertise
- Predictable commercial and contract models

This ensures we act as a **strategic long-term partner**, not a transactional supplier.

Global Recognition and Strategic partnerships

These global accreditations partnerships show our commitment to customer satisfaction, data safety, security and overall quality. We're independently audited every year to give our customers confidence in our approach.

From agile managed cloud platforms to next-gen security services that supercharge defences, our local team of specialists provide proactive, round-the-clock management. With one Ekco Cloud & Security team delivering a combination of services, our customers quickly gain control and visibility over their technology.