SECURING SENSITIVE DATA: THE POWER OF INFORMATION RIGHTS MANAGEMENT (IRM)

An overview of how Information Rights Management (IRM) empowers organizations to control and protect their critical digital assets

INTRODUCING INFORMATION RIGHTS MANAGEMENT (IRM)

Digital Asset Control

IRM allows organizations to control how digital assets, such as documents, emails, or images, are accessed, shared, and used.

Embedded Security Policies

IRM embeds security policies that remain with the data throughout its lifecycle, ensuring protection even as the data moves.

Granular Protection

IRM provides a granular level of protection by assigning usage rights at the file or object level, determining who can view, edit, print, or forward the content.

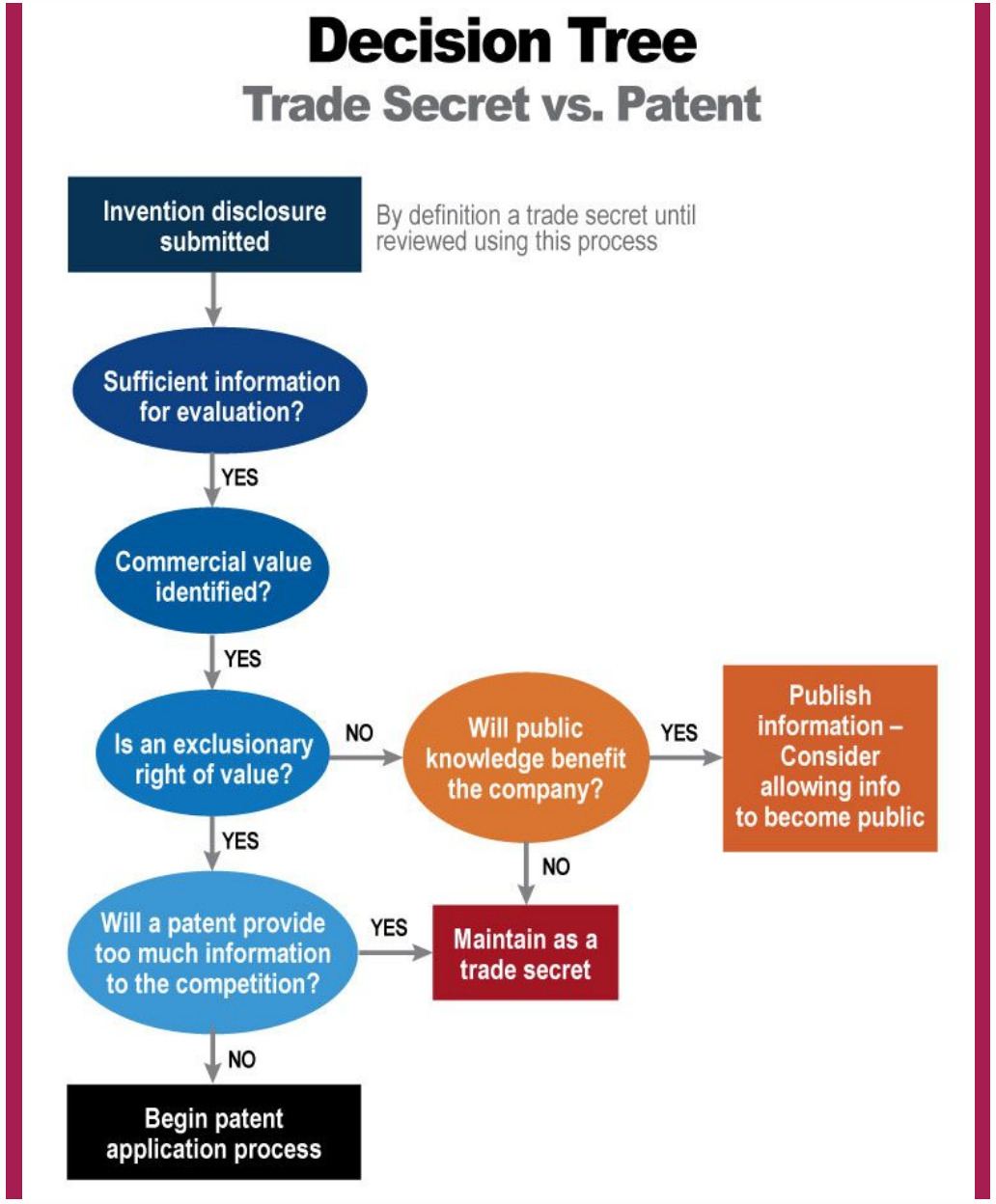
Automation and Integration

IRM solutions can be integrated with existing classification labels to automatically apply the appropriate usage rights and policies.

IRM is a critical component of a comprehensive data security strategy, ensuring that sensitive and proprietary information remains protected throughout its lifecycle, even as it moves across cloud and on-premises environments.

PROTECTING INTELLECTUAL PROPERTY WITH IRM

Information Rights Management (IRM) safeguards valuable intellectual property, such as trade secrets, patents, and proprietary data, by restricting unauthorized access and actions. IRM solutions offer dynamic controls that ensure only authorized individuals can interact with these critical assets, protecting an organization's competitive edge.



KEY TRAITS OF IRM TOOLS

Persistent Protection

Usage rights and security policies 'travel' with the file, enforcing restrictions even when accessed offline or outside the network

Integration with Identity and Access Management

IRM tools link with corporate directories and federation services to verify user credentials and apply data classification-based permissions

Policy Flexibility and Automation

Administrators can define templates that map classification levels to IRM rules, enabling consistent deployment across multiple file repositories and collaboration tools

Auditing and Revocation

IRM solutions maintain detailed logs of user actions, aiding in incident response and compliance audits, and offer the ability to instantly revoke access if needed

CASE STUDY: LEVERAGING IRM IN A GLOBAL MANUFACTURING FIRM

Assessment and Classification

The firm built on its existing data classification framework, labeling CAD drawings and design documents as "company confidential".

IRM Deployment

An IRM solution was integrated with the firm's collaboration platform, automating the application of rights restrictions whenever employees uploaded new design files. Engineers retained editing privileges, but printing or external sharing was limited to a subset of senior staff.

Cross-Border Controls

Because some designs were subject to export control laws, the IRM system leveraged location-based rules. If access was requested from outside approved territories, the system either blocked the request or required additional authorization.

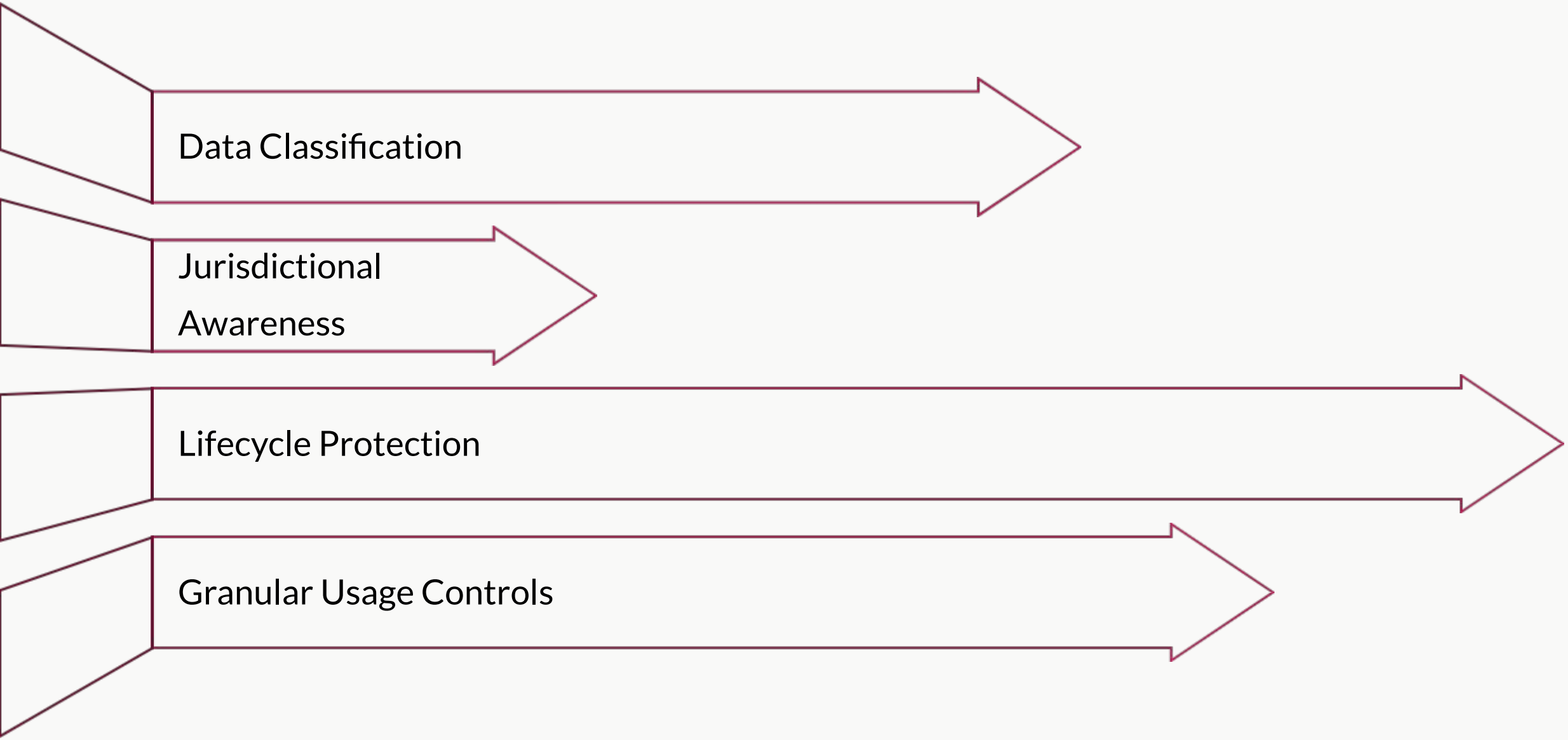
Continuous Monitoring and Alerts

The firm configured real-time alerts for any anomalies, such as repeated failed attempts to download or copy restricted files. Security teams could then revoke access instantly, preventing data exfiltration.

Results

The solution significantly reduced IP leakage concerns, aligning with international compliance standards and local regulations. Audits demonstrated that each design file's usage and distribution were tightly controlled, instilling confidence among investors and government stakeholders.

IRM IN THE DATA SECURITY LANDSCAPE



MAINTAINING DATA SECURITY WITH IRM

Comparison of IRM control effectiveness across cloud and on-premises environments