



05 November 2025

Case Study: The Classification/Collaboration Gap

Enabling Secure External Exchange for ISO 27001 Environments

1. The Challenge: Security vs. Business Velocity

Client Profile: *Apex Dynamics*, a medium-sized engineering firm specializing in complex industrial automation, operates under a robust Information Security Management System (ISMS) certified to **ISO/IEC 27001**.

The Classification Scheme: *Apex Dynamics* employed a standard, internally focused classification structure:

- **PUBLIC:** Data cleared for general, unrestricted release.
- **INTERNAL:** Business-sensitive data intended for *Apex* employees only.
- **CONFIDENTIAL:** Highly sensitive trade secrets, PII, or strategic plans, strictly limited to senior management and specific project teams within *Apex*.

The Problem: *Apex Dynamics* was awarded a high-value contract requiring close collaboration with their specialized manufacturing partner, *Precision Systems*. This partnership was vital, but it required *Apex* to share some documents classified as **INTERNAL** (e.g., specific design tolerance data and detailed component blueprints) and even **CONFIDENTIAL** (e.g., intellectual property related to proprietary control algorithms).

The current security policy presented an impossible choice:

1. **Restrict Business:** Refuse to share the data, which would violate the contract and halt the project.
2. **Downgrade Security:** Downgrade the classification of sensitive documents to **PUBLIC** to permit exchange, thereby violating ISO 27001 control A.5.10 and exposing critical IP.

The standard ISO 27001 classifications offered no mechanism to securely *release* sensitive data to a trusted, external party while maintaining the required protection level.

2. The Practical Gap in Standard Classification

Standard classifications (Public, Internal, Confidential) are **Protection Levels** defined by the originating organization. They fail to account for the need for **Dissemination Control** between two distinct legal entities.

The internal-only model treats any external party (including a trusted, contracted partner) the same as the public internet. The system could not differentiate between:

- A document marked **INTERNAL** for internal *Apex* employees.
- The **SAME** document marked **INTERNAL** but released to *Precision Systems* under a protective agreement.

Apex needed a way to extend the trust boundary for specific data to specific partners without compromising the data's inherent protection requirement.

3. The Solution: Introducing the Release Marking Mechanism

Apex Dynamics implemented a new security procedure that paired the existing internal **Protection Level** (INTERNAL or CONFIDENTIAL) with a required **Release Marking** for external sharing with trusted partners.

The mechanism defined two mandatory conditions for sharing any data classified above PUBLIC:

1. **Formal Agreement:** A formal agreement, such as a Non-Disclosure Agreement (NDA) or a comprehensive Master Services Agreement (MSA), must be in place. This agreement explicitly required the external partner (e.g., *Precision Systems*) to implement security controls equivalent to the required Protection Level (INTERNAL or CONFIDENTIAL) of the shared information.
2. **Dual Marking:** The document's marking was updated to clearly reflect both the required *Protection Level* and the *Dissemination Control* (or Release Marking).

Example Markings:

Protection Level	Release Marking (External)	Resulting Action/Business Rule
INTERNAL	RELEASED TO: Precision Systems	<i>Precision Systems</i> must protect this data as INTERNAL data, limiting access to personnel on the MSA.
CONFIDENTIAL	RELEASED TO: Alpha Partner, Precision Systems	<i>Alpha Partner</i> and <i>Precision Systems</i> must protect this data as CONFIDENTIAL , limiting access strictly according to the NDA terms.

4. Results and Business Enablement

By adopting the Release Marking mechanism, *Apex Dynamics* achieved the following:

- **Contract Fulfilment:** They could securely share the necessary design and IP data with *Precision Systems*, enabling the contract to proceed without delay.
- **Compliance Maintained:** ISO 27001 integrity was preserved because the classification (the required protection level) was not downgraded. Instead, the security boundary was *legitimately extended* by contract, fulfilling the requirements of risk acceptance and due diligence control A.5.15 (Information security in supplier relationships).
- **Accelerated Collaboration:** Project managers no longer had to wait for lengthy, risk-laden exceptions or laboriously redact documents. They could utilize the authorized Release Marking, streamlining secure B2B exchange.

5. Enabling the Solution with ClassifyIt

The crucial success factor was ensuring the Release Marking policy was *enforced* consistently across all digital documents and amongst the 2 companies: *Apex Dynamics* and *Precision Systems*.

ClassifyIt provided the technical and advisory framework for this solution:

- **Technical Enforcement:** ClassifyIt's data classification tool was integrated to mandate and automate the **Dual Marking** process. When a user attempted to share an INTERNAL document externally, the tool prompted them to select a pre-authorized **Release Marking** (e.g., *Precision Systems*) from a whitelist, ensuring the correct metadata and visual label were applied before the file was released. This fulfilled the ISO 27001 requirement for procedural enforcement.
- **Advisory Support:** Beyond the software, ClassifyIt's support helped *Apex Dynamics* bridge the gap between policy and legal reality. ClassifyIt support assisted in defining the specific contract language and security controls required in their MSA/NDA templates, ensuring that *Precision Systems* was legally and contractually bound to the required protection levels, making the **Release Marking** auditable and compliant. The same support was provided to *Precision Systems*.

This case study demonstrates that a modern, practical Information Security Management System (ISMS) must evolve beyond simple internal protection levels to incorporate effective, auditable dissemination controls that facilitate secure, controlled collaboration.

Visit: <https://classifyit.eu>