



THIS IS MY FIRST PRESENTATION.....

KATHRYN KALDESTAD

[KKALDESTAD@ACSICONNECT.COM](mailto:KKALDESTAD@ACSICONNECT.COM)

403.836.9555

# AGENDA

- **Who is ACSI – Introduction – Myself**
- **Shared Service agreement & group solutioning**

## Data

- **Define Data – What is it? Where is it?**
- **Physical Security**
- **Human Error – New to industry in records management**
- **90% of data leaks involve employees**
  
- **Proposing two of our partners for solutioning today**
- **Benefits of a consulting approach to customer engagement**
- **Data Sentinel – Canadian-based consultative approach**
- **Varonis – leading enterprise – solutions Co-pilot and partnered with Microsoft.**



# ABOUT ACSI



Founded in 2002, with headquarters located in Calgary, serving clients across North America. A one-stop shop for your organization's IT & cybersecurity needs



ACSI's team brings 20+ years of Enterprise & End User experience to IT & Data Security problems



Proven Services Offerings - Customized IT Infrastructure services , Cyber Security, MSP Services, EDR/MDR & 24/7 SIEM/SOC, Data Governance



Our customers include Government, Education & Crown Corporations along with Mid & Enterprise Class Critical Infrastructure organizations, aboriginal organizations and networks.



ACSI's localized Teams possess industry leading Certifications and strategic alignment with select solution technology Partners

# OUR SERVICES

NETWORKING

CYBER SECURITY



## NETWORK IMPLEMENTATION SERVICES

Comprehensive IT solutions and expert support to optimize your business operations and drive growth in the digital landscape



## CYBER ADVISORY

**We help business leaders develop a cybersecurity program aligned with the organization's strategic business objectives and risk appetite.**



## CYBER IMPLEMENTATION

We leverage battle-tested experience, knowledge, and technologies to provide you with the best cybersecurity solutions.



## CYBER MANAGED SERVICES

We help organizations address growing gaps in their ongoing cyber defenses by delivering a broad range of cybersecurity services as managed services.

# PROTECT & OPTIMIZE WHAT MATTERS MOST

## NETWORK IMPLEMENTATION SERVICES

- Network Assessment
- Network Design
- Network Optimization
- Network Implementation
- Technical Forensics

## CYBER ADVISORY

- Board Advisory
- Cyber Strategy & Roadmap Dev
- Cybersecurity Posture Assessment
- Privacy Risk Management
- Compliance Readiness Assessment
- Supplier Risk Management
- Cyber Insurance Advisory

## CYBER IMPLEMENTATION

- Governance, Risk & Compliance
- Penetration Testing
- Vulnerability Assessment
- Cloud Security
- Endpoint Protection
- Network Protection
- DevSecOps
- Identity & Privilege Access Management

## CYBER MANAGED SERVICES/ DATA GOVERNANCE

- vCISO
  - Cyber Awareness Training
  - Exposure Management
  - Security Operations Center
  - Cyber Threat Intelligence
- Governance:
- Risk Assessments
  - Consultancy
  - Implementation

---

**DATA SENTINEL – EMPLOYEE ADRIENNE MORRISON CURRENTLY WORKING ON A NUNAVUT – ARCTIC COLLEGE DELIVERY AND ASSESSMENT OF DATA POLICY, RULES AND BUILDING OUT A PLAN.**

**EXTENSIVE FIRST NATIONS EXPERIENCE ON SERVICES AND PROJECT DELIVERY.  
BEST RESOURCE: [HTTPS://FNIGC.CA/](https://fnigc.ca/) DEVELOPED THE OCAP PRINCIPLES FOR INFORMATION GOVERNANCE.**

**BC RESOURCE RELEVANT FOR ALL FN'S:  
[HTTPS://WWW.BCFNDGI.COM/BCNDGI](https://www.bcfndgi.com/bcndgi)**

AN INFORMATION/RECORDS MANAGER SPECIALIZING IN CREATIVE INFORMATION MANAGEMENT AND INFORMATION GOVERNANCE SOLUTIONS, DATA MANAGEMENT, POLICY DEVELOPMENT, RECORDS PROGRAM BUILDING AND IMPLEMENTATION, TRAINING AND EDUCATION AND SCALABLE RECORDS MANAGEMENT STRATEGIES. SHE ESTABLISHED THE RECORDS MANAGEMENT PROGRAM FOR TSLEIL-WAUTUTH NATION. AS AN INFORMATION MANAGEMENT CONSULTANT, SHE WORKS WITH ORGANIZATIONS TO ANALYZE AND DEVELOP SOLUTIONS AND STRATEGIES FOR IMPLEMENTING A RECORDS MANAGEMENT PROGRAM, FROM THE FOUNDATIONS TO SPECIAL PROJECTS. THROUGH HER WORK WITH INDIGENOUS ORGANIZATIONS AND FIRST NATIONS, SHE HAS PROMOTED RECORDS MANAGEMENT DEVELOPMENT AT ANY CAPACITY.

---

## **DATA IS THE SUBJECT – HOWEVER AI MUST BE INCLUDED**

Highly recommend joining the Cyber Alberta Community of Interest – It's free and they meet monthly for 90 minutes. Just completed the first in person event last week.

Also starting a “cyber” specific toastmaster chapter – can look at including the NIITA group in the future.





---

# Why Data Governance ?

Our goal is not to implement Data Governance, Data Quality  
Or Data Privacy...

Our goal is to identify where we can help you mitigate data risk and realize  
more value from your data assets.

# Common Outcomes

Reduced corporate risk associated with data privacy exposures

Reduced costs related to data issues (remediation and exception processing)

Reallocated knowledge resources to higher value activities

Establish Data policies, controls, procedures, remediation and culture that facilitate continuous improvement in the value realized from your data assets

Organizational structure to manage on-going Data Privacy program

Initiated culture shift toward more effectively managing data as a valuable corporate asset

# Approach

Establish methods to monitor the Data program impact on business KPI's (e.g., improved data trust, reduced data redundancy, reduced ROT data, more timely availability of high-quality data)

Identify people, processes, and data associated with the exceptions and the business processes to remediate data and process issues

Apply our cutting-edge technology with our data privacy and data quality scanning output to address pressing business needs

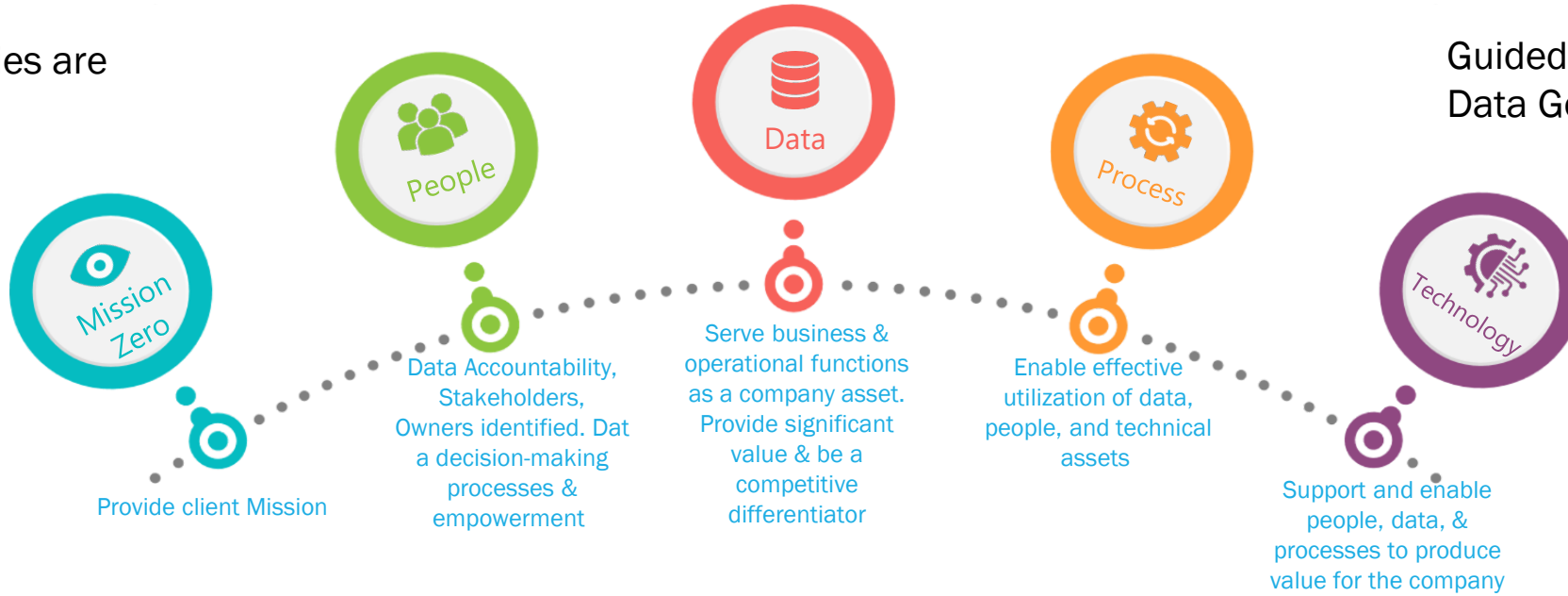
Initiate a cultural shift toward embracing the value and risk of the organizations data

Communication/Celebration of our data successes and associated business value

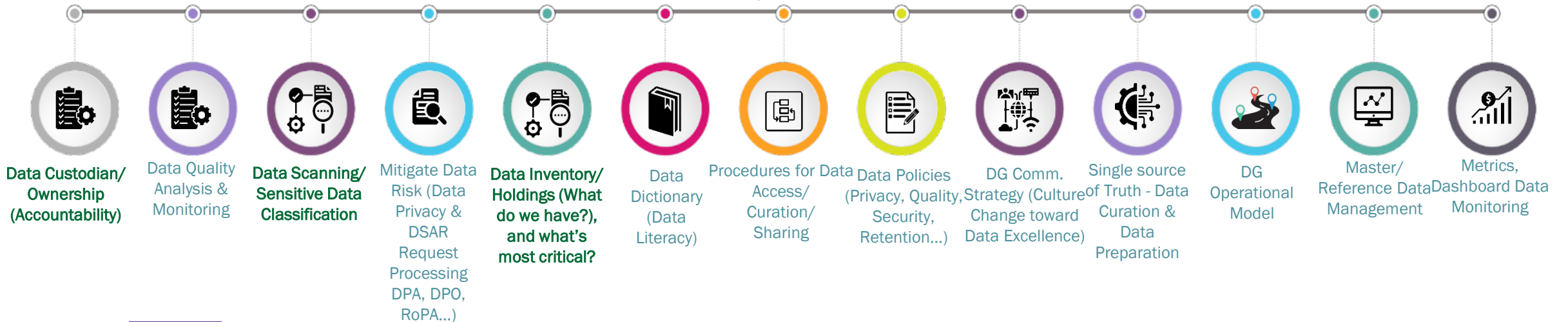
# Data Governance - Framework

Example DG capabilities are provided below:

Guided & Supported by the Data Governance Council



## Client DG Capabilities needed

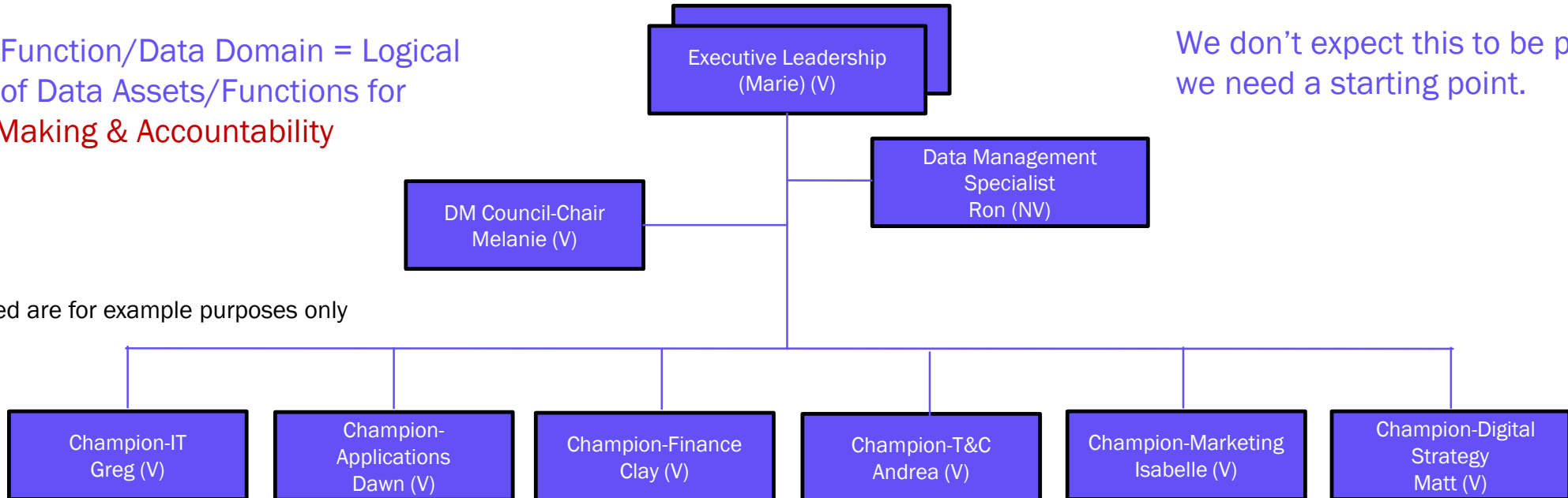


# DATA GOVERNANCE COUNCIL

Business Function/Data Domain = Logical Grouping of Data Assets/Functions for Decision-Making & Accountability

We don't expect this to be perfect. But we need a starting point.

The names listed are for example purposes only



# GUIDING PRINCIPLES

## Following Guiding Principles is vital to the success of Data Governance

**Data is a company asset** - It will be managed according to the prescribed governance policies.

**Data is identified and classified** - Information stored by the company will be identified and classified according to its sensitivity and content. This classification will determine how the information will be used and governed.

**Data is a sharable resource** - Data Assets shall be available for all legitimate and approved needs of the company.

**Individuals are Responsible for Data Assets** - There is an individual accountable for the appropriate management and governance of each information asset.

**Data users are identified and responsible** - An individual will be identified and be responsible for each access and change they make to information.

**Data is protected** - data is secured from unauthorized access and use.

**Data users are responsible** – each user is responsible for safeguarding the data under they have access to and use.

**Decision makers use appropriate data** - Decision makers are responsible for ensuring they are using information of appropriate quality and integrity for their work.

**Data is kept only as long as it is needed** - Information is disposed of appropriately when it is no longer needed for the purposes in which it was collected.

**Data quality is everyone's responsibility** - Information is validated, and where necessary, it is corrected and made complete.

**Data is managed in a cost-effective manner** - This is achieved through a well-defined data architecture that follows policies, standards, and best practices.

**Data and analytics will be used only for approved, ethical purposes** - Each new use of data for analytics will be reviewed by the DGC to ensure it adheres to policies and is used ethically, legally, and will not negatively impact the organization.

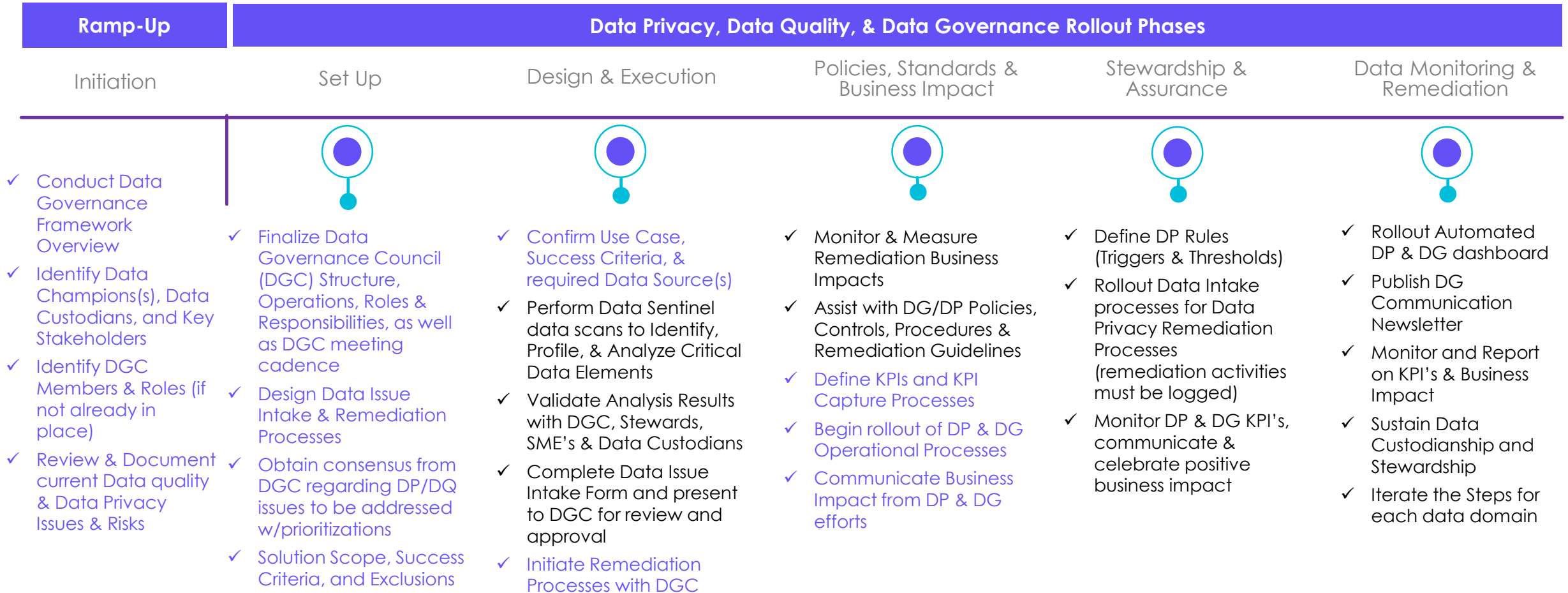
# Data Governance Roadmap Plan

---

The following Data Governance Implementation Roadmap Plan provides a stepwise approach for data remediation based upon the scan and profiling output

# KEY ACTIVITIES & TIMELINE

Next Steps (the DGC will determine objectives & priorities)





# Findings and Remediation Process

---

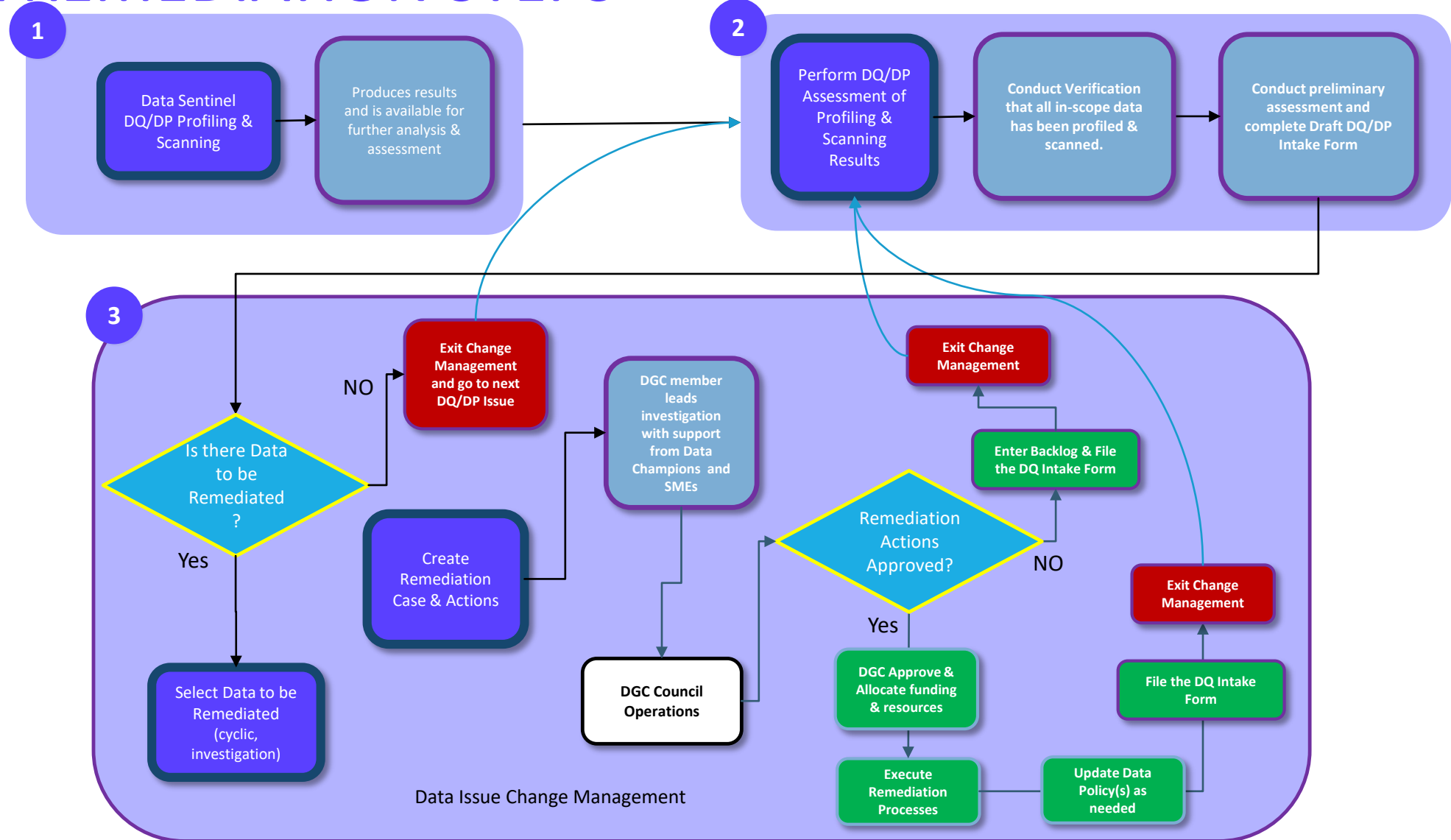
The following findings are from the Data Sentinel Discover, Scan, and Classify processes. We need actionable data issues to apply Data Governance Processes

# FINDINGS TO DATE

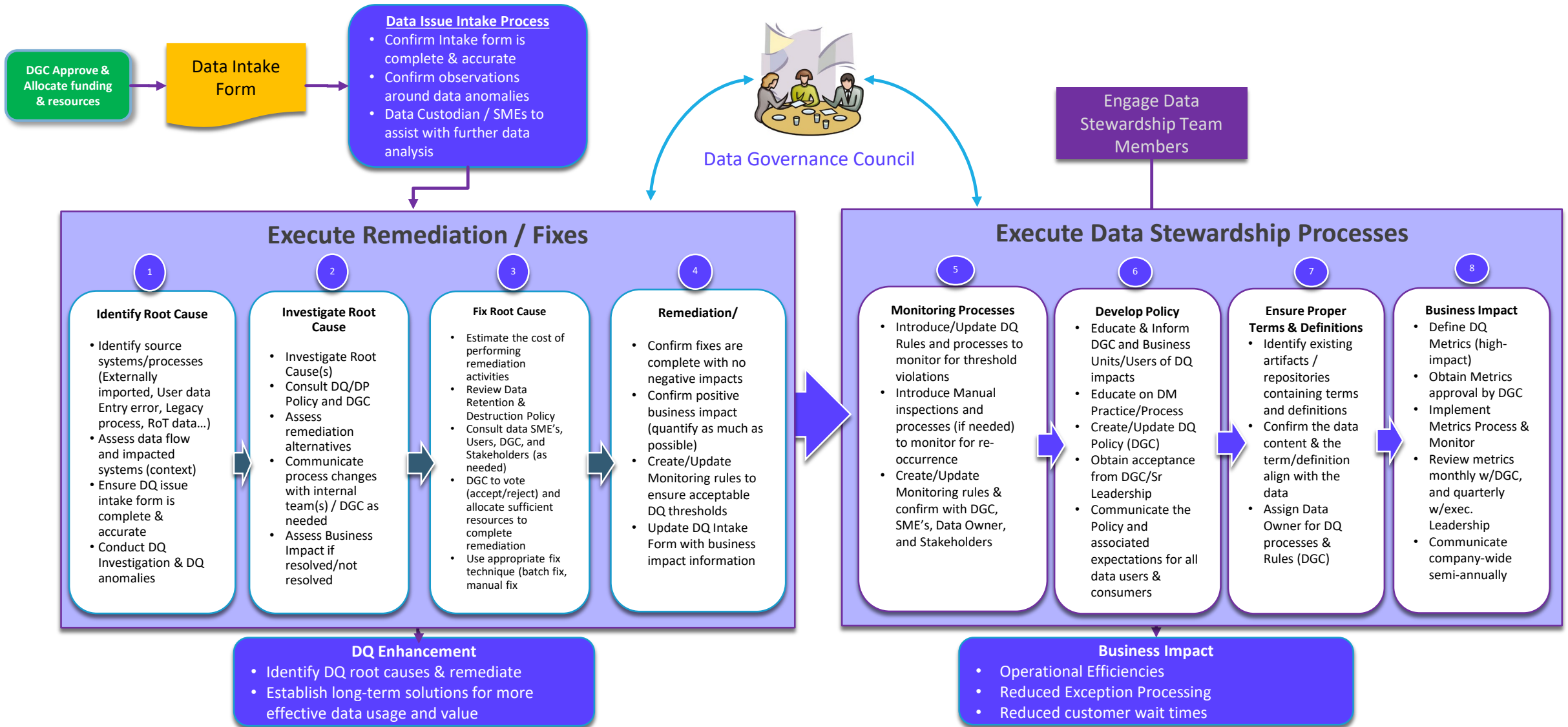
1. File Server Group – 11.7mm restricted records with many SIN's and SSN's
2. File Server GroupRCI – ~1mm SIN's, and 13k SSN's
3. File Server Shared – 940,598 restricted records
4. File Server SalesForce – 100's of SIN's, 1000's of Passports
5. File Server MTLFS01 – 100's of SIN's, 100's Bank Accts, 800 Passports
6. File Server GroupITG - ~800k Restricted records
7. File Server GroupHR - ~100k Restricted records
8. File Server First Nations – 2000 Restricted records

The Data Sentinel Scan, Classify, and Publish processes continue running, and the counts continue to grow

# DATA REMEDIATION STEPS



# DATA REMEDIATION PROCESS



# EXECUTIVE LEADERSHIP

Description	Monthly Investment (hours)		
<p>The primary roles of Executive Leadership is to communicate corporate Vision/Mission to ensure proper alignment of all Data Governance efforts and set the tone and commitment for company-wide support and participation. Finally, the executive leadership role provides guidance on corporate strategic objectives and capabilities needed to support the objectives.</p>	Meetings	Research	Implementation
	As-Needed	0	0
Functions:	Capabilities Involved with		
<p>1. Provide leadership –</p> <ul style="list-style-type: none"> <li>• Communicate corporate Vision/Mission to ensure proper alignment of all Data Governance efforts</li> <li>• Set the tone and commitment that drives company-wide support and participation</li> <li>• Provide guidance regarding corporate strategic objectives and capabilities needed to support the objectives</li> </ul>	Data Accountability		
	Data Inventory / Holdings		
	Data Privacy		
	Single Source of Truth		
	Data Dictionary/Terms & Definitions		
	Data Quality		
	Communication Strategy		
Example Activities			
<ol style="list-style-type: none"> <li>1. Occasional attendance at Data Governance Council Meetings to gain insight and status on progress and successes</li> <li>2. Provide Semi-Annual communication comments regarding the importance of data assets and the Data Governance efforts</li> <li>3. When necessary, participate in critical, high-impact data risk related matters</li> <li>4. Interact with data privacy/legal compliance team to ensure sufficient attention is given to data privacy needs</li> </ol>			

# DATA TECHNICIAN (CUSTODIAN)

Description	Monthly Investment(hours)		
<p>Technical resource, managing and providing IT , Operation, BI support and are associated with specific systems, applications, data stores, and technical processes. Their primary objective is to consistently deliver high quality governed data with context, providing business users with visibility into what data exists and where it resides and how to access and utilize it.</p>	Meetings	Research	Implementation
	2	2	4
Functions:	Capabilities Involved with		
<ol style="list-style-type: none"> <li>1. <b>Perform Data Functions</b> – such as database administration, data standardization rules, data privacy rules, data quality rules, data dictionary terms and definitions (2 hrs./month)</li> <li>2. <b>Identify Candidate Critical data sources</b> – and Critical Data Elements (1 hr./month)</li> <li>3. <b>Active Participation</b> – in data stewardship and data domain meetings (1 hr./month)</li> <li>4. <b>Provide Continued Creation &amp; Awareness</b> – of best practices, which may include data quality, data sharing, data curation, and data privacy activities (2 hrs./month)</li> <li>5. <b>Participate in cross domain collaboration</b> - to ensure continuity of applications/data that span data domains (this will likely occur frequently) (2 hrs./month)</li> </ol>	Data Accountability		
	Data Inventory / Holdings	✓	
	Data Privacy	✓	
	Single Source of Truth	✓	
	Data Dictionary/Terms&Definitions	✓	
	Data Quality	✓	
	Communication Strategy		
Example Activities			
<ol style="list-style-type: none"> <li>1. Assist Data Stewards, Data Custodians with data related questions, the go to person from IT and Operations.</li> <li>2. Facilitate questions and answers to specific technical data functions (i.e., data ingestion, data access, data staging, data movement, data transformation, data quality...).</li> <li>3. Participate in data issue resolutions requiring technology functions</li> <li>4. When possible, make intentional efforts to share their data knowledge with others throughout the data community</li> <li>5. Work with data privacy legal compliance team to ensure data, processes, and technology functions are obfuscated if/as needed</li> <li>6. Provide expertise in technologies used to analyze and manage data assets</li> </ol>			

# PRIVACY / LEGAL

Description	Monthly Investment (hours)		
<p>The legal, compliance and enterprise risk functions will operate at the enterprise level to ensure data regulatory risk activities are centralized for oversight. These functions will ensure alignment with geographical regulatory requirements, and monitor the data risk profile of the organization</p>	Meetings	Research	Implementation
<p><b>Functions:</b></p> <ol style="list-style-type: none"> <li><b>Ensure Data Privacy Risk Management</b> – is established as a business function that aims to identify, assess, and prepare for scenarios that may introduce data risk to operations and objectives. In addition, this role will help to ensure a plan is in place to mitigate these risks with internal controls and audits (1 hr./month)</li> <li><b>Align Regulatory Rules with Corporate Investment Policy</b>– Implement solution to align geographical data regulatory requirements with internal policy and assist in regulatory obligations such as conducting a Data Privacy Assessment, responding to Data Subject Access Requests... (1 hr./month)</li> <li><b>Participate In Data Compliance Oversight Activities</b> – Commence efforts to design processes that ensure proper oversight of data related communications to ensure alignment with legal and corporate data privacy policy (2 hrs./month)</li> </ol>	1	3	0
<p><b>Example Activities</b></p> <ol style="list-style-type: none"> <li>Leverages expertise and capabilities of compliance functions to reduce data privacy related risk</li> <li>Define repeatable processes to ensure continuity across regions</li> <li>Technology allows for greater analysis, identification, and monitoring for data privacy risk</li> <li>Enable the organization to be more proactive to potential data privacy issues</li> </ol>	Capabilities Involved with		
	Data Accountability	✓	
	Data Inventory / Holdings	✓	
	Data Privacy	✓	
	Single Source of Truth	✓	
	Data Dictionary/Terms & Definitions		
	Data Quality	✓	
	Communication Strategy		

# DATA STEWARD

Description	Monthly Investment(hours)		
<p>The Data Steward is an expert on the application, meaning, and history of various data assets, and contributes insight and guidance to the Data Governance team regarding their detailed working knowledge of the data.</p>	Meetings	Research	Implementation
	3	2	2
Functions:	Capabilities Involved with		
<ol style="list-style-type: none"> <li><b>Provide Guidance</b> - in terms of functional and operational data expertise, including specific data creation/origination, consumption, and disposition details (2 hrs./month)</li> <li><b>Enable/Facilitate</b> - the free flow of data knowledge throughout the enterprise (1 hr./month)</li> <li><b>Assist with determining the most critical data elements</b> – and specifics regarding data characteristics (1 hr./month)</li> <li><b>Attend various data stewardship meetings</b> – to contribute their data expertise on an as-needed basis (2 hrs./month)</li> <li><b>Participate in cross domain collaboration</b> - to ensure continuity of applications/data that span data domains (this will likely occur often) (1 hr./month)</li> </ol>	Data Accountability	✓	
	Data Inventory / Holdings	✓	
	Data Privacy	✓	
	Single Source of Truth	✓	
	Data Dictionary/Terms&Definitions	✓	
	Data Quality	✓	
	Communication Strategy	✓	
Example Activities			
<ol style="list-style-type: none"> <li>Facilitate questions and answers pertaining to their area of data expertise</li> <li>Recommend and in some cases develop data quality rules/fixes</li> <li>Participate in data quality issue resolution</li> <li>When possible, make intentional efforts to share their data knowledge with Data Domain Custodians, IT, and Data Consumers</li> <li>Help to embed Data Governance practices at the point of access, making it an active and natural part of the work activities</li> <li>Assist with creation of Business Terms/Definitions, Classification, Data Policies/Governance Rules definitions are complete</li> </ol>			



# DATA CONSUMER

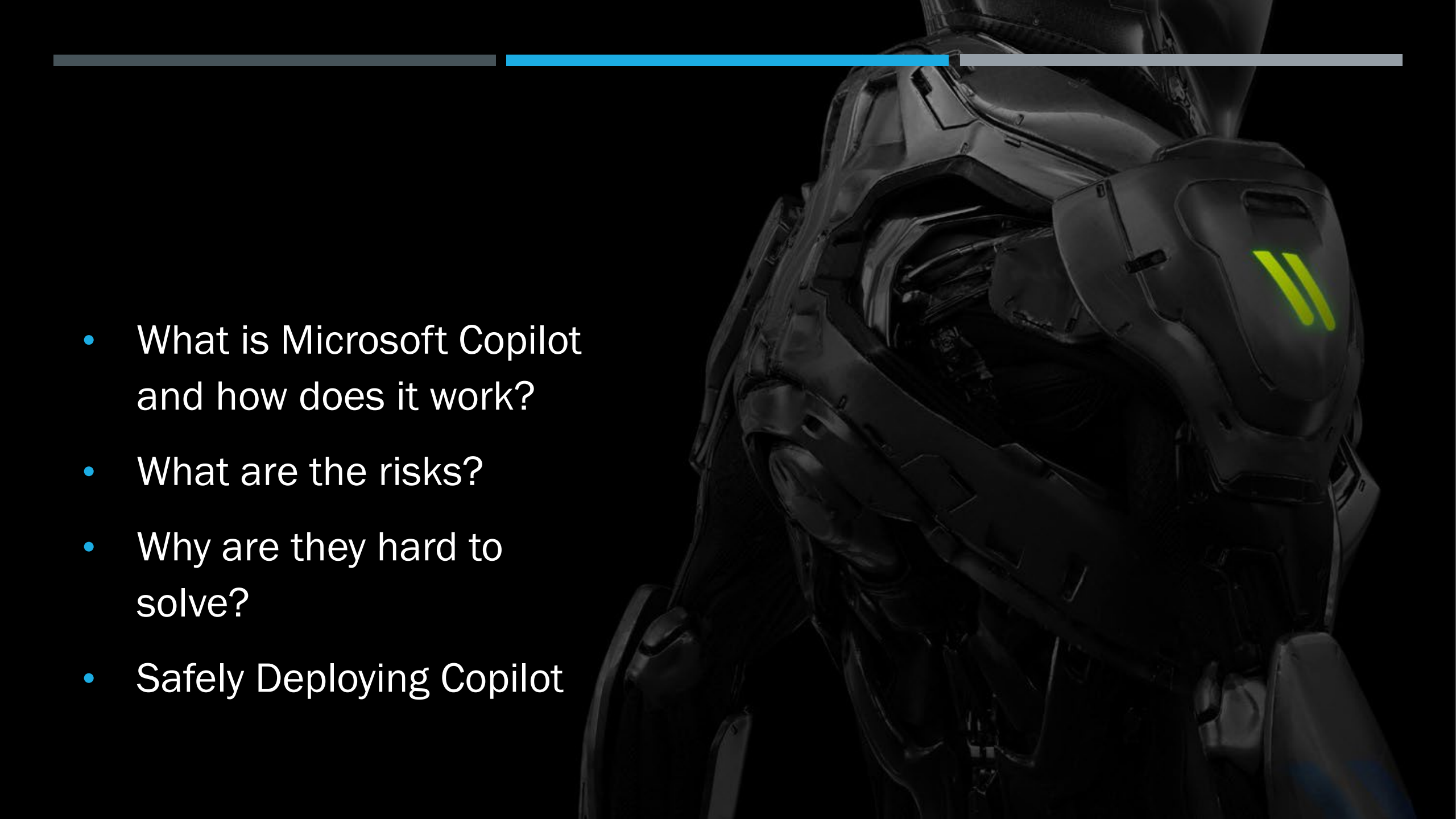
Description	Monthly Investment (hours)		
<p>An employee/consultant/third party organization or application/system having some level of interaction with data in their day-to-day responsibilities either to share or to use or to retrieve the information for business needs as part of their role within the organization. It is one of the most generic roles.</p>	Meetings	Research	Implementation
	4	2	2
Functions:	Capabilities Involved with		
<ol style="list-style-type: none"> <li>1. Have access to data for operational and analytical needs</li> <li>2. Ensure data has business value and use only for the purpose for which it is collected</li> <li>3. Assist in Identifying/rectifying data issues associated with processes and applications</li> <li>4. Adhere to data guidelines and standards</li> </ol> <p>Data Consumers can also be value-add consumers that curate and distribute to other downstream consumers</p>	Data Accountability		
	Data Inventory / Holdings		✓
	Data Privacy		✓
	Single Source of Truth		
	Data Dictionary/Terms&Definitions		✓
	Data Quality		✓
	Communication Strategy		✓
Example Activities			
<ol style="list-style-type: none"> <li>1. Consumer of the Reports generated – Business Analytics Services</li> <li>2. An automation using the data to drive processes (Tool and process consuming data without human intervention I.e., auto-adjudication)</li> <li>3. Report data anomalies via the Data Issue Intake process</li> </ol>			



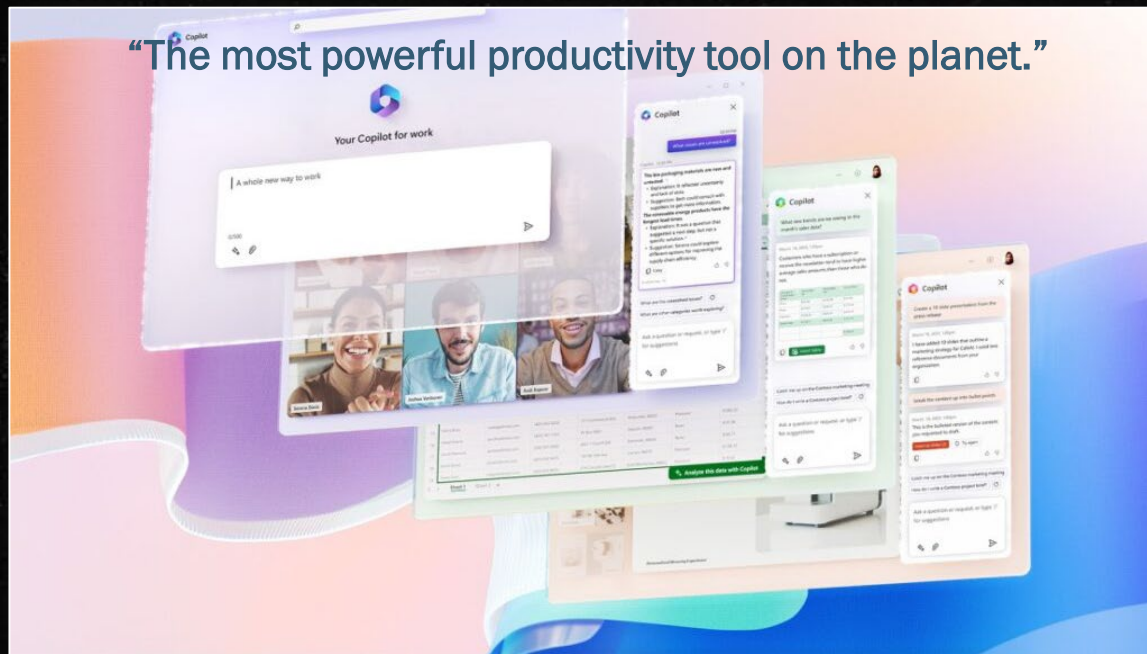
All [Microsoft] partners noted that **security** and **privacy** concerns continue to be the primary issue to [Copilot] adoption

- Karl Kierstead, UBS Research



- 
- What is Microsoft Copilot and how does it work?
  - What are the risks?
  - Why are they hard to solve?
  - Safely Deploying Copilot

# What is Microsoft Copilot?



- Generative AI enabling the automatic combination of data based on user prompts
- A content creation shortcut relying on user permissions for data access
- Good-intentioned exploiter of immature data access governance and lifecycle management programs/processes
- Creator of additional risk by providing end user visibility to data not relevant to job role

Chat

Teams

Calendar

Calls

Files










...

Apps

Pinned

-  **Copilot** 9:15 AM  
Good morning Kat!
-  **Cassandra Dunn** 6/2  
Ok. I'll send an update later
-  **Aadi Kapoor** 6/2  
You: Great work!
-  **Eric Ishida** 8:40 AM  
Sure, I'll set something for next week t...

Recent

-  **Cortex Framework** 8:41 AM  
Kayo: The review went really well! Can't wait...
-  **Will Little** 7:45 AM  
I don't see that being an issue, Can you ta...
-  **Marie Beaudouin** 1:21 AM  
Ohh, I see, yes let me fix that!
-  **Hillary Reyes** 1:07 AM  
Haha!
-  **Charlotte and Babak** 12:48 AM  
Charlotte: The client was pretty happy with...
-  **Reta Taylor** 12:40 AM  
Ah, ok I understand now
-  **Joshua VanBuren** 12:29 AM  
Thanks for reviewing
-  **Daichi Fukuda** 12:20 AM  
You: Thank you
-  **Kadji Bell** 12:03 AM  
You: I like the idea, let's pitch it!

Copilot 9:15 AM



Good morning Kat!

Here are some ideas that might help you get started:

- Get a summary of everything you need to catch up on, including meetings
- Find and use info that's buried in documents or lost in conversations
- Create content with all of it—drawing from your files, conversations, events, topics, and more

As your Copilot, I'm here to assist you but I do make mistakes, so sources are provided for your review when possible.

What's going on with EraNext?

Summarize the Green Builder's summit doc





**Create content with Copilot** [X]

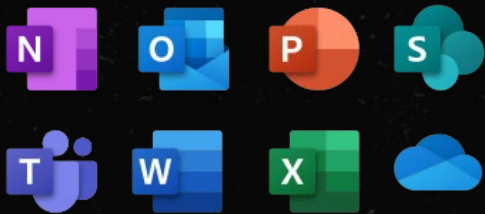
A job description for... 10 ideas for... A press release for... A project proposal about... [refresh]

Describe what you'd like to create, and Copilot will generate a draft

[grid] [eraser] [send]



## Microsoft 365 Copilot



## Microsoft's approach to AI security:

- ❑ User inputs a prompt in an app like Word, Outlook, or PowerPoint
- ❑ Microsoft gathers business content based on their M365 permissions
- ❑ Prompt is sent to the LLM to create a response
- ❑ Microsoft performs post-processing responsible AI checks

# Microsoft's Cloud Permissions Report

- Most identities are greatly over permissioned
- More than half of permissions are high risk
- 99% of user permissions are unused





# What does Microsoft say you should do?

The following capabilities from Microsoft Purview strengthen your data security and compliance for [Microsoft 365 Copilot](#):

- Sensitivity labels and content encrypted by Microsoft Purview Information Protection
- Data classification
- Customer Key
- Communication compliance
- Auditing
- Content search
- eDiscovery
- Retention and deletion
- Customer Lockbox

Microsoft 365 Copilot uses your existing permissions and policies to deliver the most relevant information, building on top of our existing [commitments](#) to [data security and data privacy in the enterprise](#). This means it is important to have good content management practices in the first place. For many organizations, content oversharing, and data governance can be a challenge. Content oversharing is when content is shared beyond the needed audience either intentionally or accidentally. Learn about some of the things your organization can do to detect and prevent oversharing in the [new era in content management and security in SharePoint, OneDrive, and Teams](#), watch [this video](#), and read [this article](#) to get details on how to adopt content management best practices.

# Copilot Security Challenges

Employees have access to far too much data

Sensitive data is often not labeled or mislabeled

Insiders can quickly find and exfiltrate data

Shared links expose data org-wide and publicly

Right-sizing access and enforcing least privilege is impossible to do manually

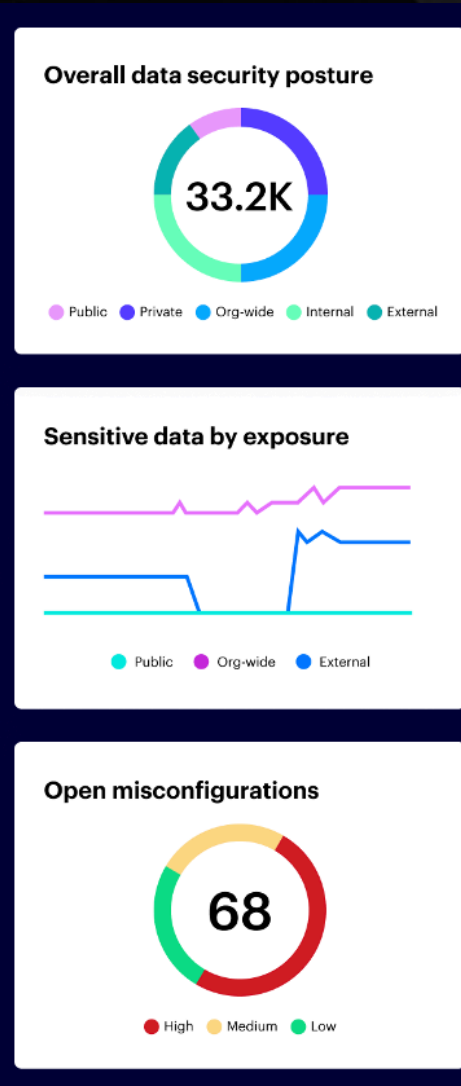
Generative AI can create net new sensitive data extremely fast



**PHASE 1: BEFORE COPILOT**









# 1. Deploy and Complete Initial Scans

- ✓ Data sensitivity
- ✓ Configuration and security posture
- ✓ Access controls and shared links
- ✓ Connected third-party apps
- ✓ Existing labels



## 2. Add/Fix Purview Sensitivity Labels

- + Automatically identify files that are missing or don't have accurate labels
- + Automatically identify and fix misapplied labels
- Automatically identify and fix files with missing labels

File	Classification results	Classification labels
	PCI	
	GDPR, PII	 
	CCPA, PII	 

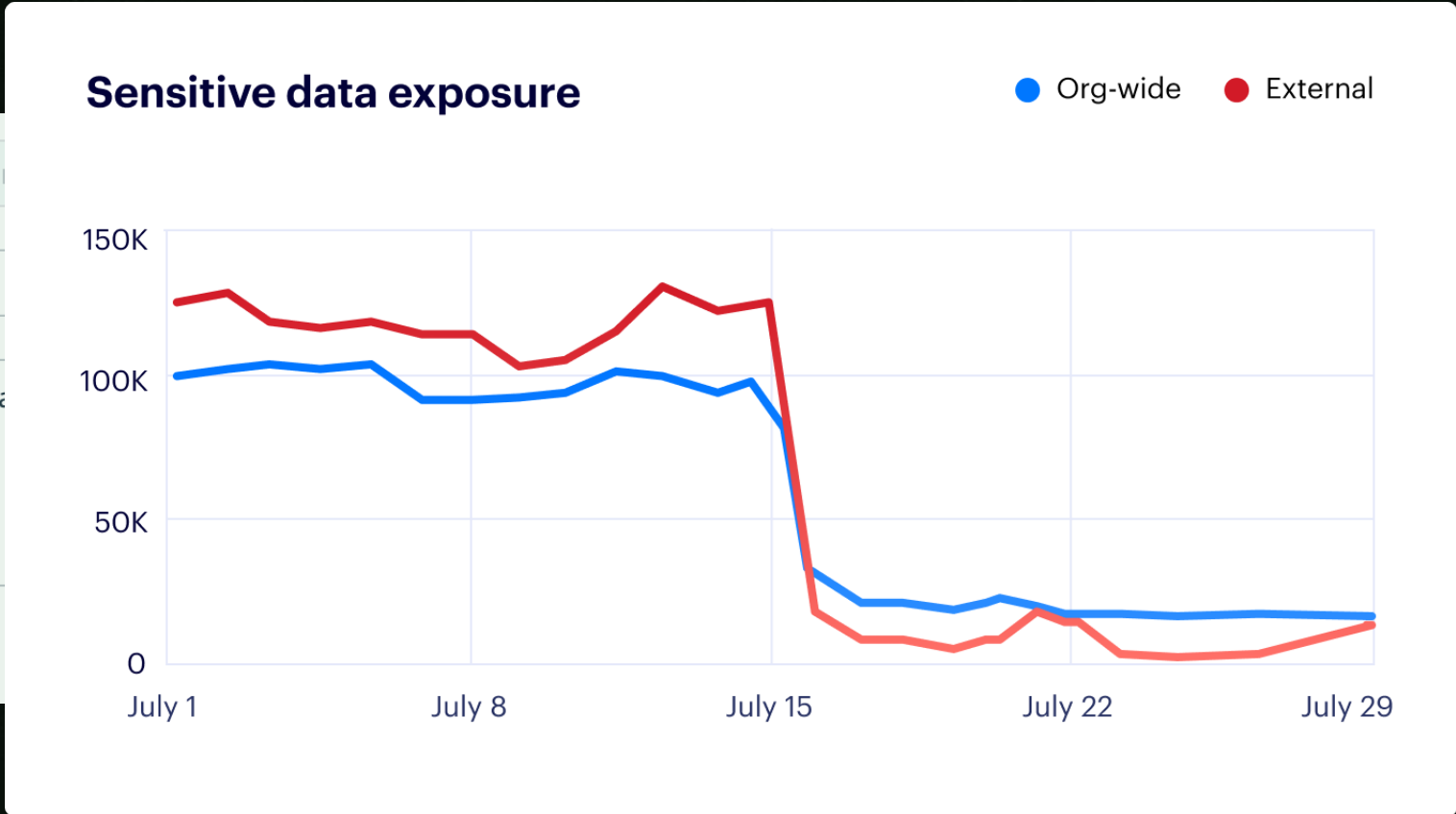
# 3. Remediate High Risk Exposure

Type: Remove collaboration links

Policy name: Remove "Anyone in the organization" type

Description: This policy removes collaboration links with the link type.

State:  Enabled



# 5. Enable Downstream DLP

- ✓ Encrypt sensitive data
- ✓ Prevent risky sharing
- ✓ Block attempted exfiltration
- ✓ Apply file-level controls
- ✓ Enforce residency and retention

Microsoft 365 compliance

Data Loss Prevention > Create a policy

Choose the information to protect

Name your policy

**Locations to apply the policy**

Policy settings

Test or turn on the policy

Review your settings

### Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info on Windows devices is now in preview. [Learn more about the capabilities](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All <a href="#">Choose distribution group</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	SharePoint sites	All <a href="#">Choose site</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	OneDrive accounts	All <a href="#">Choose account</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All <a href="#">Choose account</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Devices	All <a href="#">Choose user or group</a>	None <a href="#">Exclude</a>
<input checked="" type="checkbox"/> On	Microsoft Cloud App Security	All <a href="#">Choose instance</a>	None <a href="#">Exclude</a>



## **PHASE 2: AFTER COPILOT**





## Immediate pattern detected: user actions resemble ransomware

### Risk Reasons

- [10] The alerted user is not the owner of any accessed paths
- [10] There have been low number (2) of distinct users which triggered alerts of the same type in the last 7 days
- [10] The user has experienced a surge in OpCodes within the past 24 hours.
- [5] Few (2) distinct authentication attempts to the device were made.
- [5] The user triggered the Threat Model with a Low frequency (3 alerts in the last 30 days).
- [0] The alerted user has not been enabled or disabled during the specified timeframe.
- [0] The alerted user is an old user and was created on 2008-11-18 10:22:18.
- [0] The alerted user did not generate any new event codes in the last 5 days.
- [-5] The Threat Model alert triggering frequency is Medium (13 alerts in the last 30 days).
- [-10] The device alert triggering frequency is high (21 Alerts across 30 days).
- [0] The Alerted user has not authenticated to any new devices in the 3 days.
- [-10] Couldn't detect the ransomware extension



15 (Not a Real Threat)

# 7. Automate Policies for Access Control

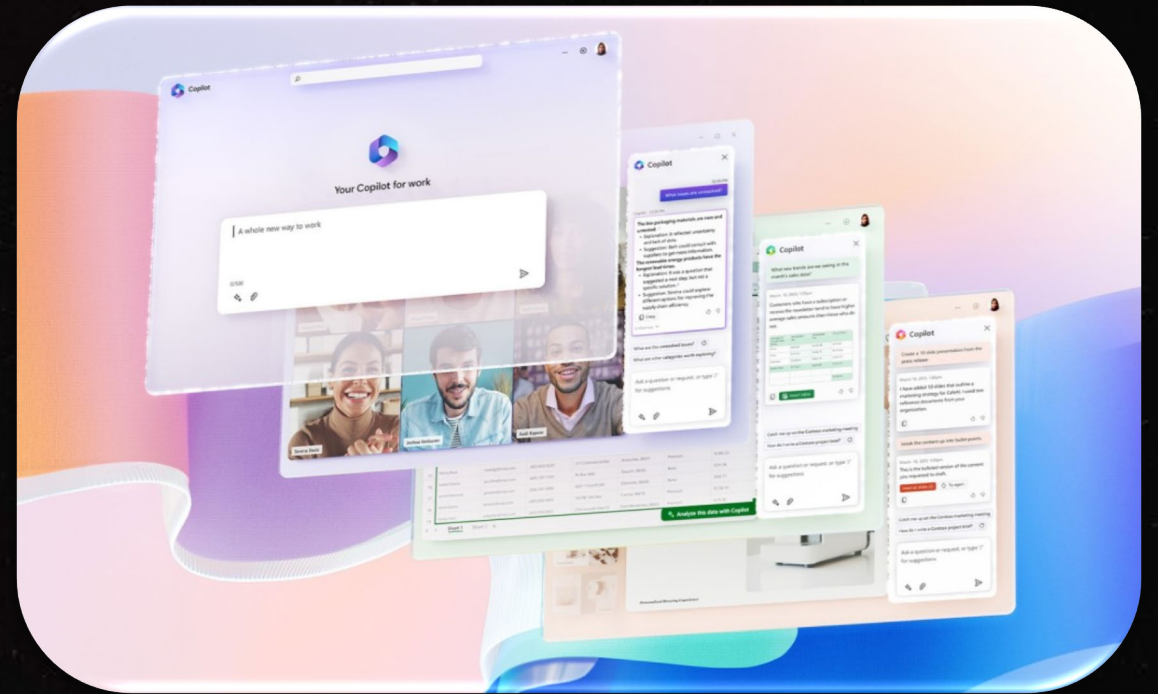
The screenshot displays the Microsoft Purview compliance center interface for configuring an automated policy. At the top, the resource is set to 'prod1.sharepoint.com'. Below this, there are several filter criteria: 'Permission' (set to 'Removal link'), 'Removal link' (set to 'Yes'), 'Link type' (set to 'anyone on the internet' and 'org-wide'), and 'Sensitive (incl. subfolders)' (set to 'OneDrive' and 'SharePoint Online'). An 'Add filter' button is visible below the filters. In the 'Actions' section, the 'Remove permission' action is selected. The 'Execute actions' dropdown is set to 'Continuously'. An inset line graph titled 'Org-wide sharing links' shows the number of links over time, with a sharp drop in August.

Month	Number of Links
4/1	~40k
5/1	~45k
6/1	~70k
7/1	~75k
8/1	~0
9/1	~0

- ✓ Revoke excessive access
- ✓ Fix misconfigurations
- ✓ Fix labels
- ✓ Disable third-party apps
- ✓ Data lifecycle
- ✓ Data residency

# Use Copilot Safely with Varonis

- Automatically enforces least privilege by removing excessive permissions and sharing links
- Automatically fixes incorrect or missing labels – on data generated by humans or AI
- Ensures downstream controls like encryption and DLP work without disruption
- Monitors data and alerts on abnormal behavior



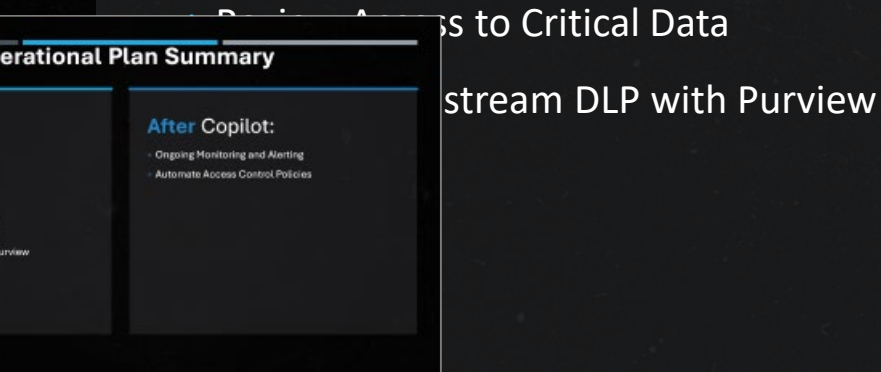
# Operational Plan Summary

## Before Copilot:

- + Deploy Varonis
- + Complete Initial Scans
- + Add/Fix Data Labels
- + Remediate High-Risk Exposure

## After Copilot:

- + Ongoing Monitoring and Alerting
- + Automate Access Control Policies



# Varonis enhances your existing stack

## What we can replace:

- DSPM
- SSPM
- Data Discovery & Classification
- Data Access Governance
- Identity Security (ITDR)
- File & AD Auditing Tools
- UBA
- Insider Risk Management

## What we make better:

- Microsoft Security (E5, Purview)
- Endpoint (EDR)
- Perimeter (SASE, CASB, ZTNA)
- AppSec (SAST, WAF)
- Cloud Infra (CWPP, CNAP, CSPM)
- SecOps (SIEM, SOAR, XDR)
- Identity Management (IAM)

# How we start: Free Copilot risk assessment

## Map key data stores

- Enable full platform access
- Analyze permissions, identities, configurations
- Discover & classify data

## Monitor data usage

- Enable activity
- Enable meaningful, high-fidelity alerts
- Accelerate Investigations

## Prioritize risks

- Exposed sensitive data, shared links, rogue admins
- Active Directory & SaaS attack paths
- Compliance gaps

## Assign IR team

- Introduce dedicated IR analyst
- Optimize alerts as-needed
- Notify you of any suspicious activity





**ACSI**  
SECURING NETWORKS

**THANK YOU – QUESTIONS?**