Strengthen your Microsoft Information Protection implementation

Maximize your deployment through an information-centric approach.

pwc | Microsoft

June 2021
PwC.com/us/microsoftcybersecurity

Table of contents

1 Executive Summary

Businesses are increasingly motivated to deploy innovative new capabilities that bolster their ability to protect and govern their information estate, whether the data is housed on premises, in a user device, or in the cloud. But designing a holistic information governance and protection program that combines the right people, process, and technology capabilities to manage and safeguard information is an ambitious undertaking. It requires a careful balance of focusing on information assets that need additional protections, the business user's role in identifying and protecting that information, and minimizing business disruption while doing so.

Organizations that struggle to maximize their information governance and protection investments tend to take a "tool-based" approach that emphasizes deployment of a specific technology rather than understanding the context of data as well as end-user and business experience dynamics. This approach often minimizes the need to engage with business leaders and end users to understand and tailor governance and protection policies to fit their workflows.

The results can be calamitous. Consider this: A solution that offers rapid deployment may be siloed or non interoperable with other systems. Consequently, users are less likely to adopt the solution, which could arguably cause alerting, monitoring, and business disruption challenges —rather than deliver information governance and protection benefits.

We believe there's a better way. PwC's experience shows that an information-centric approach to information governance enables organizations to help overcome implementation constraints while minimizing business disruption and promoting end-user engagement and adoption.

An information-centric approach focuses on understanding the information assets in a given business workflow or use case, and using the information asset and its context—its lifecycle, the users interacting with the information, and commensurate protections—to help configure, manage, and communicate deployment of tools.

This type of strategy can bring long-term benefits that include:

- A phased deployment focuses on a narrow set of business processes and information assets
- Minimized business disruption through better understanding user behavior and needs for a given information asset
- End users can better understand and anticipate the controls and behaviors that a protection policy enforces

Platforms like Microsoft 365 and Microsoft Information Protection (MIP) can enable strong protections and controls that align and support an information-centric approach. The Microsoft solution set, coupled with PwC's information-centric focus, helps enable a robust security program that helps reduce user friction.

Our goal in this paper is to demonstrate how an information-centric approach combined with Microsoft 365 security tools can help overcome the challenges associated with designing and deploying an information governance and protection program.

2 Why information governance is a must-have

As organizations struggle to manage today's explosion of data, information governance has become a business-critical capability. Yet only 29% of global organizations have implemented an enterprise-wide information governance model, according to PwC's Global Digital Trust Insights Survey 2021.[1]

A number of converging factors are inhibiting adoption of information governance. Chief among them is the seismic eruption of data across industries and geographies. This explosion of data often inhibits the ability to know where information resides and how to classify and protect it.

Compounding matters, organizations must contend with new consumer data privacy laws that are increasingly information-centric. The California Consumer Privacy Act (CCPA) and its successor the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act, and the EU General Data Protection Regulation (GDPR) all address data and information at a more granular level.

Not only do these regulations seek to protect personally identifiable information (PII) like Social Security numbers, but they also cover health data, biometrics, and personal information that can reveal racial, political, and religious details. These laws also demand complex technical processes—in an information-centric manner—for information protection, retention, and disposal. It's no wonder, then, that 92% of businesses expect more intense regulatory scrutiny of third parties, while 85% say their third-party risk exposure is increasing.[2]

Collectively, these factors help explain why businesses may be confused, and therefore reluctant, about diving into an implementation of information governance. Yet the risks of inaction can be significant. Chief among them is loss of sensitive information due to carelessness or malevolent intent by insiders.

Despite the complexities, understanding and governing information is not an insurmountable hurdle. Far from it. "Companies that incorporate an information-centric approach in building an information governance program can be more comfortably prepared for security threats—without negatively impacting the user experience and productivity," said Mir Kashifuddin, Principal, PwC Cybersecurity, Privacy, and Forensics.

1 PwC, Global Digital Trust Insights Survey 2021, May 10, 2020

2 PwC, Building digital trust: The partnership of leadership and operations, April 2021

How PwC and Microsoft approach information governance

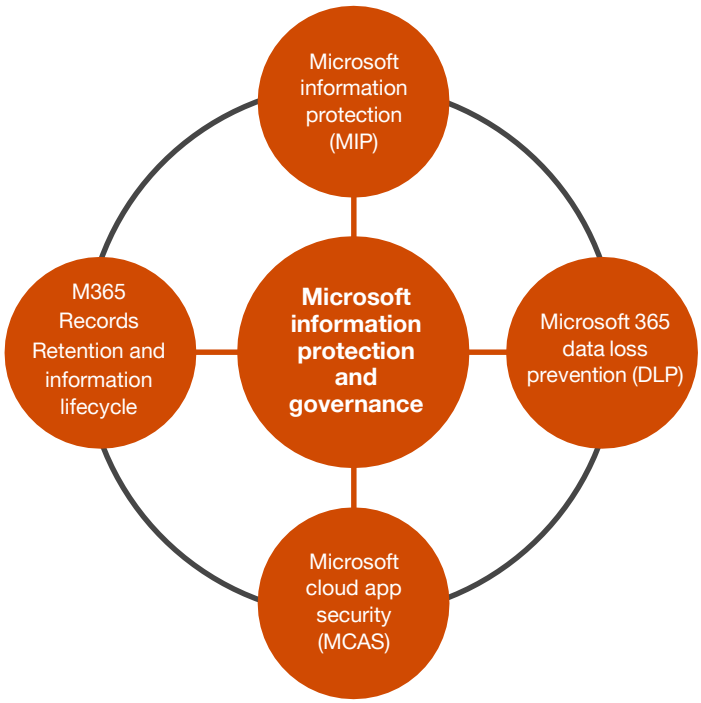
Know your data
Gain a full understanding of your data landscape. Know where data is stored and who needs access to it in order to build a data-protection strategy.

Protect your data
Implement policies and data-protection mechanisms specific to needs of users and departments. Enable tools to discover, classify, and protect sensitive data and allow for continuous monitoring and governance.

Govern your data
Enable your organization to more effectively meet compliance requirements. Manage the information lifecycle and records intelligently with archive management, automated policies, and defensible disposal.

3 PwC takes an information-centric approach

In alignment with Microsoft, PwC's information -centric methodology defines information governance as an end-to-end framework for enabling governance and data protection. It's a collaborative framework of roles and responsibilities, processes, and technologies that establishes accountability for using, improving, managing, and maintaining information across the enterprise.



The Microsoft information protection solution

Microsoft information protection (MIP) is designed to help Microsoft customers discover, classify, and protect, sensitive information across their ecosystem. MIP provides an integrated foundation upon which businesses can build an effective data-governance program.

Our information governance framework is aligned with the guiding pillars of Microsoft's information protection approach: Know Your Data, Protect Your Data, and Govern Your Data, as well as alignment to Microsoft's enabling technologies.

Know: As noted, an end-to-end understanding of your information estate is foundational to information governance and protection. In the Know phase, PwC works with clients to help discover where sensitive information is stored, how it's used, who owns it, and who needs access to it. PwC then classifies information using Microsoft technologies such as Azure Information Protection (AIP) for sensitivity labeling and security controls.

Results can be quickly realized. For instance, a technology company recently engaged PwC to deploy a document-type labeling strategy for its information governance program. Within the first few days, hundreds of sensitive documents were identified. Subsequent rollouts to additional departments uncovered many more sensitive documents, which set the stage for reducing risk to the organization.

Protect: Robust protection of information will require security controls that follow data as it travels across the enterprise and beyond. PwC helps configure and deploys key Microsoft protection technologies that include Data Loss Prevention (DLP), AIP sensitivity labels, and Microsoft Cloud App Security (MCAS). Using these tools, PwC recently helped a financial services firm deploy sensitivity labels and associated protections using a repeatable, iterative approach. The result? The initiative was deployed within 30 days—with an approximate 99.6% user-adoption rate.

Govern: An information-centric model helps organizations identify and govern data that's subject to regulatory requirements, as well as manage the information lifecycle. In fact, 92% of businesses expect that regulatory scrutiny of third-party partners will likely intensify while 85% forecast rising exposure to third-party risk, according to a recent PwC study.[3] Our teams also assess the data privacy and governance practices of third-party vendors. To help govern regulated information, we leverage Microsoft tools that include Compliance Manager, AIP, MCAS, and lifecycle management.

PwC collaborates with clients to combine these components in ways that best address individual business needs to help protect information. Additionally, organizations that have purchased an M365 E5 license can take advantage of a number of integrated security and compliance tools that are available in Microsoft's Office 365 Security & Compliance Center.

Before you start: A few general considerations

- Engage executives and business stakeholders in the information governance strategy. Develop a real-world business case that clearly conveys the benefits of data governance.
- Make sure that business leaders understand what sensitive data resides in the systems of each department.
- Implementation of information governance should be incremental and based on repeatable and scalable methodologies. Start small: Address two to three critical issues at a time to avoid overwhelming IT staff and users.
- Information governance targets specific areas of risk and associated functions, rather than the entire enterprise. It should be a surgically precise, friction-neutral approach that has no impact on employee productivity.

3 PwC, Building digital trust: The partnership of leadership and operations, April 2021

4 Get started in 6 steps

Implementing an information-centric governance program can seem like a formidable undertaking, but with the right methodologies and tools, you can overcome the obstacles and achieve sustainable impact. Following are six steps for starting an information governance initiative.

1. **Develop** an information-centric governance strategy leveraging Microsoft capabilities.

2. **Define** a taxonomy of sensitivity labels for use in pilot groups and identify security requirements that will be mapped to documents, including linking to company data classification policies. This process is critical to create an intuitive user experience and help employees understand the intention of information governance. All design stakeholders should review and confirm the data taxonomy. This can help demonstrate quick wins to program sponsors.

3. **Deploy** sensitivity labels and protections in monitor mode (e.g., Microsoft DLP policies) to help derive insights into the efficacy of controls. Then link these sensitivity labels with the specific security controls needed to protect documents. Certain sensitivity labels, for instance, may automatically trigger protection capabilities like encryption, content watermarking, headers, and footers.

4. **Review and tune** governance processes on a regular basis to ensure that protections remain robust without disrupting user productivity. This exercise can help refine underused labels, provide clear instruction for overused labels, and identify needs for user training.

5. **Deploy** protections and controls in enforcement mode, which activates security controls and protections.

6. **Repeat** these processes at scale to implement information governance across the organization. Make sure to align data protection with your organization's individual appetite for change, risk tolerance, and regulatory obligations.

5 Wrap it up with training and awareness

It's critical that all employees understand information governance processes and how to comply with them, as well as their individual role and responsibilities in safeguarding sensitive information.

This will require comprehensive user training on the principles and use of information governance. Awareness is critical: Employees should understand the importance of data classification in their daily work and how to apply the right protective measures. In some cases, IT and information security staff may require additional training to reinforce operational readiness.

The rewards can be real

Overall benefits of information protection

- Security is integrated in apps and services
- Automated identification and classification of sensitive information
- Unified management of information policies
- Secure third-party applications
- Enhanced operational efficiencies
- Improved user experience

6 The PwC-Microsoft Alliance

To alleviate pain points associated with secure and effective information governance, PwC and Microsoft have teamed to develop an information-centric approach to help you know, protect, and govern sensitive information.

This information governance offering is designed to help assess your organization's security capabilities, identify potential areas of improvement, and streamline adoption of effective information governance policies. Whether you're looking to adopt new Microsoft technologies or need to address gaps in your current cybersecurity and privacy environment, PwC and Microsoft can help you confidently navigate the way forward and maximize the impact of your IT investments.

Our alliance with Microsoft fuses PwC's strong industry experience with hands-on knowledge of Microsoft's security portfolio and community support. This experience undergirds our ability to help create solutions through all stages of the information lifecycle, including planning, implementation, automation, enhancement, and maintenance.

Click here to learn more about the PwC-Microsoft Alliance.

7 Now's the time to take control of your information

Data will continue to expand at lightning speed, and so too will the need for end-to-end management of information. Doing so will require a scalable information governance strategy that is founded on deep knowledge of your information. PwC's flexible design framework and business experience, combined with industry-leading Microsoft technologies, allows us to develop a governance program that is tailored to the specific needs of your business—no matter how much information you manage.

In today's data-driven world, adoption of information governance is no longer negotiable; it's a business-critical requirement. Now's the time to start building an information-centric framework to manage your data and protect sensitive information.

Get in touch

PwC

Joshua Rattan
Principal, PwC US
joshua.r.rattan@pwc.com

Joseph Nocera
Cyber & Privacy Innovation Institute Leader, PwC US
joseph.nocera@pwc.com

Mir Kashifuddin
Partner, PwC Cybersecurity, Privacy and Forensics
mir.kashifuddin@pwc.com

Microsoft

Malli Vangala
Information Protection Director, Microsoft
mavang@microsoft.com

Thank you!

www.pwc.com