

INFORMATION PROTECTION IN THE CLOUD

BEST PRACTICES FOR MICROSOFT PURVIEW INFORMATION PROTECTION & DLP



John Mancini
Chief Evangelist
Infotechtion



Sanjoyan Mustafi
Principal Product
Manager, Microsoft



Vivek Bhatt
CTO
Infotechtion



Kunal Kankariya
Principal Solution
Architect
Infotechtion

 **Infotechtion**

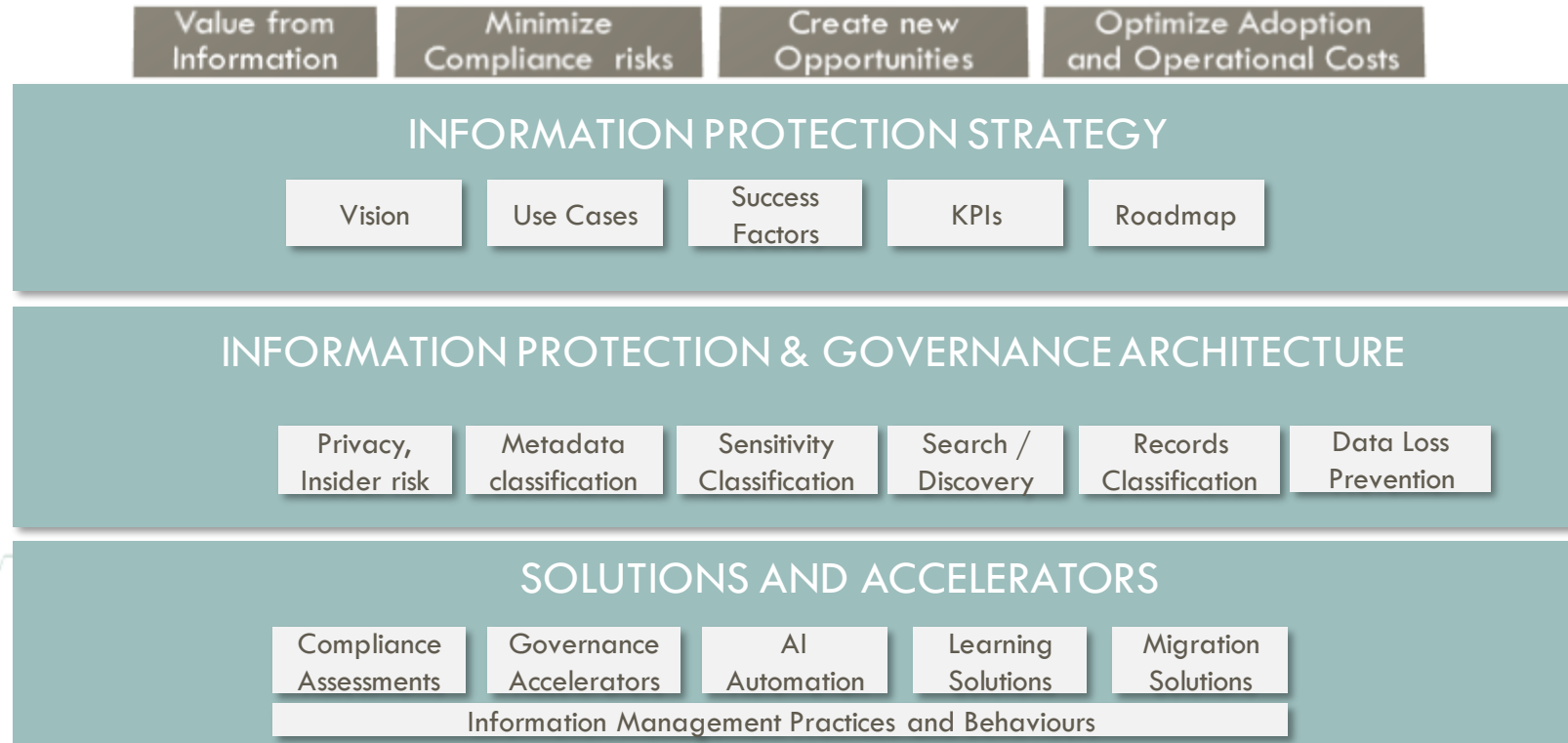
AGENDA

1. What is Information Protection?
2. Why is it relevant now?
3. What are the prevailing scenarios?
4. How can Organisations start their journey?
5. What are the Critical Technology Building Blocks?
6. Where are the key Limitations / Considerations with the current technology?
7. What is Microsoft response and roadmap?
8. What can you do today to better protect and govern your information?



OUR SERVICES

Infotechtion is a vendor independent consulting firm specializing in information governance and protection for Microsoft 365 and beyond.

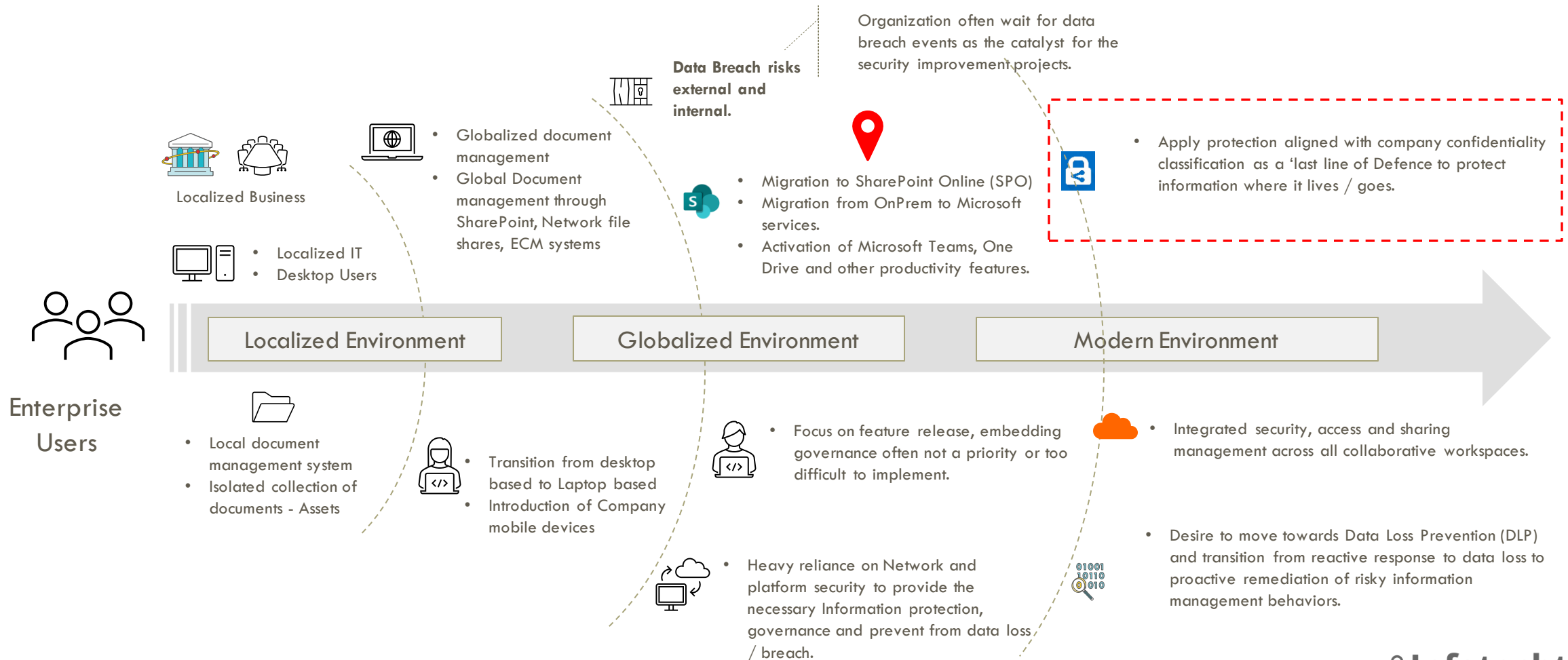


"I consider Infotechtion one of the leading experts in Microsoft information governance. Their staff work closely with our enterprise customers to maximize customer investment in Microsoft products especially Microsoft information protection and governance to enable increased levels of compliance for customer information in Microsoft 365."

Principal Engineering Manager, S+C Engineering, Microsoft.

FROM SYSTEM SECURITY TO DATA PROTECTION

Many organizations have travelled a similar journey to modernizing their IT and Information landscape over several decades. Transition to cloud provides a unique set of challenges and opportunities for both enterprise employees and their leadership.



WHY IS IT RELEVANT NOW?

Priority:

- Protecting business information, value and intellectual property as organization is transitioning into a Modern Cloud environment.

Challenges:

- Overwhelming amount of information created, and lack of governance manage its lifecycle.
- In addition to volume, information ranges in importance from “Highly Sensitive” to Trivial and transient “Unrestricted” unstructured information.
- Cloud and Identity security no longer sufficient to prevent information loss with a hugely hybrid and mobile workforce.

Risk of not addressing the problem:

- Risk factors include reputational damage, financial impact, and loss of competitive advantage.

Ideal Solution:

- A solution to know and protect data with reduced dependency on users to do take the right actions.
- Intuitive and automated classification with embedded protection.
- Ability to prevent data loss without impacting employee mobility / productivity to help prevent the accidental/intentional oversharing of the sensitive information outside of the organization.

WHY IS IT RELEVANT NOW?

What is information confidentiality classification?

Information confidentiality classification is a specialized term to describe the process of identifying, categorizing, and protecting content according to its Confidentiality/ sensitivity or impact level to an organization.

In its most rudimentary form, information classification is a means of safeguarding your information from unauthorized disclosure, alteration, or destruction based on its sensitivity or confidentiality and impact to the organization.

What is an information classification framework?

The framework to classify data based on an enterprise-wide policy, a classification framework (sometimes called a 'data classification policy') is typically comprised of 3-5 classification levels based on sensitivity/confidentiality. The framework also contains data handling rules or guidelines that define how to put these policies in place from a technical and technology perspective.

Why is information protection important?

\$4M

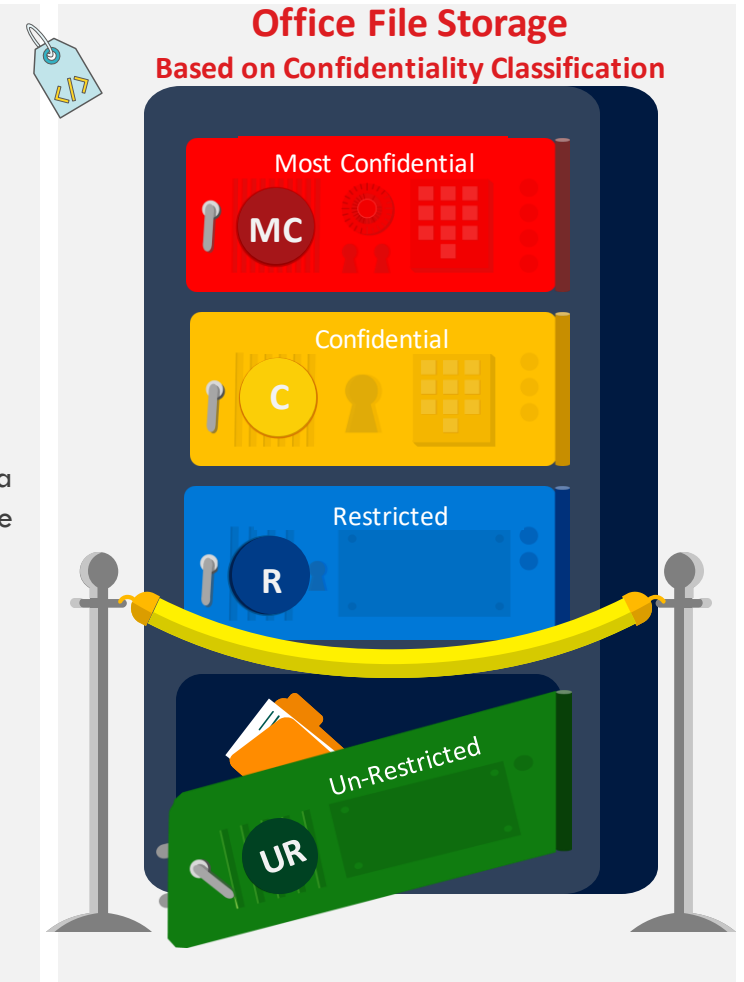
The global average cost of a data breach in 2019.

88%

Organizations lacking the confidence to prevent sensitive data loss.

4%

Potential Annual revenue loss due to non-compliance with Data Privacy regulations



WHAT ARE THE PREVAILING SCENARIOS?

Simplified /
Consistent
confidentiality
classification

Prevent Data
exfiltration while
supporting internal /
external collaboration

Establish better
protection controls to
Records

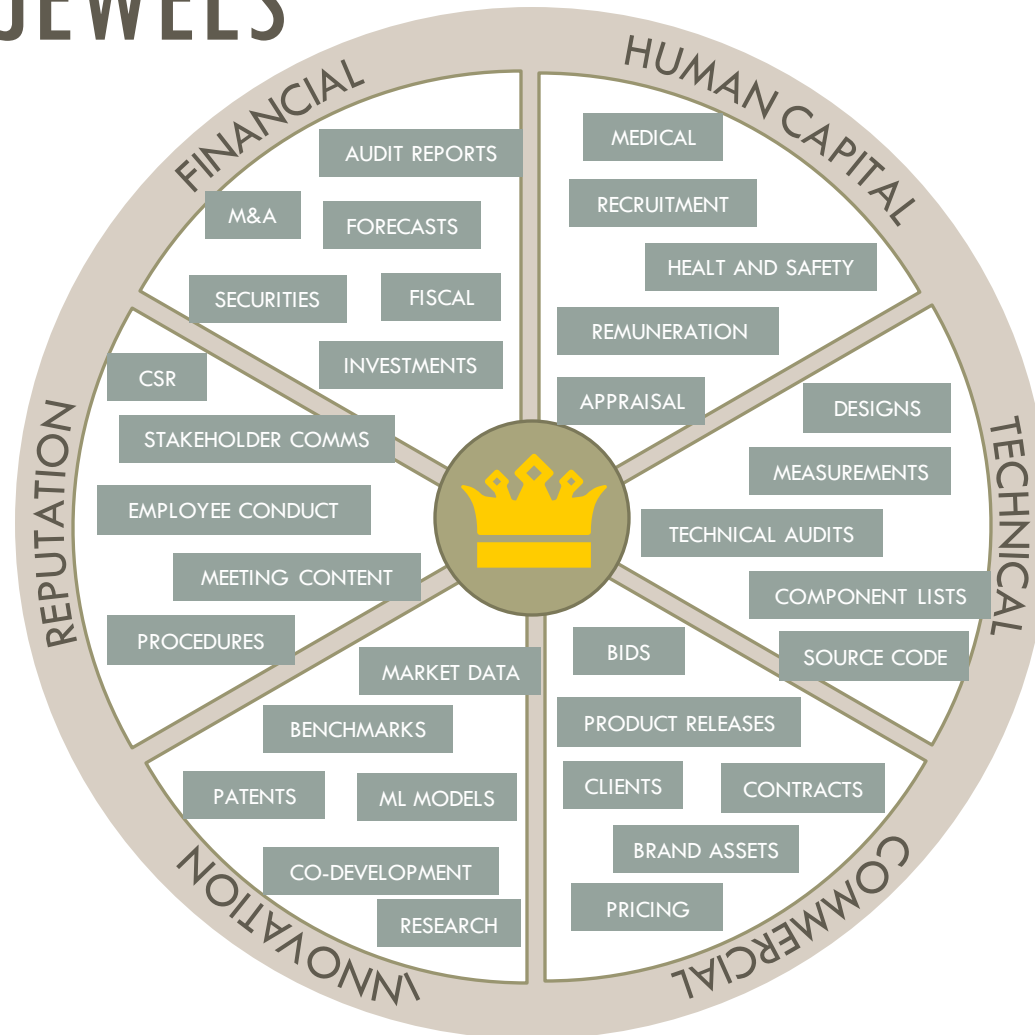
Manage protection in-
place consistently
across content / Data
services

Establish Information
protection controls
due to upcoming
Government / NATO
changes



Safeguard data
wherever it lives

CROWN JEWELS



*Information assets of which a breach of confidentiality might threaten business continuity and growth. Information assets are intangible assets which are conservatively valued at 20-45% of a company's value, but when you factor in brand reputation, proprietary software, investor and partner trust, et cetera, then intangible assets likely represent 80-85% of many companies current and future value. (Source: Protecting intangible assets: Preparing for a new reality. Lloyds/KPMG August 2020.)



PRACTICAL STEPS TO ESTABLISH A PLAN FOR YOUR INFORMATION PROTECTION PROGRAM.

HOW CAN ORGANISATIONS START THE JOURNEY?

Microsoft Information Protection (MIP), a unified, and extensible solution to protect information across enterprise. Data at rest and motion can be encrypted– in Microsoft 365 cloud services, on-premises, third-party SaaS applications, and more.

What?

Why?

Who?

How?

1

Review your confidentiality classification and simplify it for effectiveness

Make the confidentiality classification relevant to the ways of working of an organisation

All users can leverage the ability to classify information regardless of where it is stored.

Automatically based on rules or directly from Microsoft Office Web, Desktop and mobile interfaces

2

Capture your information protection choices based on various use case scenarios

To prevent operational chaos with the spaghetti of protection choices

Protection generally available to all users or available to specific users

Targeted classification and choosing the right protection configurations

3

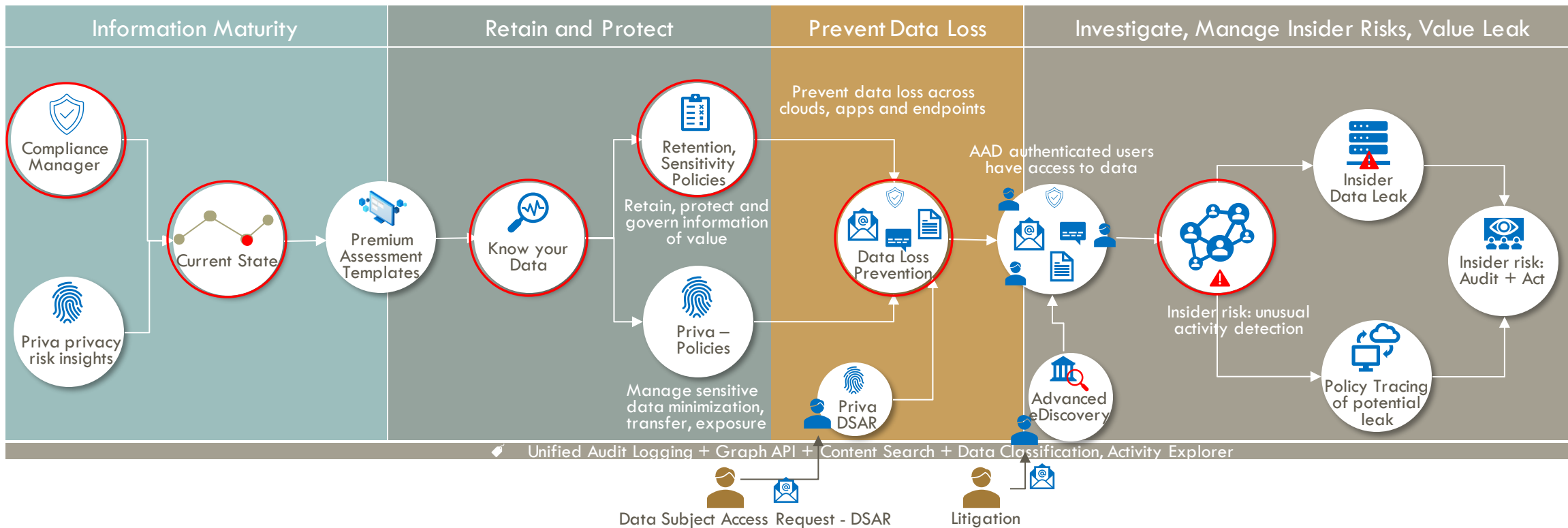
Plan for ability to detect unusual activities and proactively manage your data loss risks

Improve protection of value, automated controls on data loss by accidental or intentional sharing.

Centralized team monitoring and triaging risky activities

User activity-based detection against centrally configured policies and apply preventative controls.

WHAT ARE THE TECHNOLOGY BUILDING BLOCKS?



WHERE ARE THE KEY LIMITATIONS / CONSIDERATIONS WITH THE CURRENT TECHNOLOGY?

Connected Apps

Bulk classification
or reclassification

Records
Interoperability

Hybrid setup

Configuration
options – Files OR
Emails

Export sensitive
information types

Enhanced support
for User defined
permissions



MICROSOFT ROADMAP AND KEY ANNOUNCEMENTS FOR INFORMATION PROTECTION



Sanjoyan Mustafi

Principal Product Manager






Microsoft SharePoint and OneDrive

<https://www.linkedin.com/in/sanjoyan/>

WHAT IS MICROSOFT RESPONSE AND ROADMAP?



Available Now






-  Default sensitivity label for SharePoint Document Libraries v1 (GA)**
-  Syntex models support Sensitivity Labels (GA)
-  Restricted access control (RAC) policy for OneDrives v1 (GA)
-  Granular access policy at SharePoint/OneDrive/Team level (GA) **
-  Restricted access control (RAC) policy for Sites v1 (Preview)

GA – Generally Available

** Capabilities available by end of this calendar year



H1 CY23 and beyond

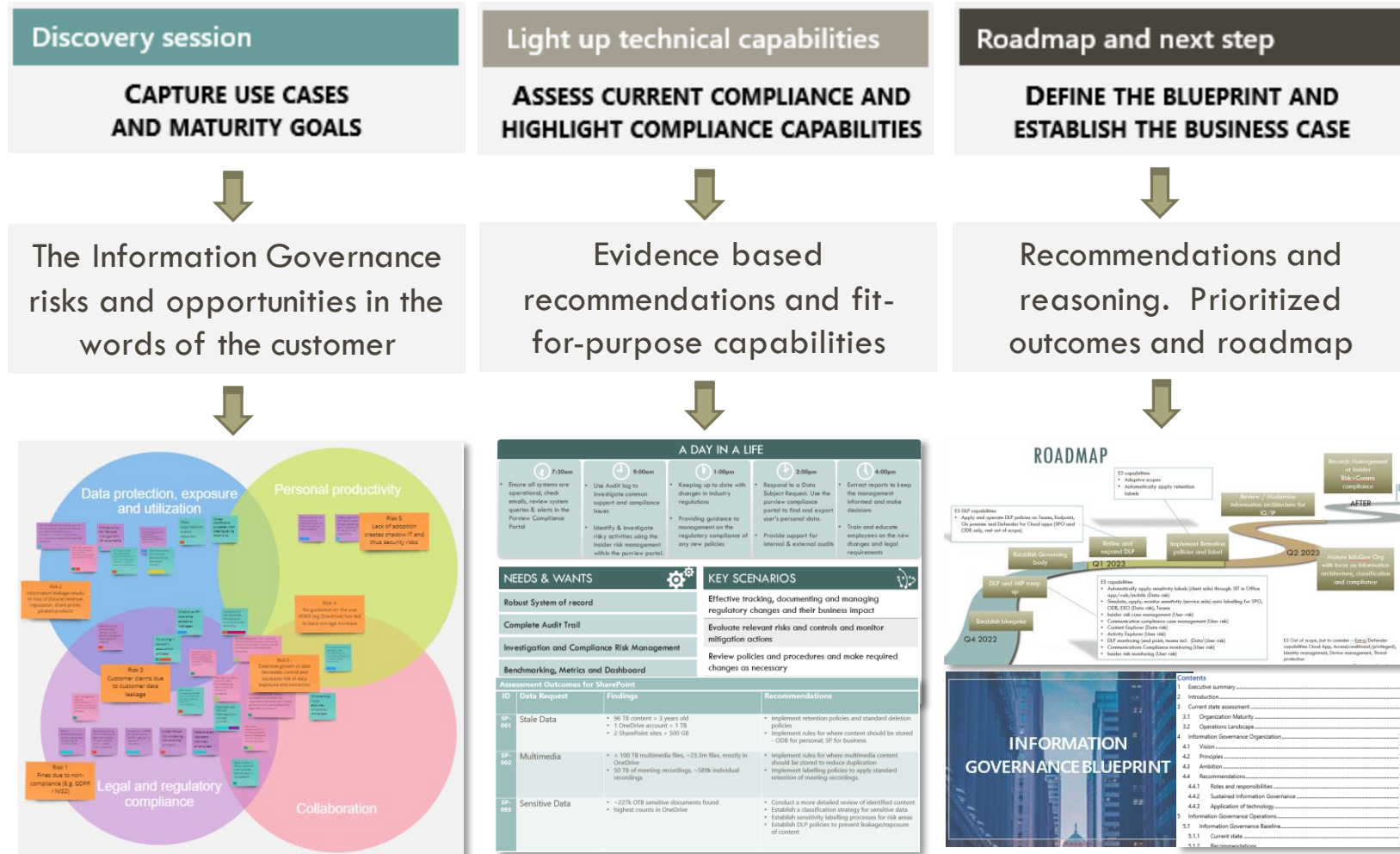
-  User-defined-permissions (UDP) files in SharePoint (Preview)
-  Protected PDFs support (Preview)
-  Programmatic way to set sensitivity labels in SharePoint/OneDrive (Preview)**
-  Block download policy for files in SharePoint/OneDrive/Teams (Preview)
-  Data access governance (DAG) insights v1 (GA)

**In design: Retention and Sensitivity labels works in harmony.*



Signup for preview here: <https://aka.ms/ODSPSecurityPreviews>

NEXT STEP: CALL TO DISCUSS COMPLIANCE ASSESSMENT



NEXT STEPS: DISCUSS CUSTOMER LESSONS



Rabobank

Microsoft has just published a [case study](#) about how RaboBank turned to Microsoft Purview Data Loss Prevention to curtail inappropriate data sharing, regardless of the location of its employees or data.

- “We’ve found that Microsoft gets closer to the data than any other vendor. We benefit from getting our business apps, security, and DLP tooling from the same source because they all work together seamlessly.”



equinor

Microsoft has published a [case study](#) about how the global energy company Equinor has standardized on Microsoft 365 (M365) for both collaboration and records management.

- *“Equinor tested many of the leading solutions in the records management space against several use cases. We felt that Microsoft Information Governance was the best approach and verified our decision with several POCs.”*



THANK YOU



INFO@INFOTECHTION.COM



[HTTPS://INFOTECHTION.COM/](https://infotechtion.com/)