Reactive approaches to data risk
Discovering the Data Compliance Opportunities

Leon Butler – Director, Advisory

Microsoft + Lighthouse Alliance

- Relationship began 20+ years ago

- Lighthouse is Microsoft's #1 Legal and Compliance Partner for Microsoft Office 365 (M365) Advisory Services

- Lighthouse is Microsoft's primary eDiscovery partner (giving us unique insight into Microsoft-data)

- Engaged in all major U.S. regions, UK, EU and across APAC.

- Key advisory positions include PAC (Partner Advisory Council); GDPR partner program; heavily regulated entity groups

- Strategic partner program between Microsoft and Lighthouse

The amount of data is expected to more than double every two years

Complexity of managing the influx of data

54% of organizations say lack of visibility across their digital estate is a major concern

Limited visibility into risks within the organization

220 daily updates from over 1000 regulatory bodies worldwide

Lack of in-house expertise on standards and regulations

Manual data management tasks can be reduced by 45% with the addition of machine learning and automation
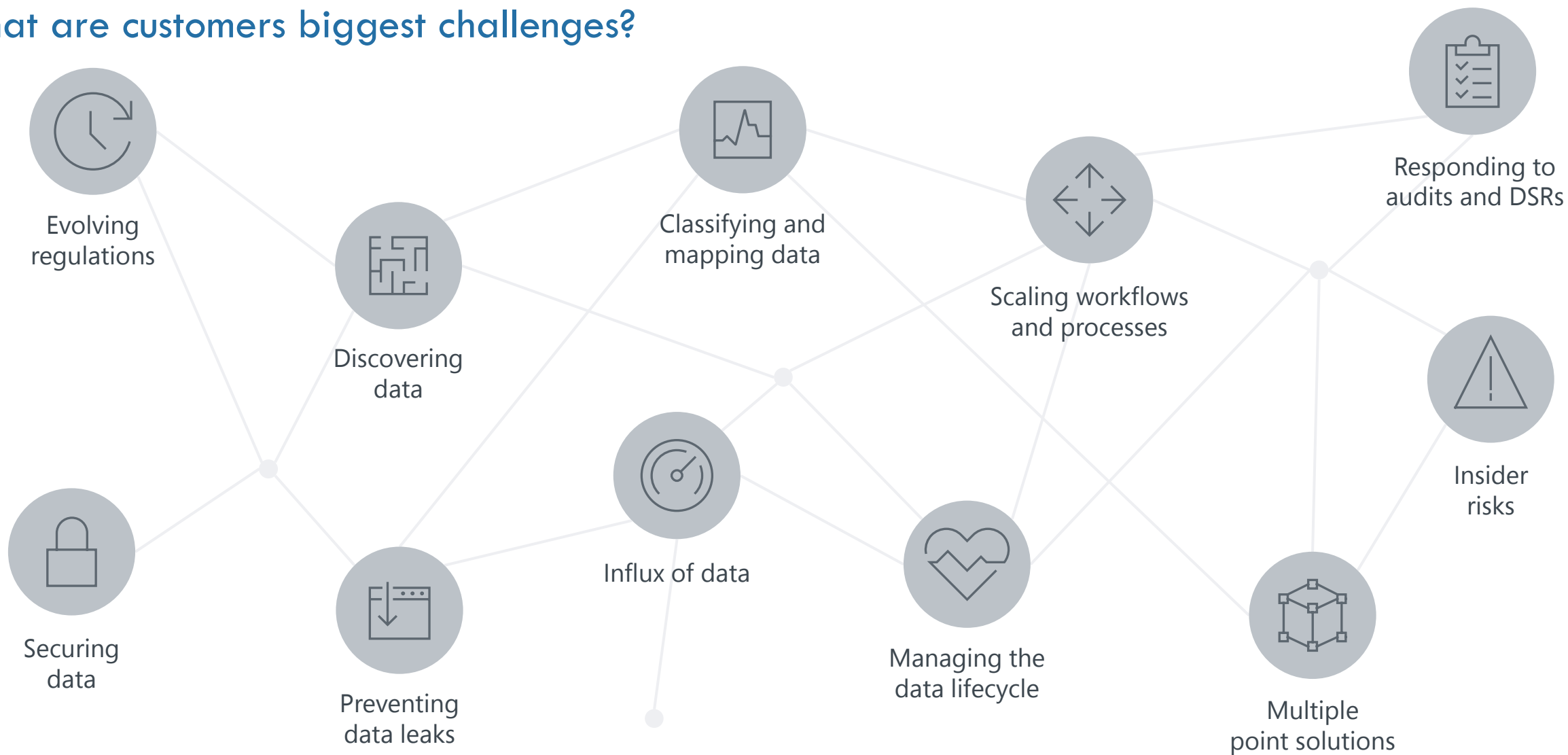
Need to scale processes with automation

Variety of different businesses

Compliance

Sensitive data

Insurance

On-premises systems

Traders

Data retention

IT

Finance

Compliance health

Data disposal

Legal

What are customers biggest challenges?

Evolving regulations

Discovering data

Classifying and mapping data

Scaling workflows and processes

Responding to audits and DSRs

Insider risks

Securing data

Preventing data leaks

Influx of data

Managing the data lifecycle
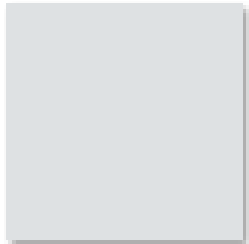
Multiple point solutions

Shared responsibility model

Customer management of risk
Data Classification and data accountability

Shared management of risk
Identity & access management | End Point Devices

Provider management of risk
Physical | Networking
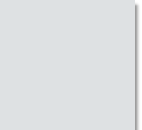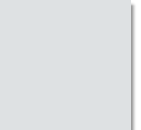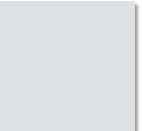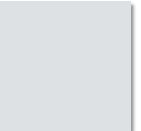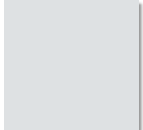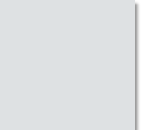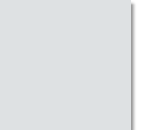
■ **Customer**   ▢ **Cloud Provider**

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	◩
Network controls	■	◩	▢	▢
Host Infrastructure	■	◩	▢	▢
Physical Security	■	▢	▢	▢

Global, regional, industrial regulations and standards

Shared responsibility examples

Microsoft's responsibility

Organization's responsibility

Access to production environment

Set up access controls that strictly restrict standing access to customer's data or production environment

Access to production environment

Set up access control policy and SOP, leveraging Customer Lockbox*/ identity management solutions

Protect data

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

Protect data

Encrypt data based on org's compliance obligations. E.g. encrypt PII in transit between users, using its own encryption key, etc.

Personnel control

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process

Personnel control

Allocate and staff sufficient resources to implement and operate an organization-wide privacy program, including awareness-raising and training

The extent to which the security and compliance features are being used varies significantly

Some clients are barely using the functionality
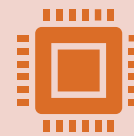
Where clients are using the functionality, they are often focused on manual processes

There is a growing interest in information protection and insider risk management

Compliance Microsoft 365

Compliance Management

Assess compliance and respond to regulatory requirements.

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints.

Insider Risk Management

Identify and take action on critical insider risks.

Discovery & Response

Quickly investigate and respond with relevant data.

Privacy Management

Safeguard personal data and build a privacy resilient workplace.

How many of your have a data map?

LIGHTHOUSE

Microsoft

Use Compliance Manager to understand and demystify the specific improvement actions required from industry-standards and regulations

Automatically identify information with built-in sensitive information types and trainable classifiers.

Leverage intelligent dashboards and key metrics to ensure your estate is protected.

Quickly and effectively place holds and automate the notifications required for the eDiscovery process.

UNDERSTAND REQUIREMENTS

IDENTIFY ASSETS

MEASURE CONTROL EFFECTIVENESS

GATHER EVIDENCE

PLAN & STRATEGIZE

APPLY CONTROLS

MONITOR ENVIRONMENT

ADAPT TO CHANGES

Use control-mapping to understand how your organization can improve its compliance and security posture with Microsoft's built-in integrated solutions.

Automatically protect documents through encryption, watermarks, and tailored automatic disposal workflows

Utilize further monitoring and automated workflows to prevent from insider risks from materializing.

220+ Updates per day in global regulatory landscape, but Compliance Manager does the heavy lifting.

Best Practices

Records Management

Legal Holds

eDiscovery

LIGHTHOUSE
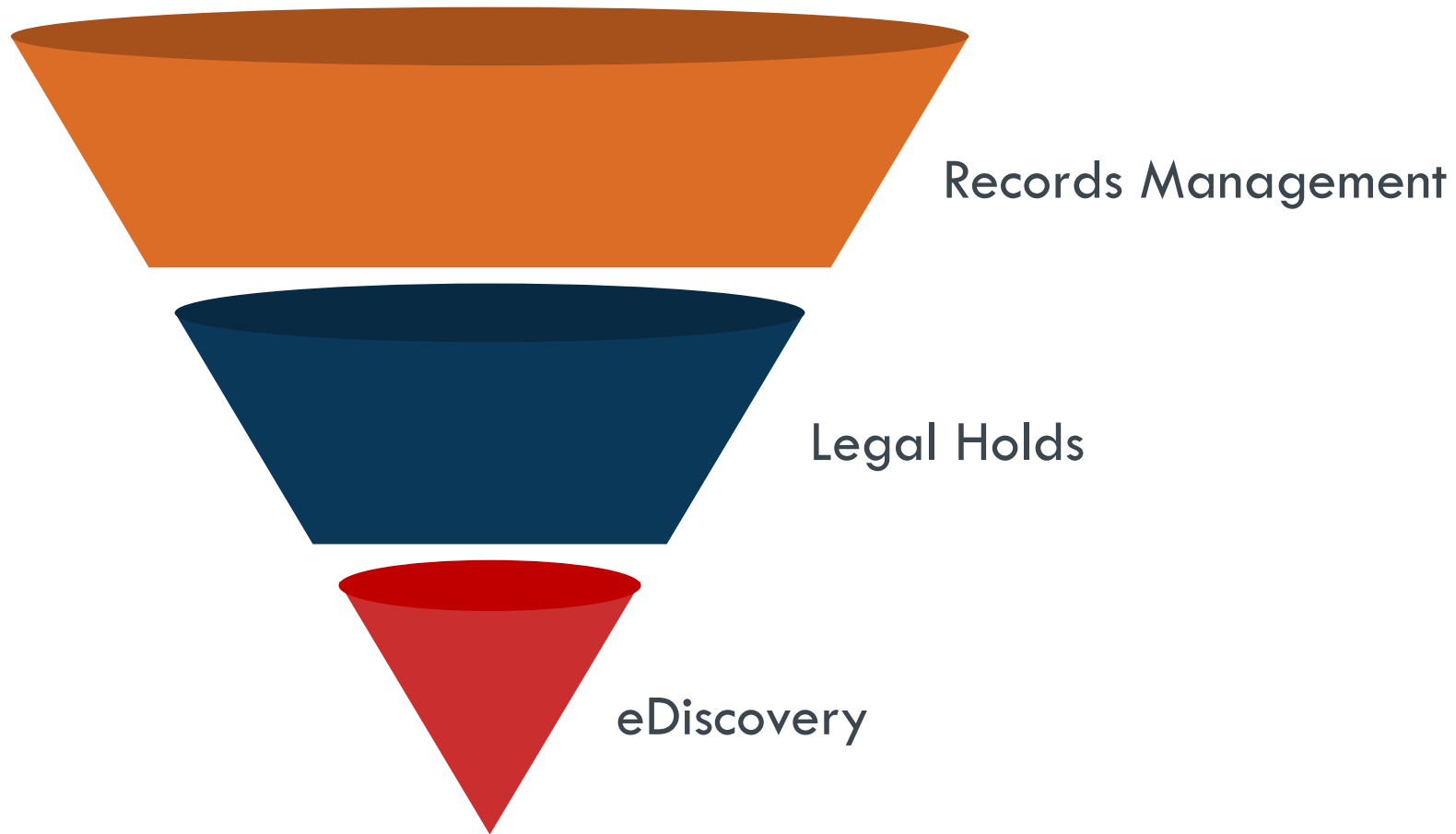
Best Practices – Records Management
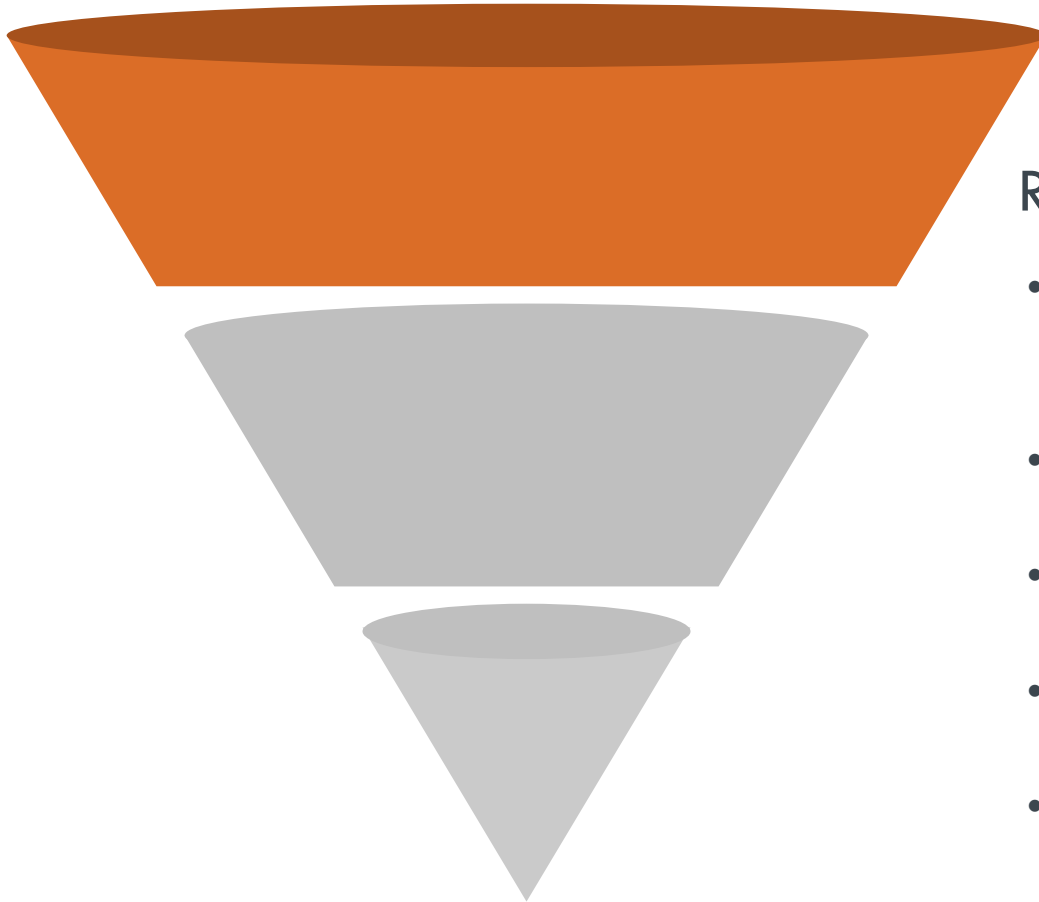
Records Management

- Defensible Deletion more important than records preservation (more liability in over-retention than under)

- 40-60% of info is ROT

- Consistency across data sources

- Simplify records declaration to minimize user involvement

- Cost savings are significant: born-digital through eDiscovery

- Breaches: can't steal what you don't have

LIGHTHOUSE

Best Practices – Legal Holds
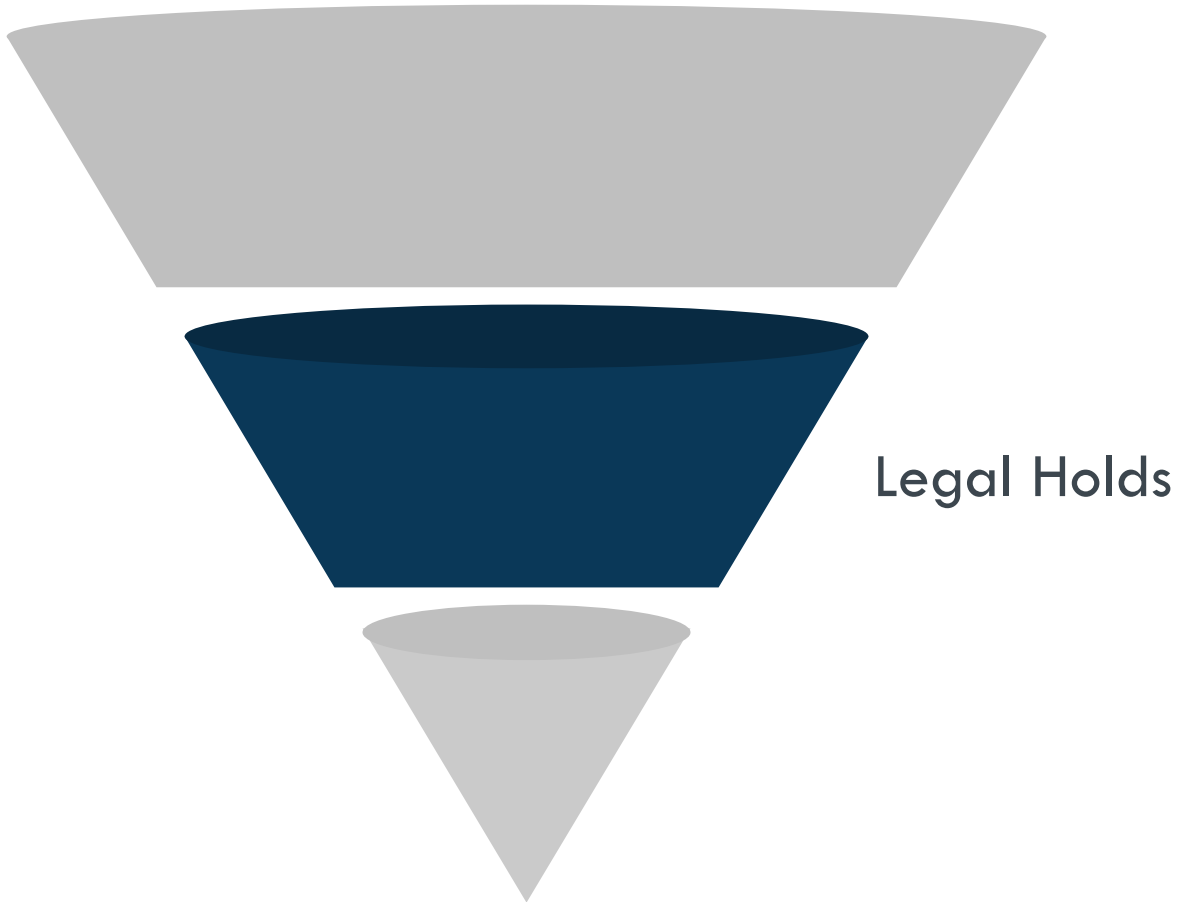
Legal Holds

- Manage in Place > Copy and Duplicate

- Apply across source systems: not just email

- Teams and collaboration tools are critical

- Single pane of glass

- Aggressively release legal hold and allow defensible disposition to resume in accordance with policy (must have the policy in place)

Best Practices - eDiscovery

eDiscovery

- Minimize number of search tools (M365 AED and others)

- Have ESI map for 26(f) discovery protections (negotiate a quality standard instead of workflow)

- Stop paying for duplicate file analysis (especially for priv)

- Use a Playbook

- Anticipate concepts like Teams, emojis, sentiment, analytics, and PowerShell integration for AED

Compliance Check Workshops

Customer Challenge
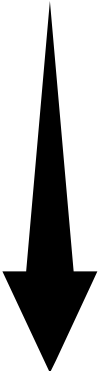
Microsoft/Lighthouse Solution
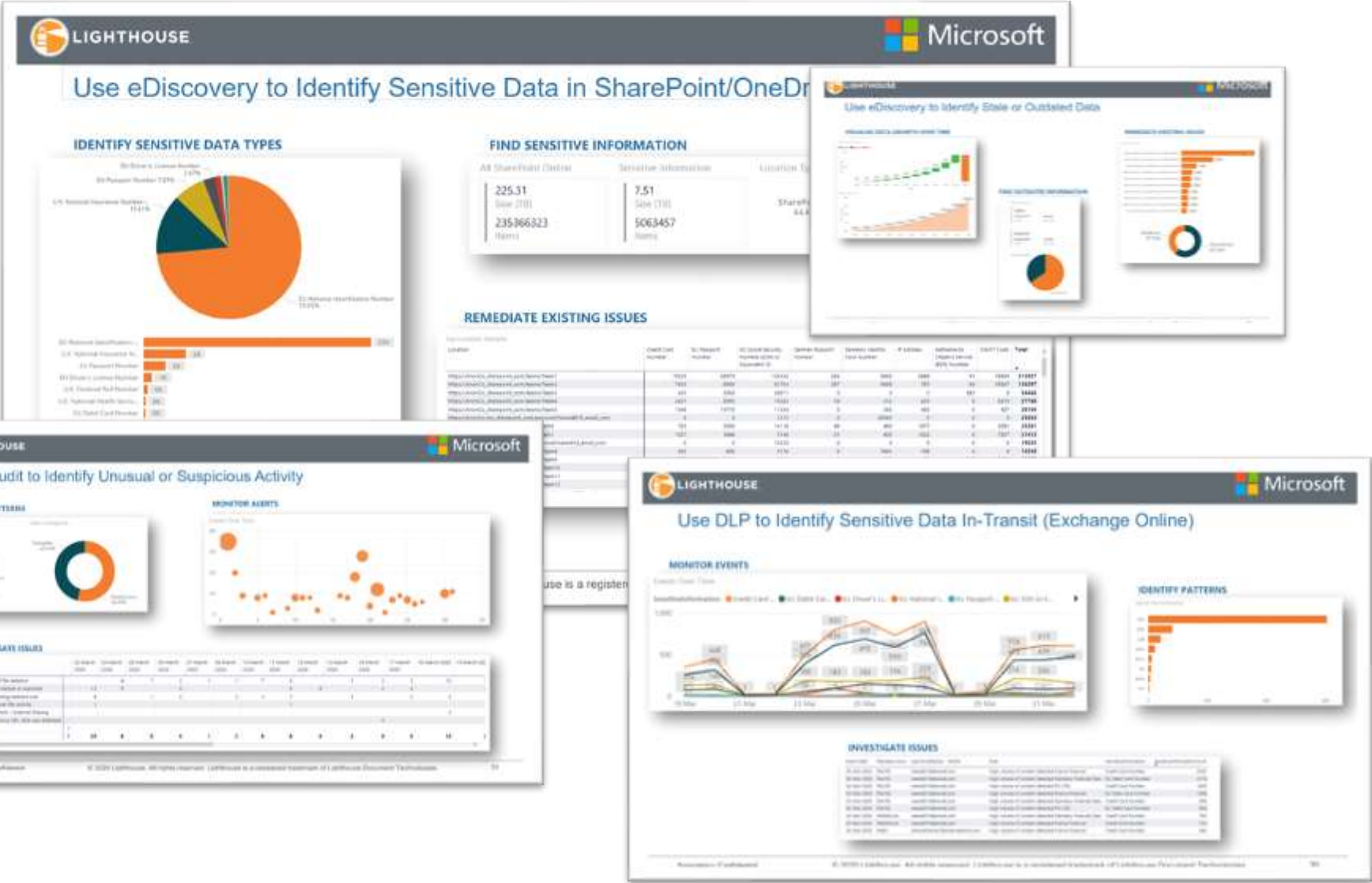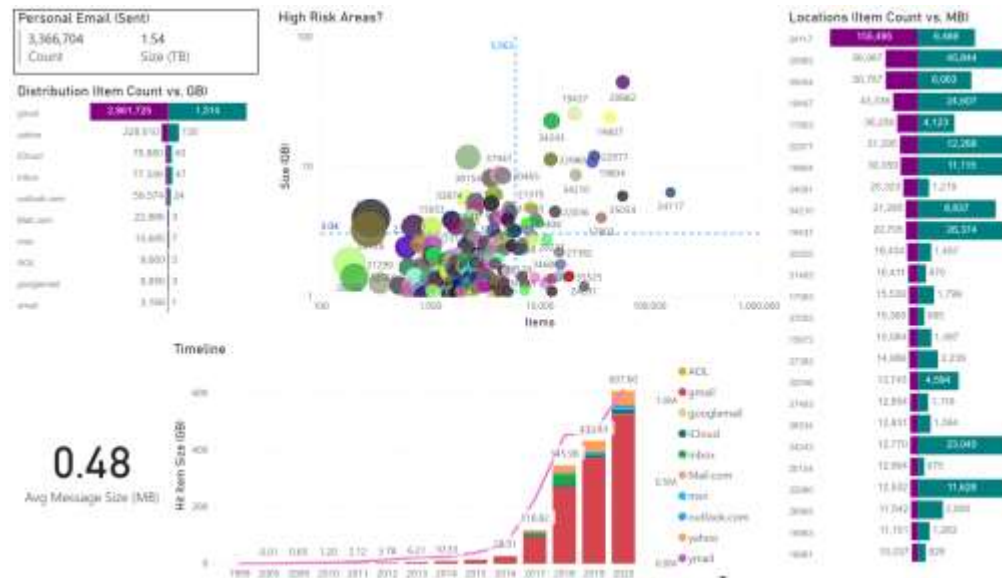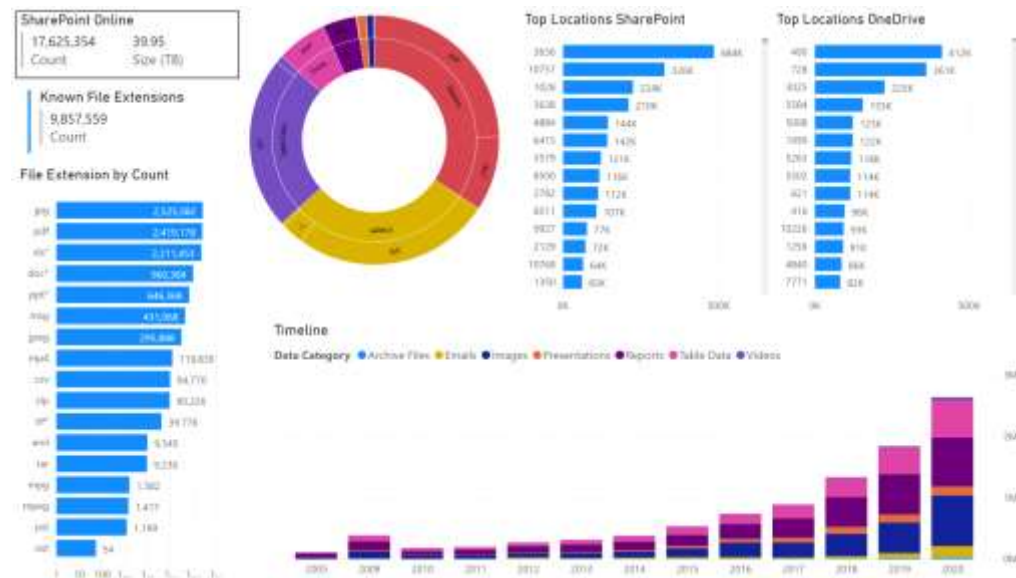
The dashboards

Compliance Microsoft 365

Compliance Management

Assess compliance and respond to regulatory requirements.

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints.

Insider Risk Management

Identify and take action on critical insider risks.

Discovery & Response

Quickly investigate and respond with relevant data.

Privacy Management

Safeguard personal data and build a privacy resilient workplace.

Compliance is a Cross-Departmental Initiative
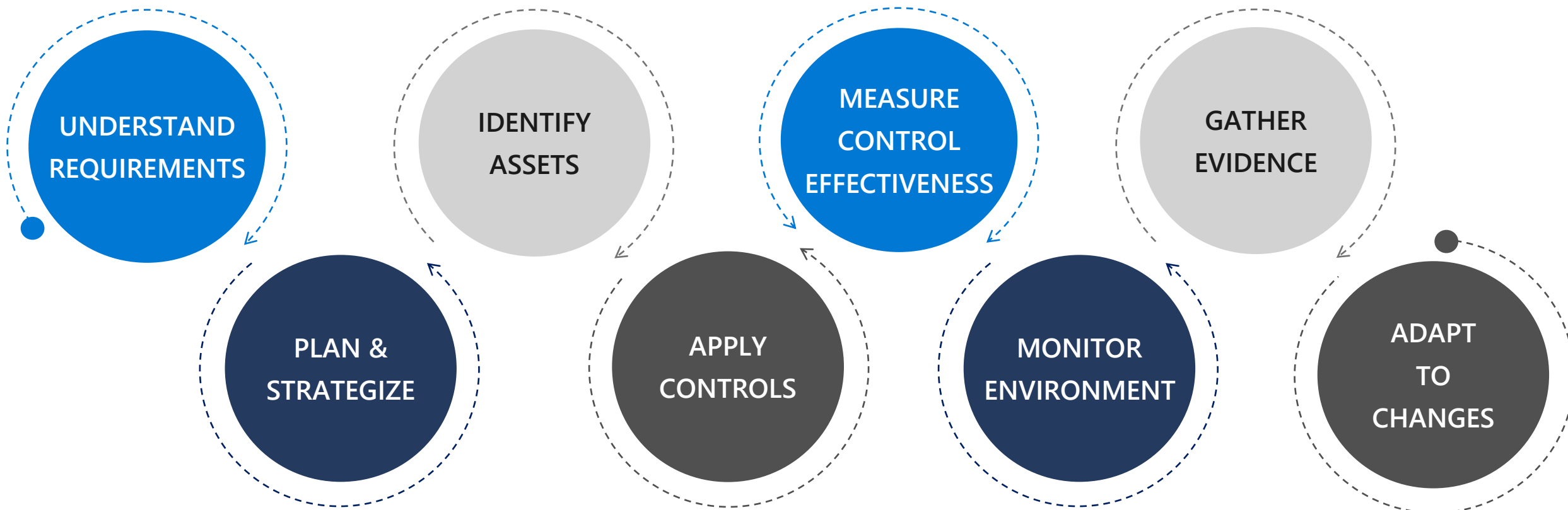
Privacy

Though it may not be a defined function in all orgs, privacy typically spearheads the **creation of policy and teaching of privacy best practices** across the org.

Legal

Legal, in partnership with outside counsel, **provide expertise and application on regulations** while simultaneously executing contracts and data sharing agreements.

Information Tech / Security

IT / InfoSec is responsible for **implementing technical solutions dictated by the privacy and compliance teams**. They are tasked with securing and protecting company data.

Risk / Compliance

Compliance, which is **generally a well-established function, especially in regulated orgs**, is tasked with ensuring the solutions and policies in place are sufficient and functional.

HR

HR is not only involved in recruitment, but also measured on **keeping talents in the company**, and connected with the compliance and privacy teams on specific requests like **Data Subject Requests** or **Insider Treat Tracking**.

Customers face a broad range of Insider risks

Data spillage
People overshare data and don't remove access rights after valid access.

IP theft
People go to the competition and take data with them for an advantage.

Illicit Activity
Corporate Fraud, Blackmail, and other Illegal activities.

Insider trading
Only the need-to-know should have access to critical financial data.

Leaks of sensitive data
M&A activities, Marketing strategies, Financial results, R&D results.

Data Loss
Mobile devices get stolen, lost and forgotten. Records get deleted without recovery options

"The right to be forgotten"
Registered consumers might request to be removed, as per Privacy regulations.

CISO   R&D   Legal   CFO   CISO   DPO   DPO

Supply Chain   HR   HR   IT Infra   M&A   Compl. Officer   Business

Leaks of sensitive 3rd party data
Supplier prices, competitor information, etc.

Confidentiality Violations
Unintentional sharing of confidential information.

Workplace violence and harassment
Company culture violations due to bad language and abuse.

Data Proliferation
Many tools can be used on various devices and in multiple locations, companies lose oversight.

Conflicts of Interest
People act in their own interest rather than in the companies' interest.

Regulatory compliance violations
Many new regulations and updates every day.

Accidental data leakage
Information which is derived through technological functions leads to a breach. (Autocomplete, for example)

What percentage of people do you think would take intellectual property from their previous employer?

Compliance Microsoft 365

Compliance Management

Assess compliance and respond to regulatory requirements.

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints.

Insider Risk Management

Identify and take action on critical insider risks.

Discovery & Response

Quickly investigate and respond with relevant data.

Privacy Management

Safeguard personal data and build a privacy resilient workplace.

Analytics

Results from the last scan for risk activities

The insights below provide a summary of anonymized user activities detected. Activities scanned are the same ones detected by insider risk policies. After reviewing the insights, view their details to drill down further and set up a recommended policy to address potential risks.

Insights from September 15 - September 28

Potential data leak activities

1.3% of your users performed exfiltration activities

Activity from 23K users scanned

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

View details

1.1% of users performed activities involving sensi info
0.8% of users downloaded SharePoint files
0.7% of users shared SharePoint sites with people outside your organization

Potential data theft activities

5.9% of users with a resignation date performed exfiltration activities

Activity from 219 users scanned

Recommendation: Set up a 'Data theft by departing users' policy

Detects and alerts you of potential data theft by departing users near their resignation or termination date.
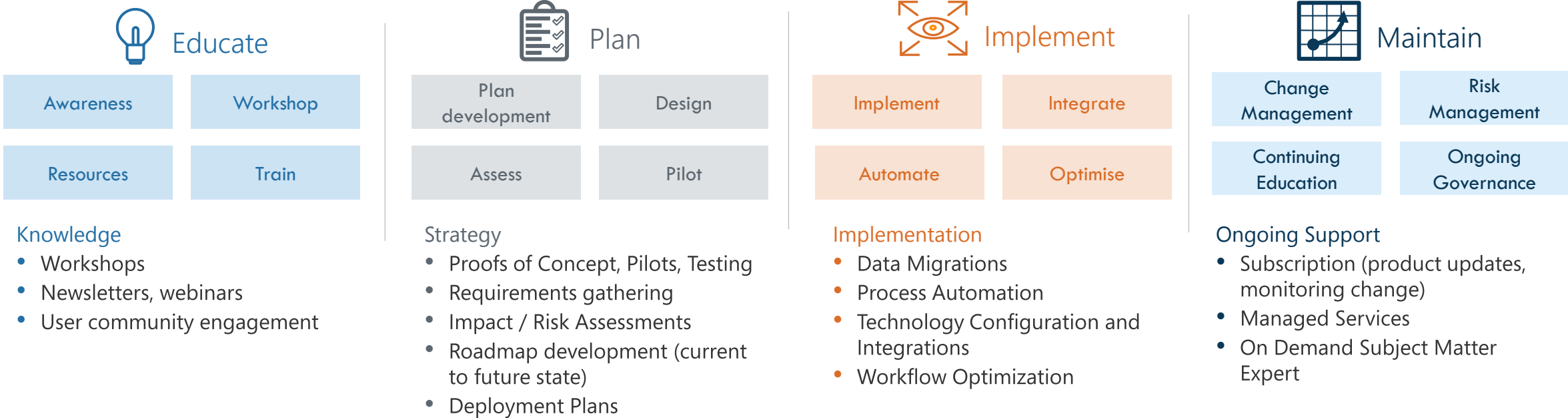
View details

4.6% of users with a resignation date performed activities involving sensitive info
3.2% of users with a resignation date downloaded SharePoint files
2.7% of users with a resignation date shared Shar sites with people outside your organization

Lighthouse supports the entire cloud transformation journey to M365

Educate

Awareness	Workshop
Resources	Train

Knowledge
- Workshops
- Newsletters, webinars
- User community engagement

Plan

Plan development	Design
Assess	Pilot

Strategy
- Proofs of Concept, Pilots, Testing
- Requirements gathering
- Impact / Risk Assessments
- Roadmap development (current to future state)
- Deployment Plans

Implement

Implement	Integrate
Automate	Optimise

Implementation
- Data Migrations
- Process Automation
- Technology Configuration and Integrations
- Workflow Optimization

Maintain

Change Management	Risk Management
Continuing Education	Ongoing Governance

Ongoing Support
- Subscription (product updates, monitoring change)
- Managed Services
- On Demand Subject Matter Expert

LIGHTHOUSE

Microsoft 365 Compliance Check

Implement a compliance strategy that accelerates and streamlines data security and governance while reducing risk.

ASSESSMENT

Assessment of your risk management priorities and compliance requirements.

ANALYSIS

Identify hidden compliance risks related to existing data within your organization.

RECOMMENDATIONS

Use M365 to simplify compliance efforts and improve data protection, retention, and compliance.

Microsoft 365 Compliance Assessment + Use Case Design

Onsite assessment to optimize efficiency of Microsoft 365 for eDiscovery, Data Loss Prevention, Information Governance, Records Management, and GDPR Compliance.

FORUM

Bring together cross-functional stakeholders
to discuss current and future state planning and evaluate configuration options.

CURRENT STATE

Understand the client's current operational models, identify risks or opportunities for improvement. Pair with data findings from Compliance Check.

EDUCATE

Educate stakeholders on Compliance technologies in context of their current processes.

RECOMMENDATIONS

Provide Target Operating Model Leverage Microsoft 365 to meet records management, eDiscovery, data governance, regulatory compliance goals and requirements.

Compliance Microsoft 365

Compliance Management

Assess compliance and respond to regulatory requirements.

Information Protection & Governance

Safeguard sensitive data across clouds, apps and endpoints.

Insider Risk Management

Identify and take action on critical insider risks.

Discovery & Response

Quickly investigate and respond with relevant data.

Privacy Management

Safeguard personal data and build a privacy resilient workplace.

Go to action

Business discussions	Compliance Accelerators	Processes vs Tech	Extended Services
Bring us in early to have the business discussions.	Compliance accelerators can be a foot in the door.	Business processes and strategies, harder than technology.	Managed service for customers.

LIGHTHOUSE