M-Files®

The Smarter Way to Work.

6 BEST PRACTICES FOR AUTOMATING SECURITY AND COMPLIANCE WITHIN YOUR INFORMATION MANAGEMENT SYSTEM

Automate Security and Compliance within Your Information Management System

Are security and compliance requirements keeping you up at night? Let's face it - you're not alone.

Even with what seems like a growing number of security and compliance requirements that need to be monitored and carefully applied - it sometimes seems like an uphill battle - given that these are seldom at the top of any list when it comes to a core business strategy. There are several factors as to why this is the case - but typically it's due to the constant pressures of generating new revenue and growing your customer base.

And it's not because security and compliance are deemed unimportant - it's more of a prioritization casualty that sometimes becomes overlooked. However, regardless of the reason - security and compliance play a big role in keeping you in business and safeguarding your brand's reputation.

It all starts with compliance policies - as this is the pathway for meeting the various legal, industry, or company requirements. And given the uncertainty of new threats everyday - those policies will need to be extremely adaptable to limit the overall business and risk environment.

And it's certainly not easy—as multiple challenges exist along the way that may impact your strategy, including:

- **Malware threats:** These threats evolve and change at a rapid pace. Every day, there are 50,000 new malicious programs (malware) and potentially unwanted applications (PUA)[i].
- **Complex IT environments:** These are now becoming increasingly complex, with distributed hybrid and multi-cloud implementation.
- **Multi-tiered organizational structure:** As businesses grow, the organizational structure may consist of multiple layers and a hierarchy that calls for agile management of user and access rights.
- **Remote and hybrid work:** Remote work challenges your security policies as it puts your staff outside the perimeter of the company network.
- **Constantly changing regulations:** Compliance requirements are getting stricter, and there are different requirements and standards across different regions and industries.

While these challenges may not seem new, the increasing level of potential impact certainly is, as threats continue to grow every year that your business operates.

Lay of the land

Security and compliance are both critical for businesses today, and they cannot be separated from one another. Trust and reputation can only be lost once and are almost impossible to recover from potential data breaches or lack of compliant processes.

According to a recent 2021 study[ii], **the average cost of a data breach last year was $4.24 million**, comprising hundreds of cost factors—legal, regulatory, technical activities, loss of brand equity, customer turnover and drain on employee productivity.

The increased need for security and compliance

So, what's driving this need for increased security and compliance? Various legal requirements primarily drive the need for enhanced security and compliance. The massive risk potential of non-compliance with security regulations can expose your business to legal penalties, financial forfeiture, and material loss.

For example, organizations in breach of the General Data Protection Regulation (GDPR) can be fined up to 4% of annual global turnover or 20 million Euros (whichever is greater). And it's only going to become more stringent, as last year (between January 2020 and January 2021), penalties under the GDPR totaled a record €158.5 million ($191.5 million). So far, the biggest individual fine for GDPR breach is a 50-million euro fine for Google confirmed in 2020.[iii]

The three pillars of information security

1. **Confidentiality:** Ensuring that confidential information stays confidential. Your information management system should make sure that access rights and visibility of data are easily maintained to ensure confidentiality and privacy.
2. **Integrity:** Data needs to stay secure from accidental edits or unauthorized access. Al activity needs to be easily evidenced with a complete audit trail covering all data transactions.
3. **Availability:** Information needs to be available for everyone who needs it, but only for those who have proper access privileges.

Compliancy Challenges

Visibility and Control

More than half of companies use at least three different systems to store documents and records, and more than 20% have at least five systems in use.[iv]

Keeping track of all corporate data scattered across siloed systems and repositories can be demanding without the tools to gain visibility and control over them in a 360-degree view.

Elimination of Human Error

According to a study on the human impact, 88% of data breaches are caused by human error[v].

This often refers to employees that have inadvertently compromised information. That happens, for example, via lost or stolen devices containing sensitive information, vulnerable device protection, accidently sharing the inaccurate information with external parties or falling victim to a phishing attack.

Adding a Layer of Security

A proper, metadata-driven information management system can provide an additional layer of security. Using metadata as a core element of your information management system will let you govern everything by what it is rather than where it is stored. And, it can drive security and policies based on roles, stage of workflow, or other relevant metadata attributes.

Three reasons why an extra layer of security is important:

- Access management for internal and external users gets automated and more easily managed compared to the tedious manual management of rights in a folder structure.
- Additional security measures for data in transit and in rest, such as data loss prevention, encryption, print, and download protection, can be inbuilt into the information management system.
- Information management systems can also provide additional protection against deliberate leaks of information or cyberattacks such as ransomware. Automatic version control can push a new version each time a document or other object is accessed, facilitating easy roll-back to the previous version.

The 6 Best Practices for Security and Compliance in Information Management

#1

Build the right guardrails to support your processes

While security software can help protect you against human error, opportunities for automation improvement to learn from your most common mistakes can further enhance security awareness.

A good information management system automates how staff interacts with documents - storing, accessing, sharing, and managing them.

#2

Automate access and user right management

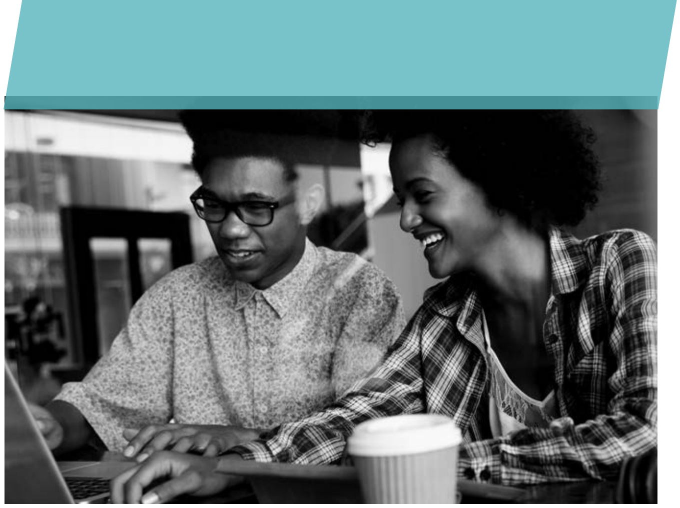
Metadata-driven permissions can help automate the control of access—read, edit, delete, change permissions. Permissions change with the context of the document, for example the role of an employee, and when that context changes, so do the permissions. All related documents and objects gain new access and user rights based on the new role.

#3

Support secure external collaboration

Working with external clients, partners, suppliers, and other stakeholders can cause potential security and compliance risks. Unauthorized access via the supply chain is one of the key risk scenarios businesses face. As many as four in ten cyberattacks are now thought to originate in the extended supply chain, not the enterprise itself.[vi]

Using information management systems allow you to build a secure, integrated way of sharing and collaborating externally. A proper information management system can extend the visibility and control to external contacts via integrated client portals, extranets, and more, minimizing the need to duplicate information.



#4

Maximize data accuracy

Data integrity ensures information is handled in the right way, by the right people, with the latest, up-to-date information at hand—you only have one version of a document, accessible by everyone who needs it.

#5

Support your business processes with automated workflows

Build in automation to support the creation, editing, proofing, and approving of official documents. And build further automated steps to ensure proper management - such as permanent archival, or deletion of data - for those documents in the future.

#6

Provide visibility and efficient, easy-to-use tools

To avoid the risk of shadow IT, your staff requires the best tools to be easily at hand. All information should be found easily when needed to avoid the risk of duplicates and unofficial archives.

Your information management system should be used to securely connect all data across the various business systems, applications, and repositories, or to share it with clients and partners. That way you can provide the necessary ease of use and visibility combined with required security of data.

The M-Files Approach

M-Files, a leading provider of information management solutions, connects content and helps build smart automation.

M-Files helps businesses provide more visibility and control to your content, minimize human error, and as a result, add an additional layer of security to your environment.

We create visibility to all data, regardless of where that data is stored - in network folders, repositories, CRM solutions, or other applications, based on the right context of that data. M-Files connects business data and documents into one view without the need for initial migration. This way, people do not need to resort to personal file sharing tools or other systems that are not controlled by corporate IT.

M-Files also provides the ability to improve customer service and security by having the same source of truth for everyone. There's no need to share an attachment in email or use other ways that would easily end up in error-prone duplicates. Duplicates that could easily get to wrong people and saved in different systems and email boxes. These duplicates pose a clear security problem as it will be hard to control who has access and how they are shared.

Automated workflows can be built in to support your business processes, industry regulations, and legal requirements. M-Files supports your security and compliance efforts and takes some of the burden off human workers.

There's an urgent need to work and collaborate, even—but to do that with adherence to guidelines, policies, and regulations. Avoid the pitfalls of security and compliance and be ready for the future.

Learn more about M-Files and how we can help your company secure your data and be more compliant.

WWW.M-FILES.COM

[i] *AV-Test.org, Malware statistics and trends*
[ii] *Cost of Data Breach Report, 2021, IBM Security and Ponemon Institute*
[iii] *Tessian: 18 biggest GDPR fines of 2020 and 2021*
[iv] *AIIM: 4 Things You Need to Know About the Real World of Multiple ECM Repositories*
[v] *Psychology of Human Error, Professor Jeff Hancock, Stanford University, in a report by Tessian*
[vi] *Securing the supply chain, Accenture, 2020*

Laminin SOLUTIONS
UNLOCK BUSINESS INFORMATION

For more information, visit lamininsolutions.com
or call US: +1 904-810-3299 UK: +44 2392 354 320

ABOUT M-FILES

M-Files is a global leader in information management. The M-Files metadata-driven document management platform enables knowledge workers to instantly find the right information in any context, automate business processes, and enforce information control. This provides businesses with a competitive advantage and substantial ROI as they deliver better customer experiences and higher-quality work with lower risk.

M-Files is a registered trademark of M-Files Corporation. All other registered trademarks belong to their respective owners.