# Sensitivity Labelling Uplift

## Introduction & Purpose

This engagement helps organisations improve visibility, control, and governance of sensitive information by deploying Microsoft Purview **Sensitivity Labels**.

Labelling is not just about “putting a sticker on a file.” When used correctly, labels:  
- Drive **consistent data classification** across Microsoft 365 (emails, files, Teams, SharePoint).  
- Enable **automatic protection actions** (encryption, watermarking, access restrictions).  
- Serve as a **foundation for compliance** (retention, auditing, DLP integration).

The purpose of this session is to help the customer **assess current labelling maturity**, align to a consistent taxonomy, and implement quick wins that will uplift their overall security and compliance posture.

This is not a full **labelling taxonomy design project** — it is an advisory to build confidence, deliver quick value, and guide next steps.

## Rules of Engagement

* **Focus on business alignment**: talk about protecting customer data, contracts, and intellectual property — not only about Purview UI clicks.
* **Stay out of deep technical design**: avoid diving into XML, regex, or custom classifiers unless there’s a follow-up engagement.
* **Strategic framing**: link labelling to compliance frameworks (Essential 8, ISO 27001, GDPR, PSPF).
* **Avoid over-engineering**: encourage customers to start simple (3–4 labels) and expand as adoption grows.
* **Red flags**: if the customer insists on 20+ labels up front or complex auto-labelling policies without discovery, steer them toward a **Label Taxonomy Design** engagement.
* **Keep adoption in focus**: emphasise communication, training, and monitoring alongside technology.

### Talking Points

* Anchor the customer on “secure-by-default before scale”: start with a small, safe baseline (few labels, clear owners), then expand.
* Use the blueprint to justify default enforcement choices (e.g., requiring justification for label downgrades, auditing before blocking).
* Position it as Microsoft’s reference approach you’re aligning to, not a custom E2 opinion.

## Step-by-Step Delivery

### Step 1 – Define Business Goals

* Ask: *Why do you need sensitivity labels?* (compliance, customer data protection, insider risk, Copilot readiness).
* Establish which business units or data categories are most at risk.
* Align to regulatory requirements (ACSC, ISO, GDPR).
* Clarify whether the drivers include Copilot or AI adoption. Without consistent labelling, Copilot could surface sensitive data inappropriately.

### Step 2 – Review Current Labels & Usage

* If labels exist, review current configuration and adoption rates.
* Identify unused or overlapping labels.
* If no labels exist, capture initial requirements (Public, Internal, Confidential, Highly Confidential).

### Step 3 – Align to a Taxonomy

* Map labels to the organisation’s information classification scheme.
* Recommend a **simple starter taxonomy** (e.g., Public / Internal / Confidential / Restricted).
* Discuss naming conventions, icons, colours, and policy actions.
* Use the Secure-by-Default blueprint to justify keeping the starter taxonomy lean — build confidence before scaling to dozens of labels.

### Step 4 – Build & Test Auto-Label Policies

* Configure 1–2 **pilot policies** in audit mode (e.g., auto-apply “Confidential” for files with TFNs or credit card numbers).
* Walk through how auto-labelling integrates with **DLP** and **eDiscovery**.
* Highlight Copilot dependencies: without consistent labelling, AI could surface sensitive data inappropriately.

### Step 5 – Adoption & Governance

* Define who owns labels (Compliance vs IT).
* Create a governance process for approving new labels.
* Train users on how and when to apply labels.
* Review adoption reports after 2–4 weeks and refine policies.
* Review user adoption reports at 2–4 weeks, not just policy matches, to understand how labels are actually being applied in daily work.

## Engagement Outputs

At the end of this engagement, the customer should have:  
- A **baseline sensitivity label taxonomy** (3–4 recommended starter labels).  
- 1–2 **pilot auto-labelling policies** configured in audit mode.  
- A **governance guide** outlining label ownership and change management.  
- An **adoption plan** with communication and training guidance.  
- A list of **next steps** for scaling labelling and integrating with DLP/IRM. - A defined reporting process (e.g., monthly usage/adoption reports for IT and quarterly summaries for executives).

## References & Learning Resources

* [Microsoft Purview — Secure by Default (Blueprint, PDF) Practical guidance for standing up Purview in a secure-by-default posture, including baseline controls and deployment patterns that underpin labels, DLP, and broader governance.](https://github.com/microsoft/purview/blob/95e2d91f802804d17f82dd58fd9fe9ce0c470106/purview-blueprints/Secure%20by%20default%20with%20Microsoft%20Purview.pdf)
* [Microsoft Learn – Sensitivity Labels Overview](https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels)
* [Best Practices for Sensitivity Labels (Microsoft)](https://learn.microsoft.com/en-us/purview/data-gov-best-practices-sensitivity-labels)
* [Syskit – Governance Tips for Sensitivity Labels](https://www.syskit.com/governance-handbook/sensitivity-labels/best-practices-sensitivity-labels/)
* [Top 5 Tips for Sensitivity Labels (HubSite365)](https://www.hubsite365.com/en-ww/crm-pages/my-top-5-tips-for-sensitivity-labels-in-microsoft-purview.htm)
* [Copilot & Sensitivity Labels – Why They Matter](https://teamcopilot.nl/2025/02/15/building-a-sensitivity-labeling-strategy-for-microsoft-purview-protecting-data-in-the-age-of-copilot/)
* [Nikki Chappell – Purview DLP & Label Best Practices](https://nikkichapple.com/microsoft-purview-dlp-best-practices/)