

# [Sample Company] | Insights Health Check

## Executive Summary

Data security concerns in M365 environment are not just limited to the sensitivity of the contents. It is also just as much about who has access to these contents. It is typical to have sensitive content in M365 and cannot be avoided for most organizations. The key is allowing the business to use M365 for sensitive contents in a way that ensures only the appropriate people have access to the content.

Microsoft 365 (M365) Data Loss Prevention (DLP) helps address this problem. However, not all organizations are mature enough to implement DLP or accommodate the additional operational overhead necessary to support DLP. In addition, there are scenarios where DLP is not adequate or too heavy handed (too much of a “one-size-fits-all” approach).

As a complement to M365 DLP, Insights identifies high risk contents in the environment and provides quick access to the audit trail of the content. This allows the organization to review and assess if the risk is justified by the business needs, and to remediate the issue if not.

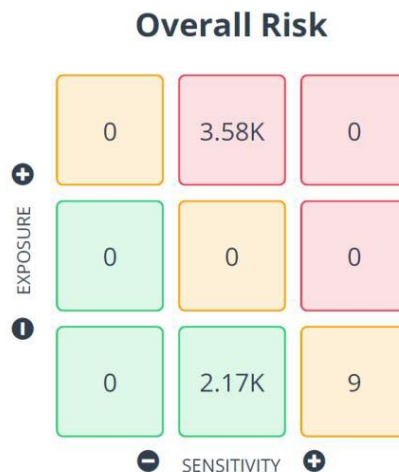
Insights looks beyond the sensitivity of the content in calculating the risk by considering the exposure of the content. A high-sensitive document that is only visible to 1 person is not as high a risk as a medium-sensitive document that is accessible to everyone in the organization or to an external guest. This Insights health check gives a summary of where the high-risk contents are at a specific point in time. The matrix below provides a high-level summary of the risk found in [Sample Company]’s M365 environment.

### Risk Summary

#### What does risk mean for your organization?

The Overall Risk analyzes your organization external risk by looking at guests or the content shared outside against potential sensitive or confidential information as set by your administrator according to rules for Microsoft 365 usage.

This helps to prioritize your risk to focus on what is important to your business.





## ***Empowering Technology. Powered by People.***

The rest of this assessment document describes the details of the health check results and recommendations on how to remediate the risks found in the environment.

### **Configuration and Definition**

Insights looks at the Sensitivity and Exposure of objects in M365 in calculating risk. Sensitivity and Exposure can be classified as High, Medium, and Low. Sensitivity level describes if the object contains any sensitive contents (and how many), whereas Exposure level describes how exposed the object is (who has access to the object).

#### **Sensitivity Level**

Insights uses native M365 sensitive information types, custom sensitive information types defined by the organization, and/or sensitivity labels to determine Sensitivity level. For this health check scan, [Sample Company] leveraged the built-in sensitivity definitions in Insights. For each built-in sensitivity definition, default settings are provided for both the High and Medium sensitivity levels.

- High sensitivity level – When ALL the conditions are matched in a sensitivity definition, the object's sensitivity level is High
- Medium sensitivity level – When ANY of the conditions are matched in a sensitivity definition, the object's sensitivity level is Medium

\*Note: There are no default settings for the Low sensitivity level. N/A is displayed for container levels and the objects that do not match the default settings for the High or Medium sensitivity level.

Refer to the table below for the conditions used in each built-in sensitivity definition by default.

Sensitivity Definition	Conditions
U.S. Personally Identifiable Information (PII) Data	U.S. Individual Taxpayer Identification Number (ITIN) U.S. Social Security Number (SSN) U.S. / U.K. Passport Number
U.S. Health Insurance Act (HIPAA)	U.S. Social Security Number (SSN) Drug Enforcement Agency (DEA) Number
U.S. Patriot Act	Credit Card Number U.S. Bank Account Number U.S. Individual Taxpayer Identification Number (ITIN) U.S. Social Security Number (SSN)
U.S. State Breach Notification Laws	Credit Card Number U.S. Bank Account Number U.S. Driver's License Number U.S. Social Security Number (SSN)
U.S. Federal Trade Commission (FTC) Consumer Rules	Credit Card Number U.S. Bank Account Number ABA Routing Number U.S. Financial Data Credit Card Number U.S. Bank Account Number ABA Routing Number
U.S. Gramm-Leach-Bliley Act (GLBA)	Credit Card Number U.S. Bank Account Number U.S. Individual Taxpayer Identification Number (ITIN) U.S. Social Security Number (SSN)

### Exposure Level

Insights scans and analyzes the permissions for each object in M365 to determine the Exposure level of each object. For this health check scan, [Sample Company] defines Exposure level as follows:

 **High Exposure Level** ⓘ

[Edit](#)

**External Sharing**

- External Users with Direct Access	> 0
- Azure AD Groups with External Users	> 0
Anonymous Link	
Everyone	
Large Azure AD Group	> 30
Direct Sharing	> 30

 **Medium Exposure Level** ⓘ

[Edit](#)

Large Azure AD Group	20 - 30
Direct Sharing	20 - 30

 **Low Exposure Level**

If an object does not match the High or Medium exposure level conditions, it will be automatically classified as Low exposure level.

See below for an explanation for each of the Exposure level setting.

**External Users with Direct Access:** The number of active external users outside your Microsoft 365 subscription with direct access has reached the threshold.

**Azure AD Groups with External Users:** The Azure AD group with access to objects in which the number of external users reaches the configured threshold.

**Anonymous Link:** Anyone with the link (inside or outside your organization) can access the object. These links can be freely passed around and are valid until the link is deleted or expires (if an expiration date has been set).

**Everyone:** The object has been shared with Everyone, All Users (membership), or All Users (windows).



***Empowering Technology. Powered by People.***

**Large Azure AD Group:** The Azure AD group with access to objects in which the number of users reaches the configured threshold.

**Direct Sharing:** The number of active users, security groups, and users in SharePoint groups to which the object has been given access reaches the configured threshold.

### **Scope of Health Check Scan**

Insights can be configured to scan Teams, SharePoint Online Sites, OneDrive for Business, and M365 Groups. It can be configured to scan all workspaces and objects or a subset of the workspaces in each of the above M365 workload. For this health check scan, [Sample Company] has configured the scope to scan the full M365 tenant.



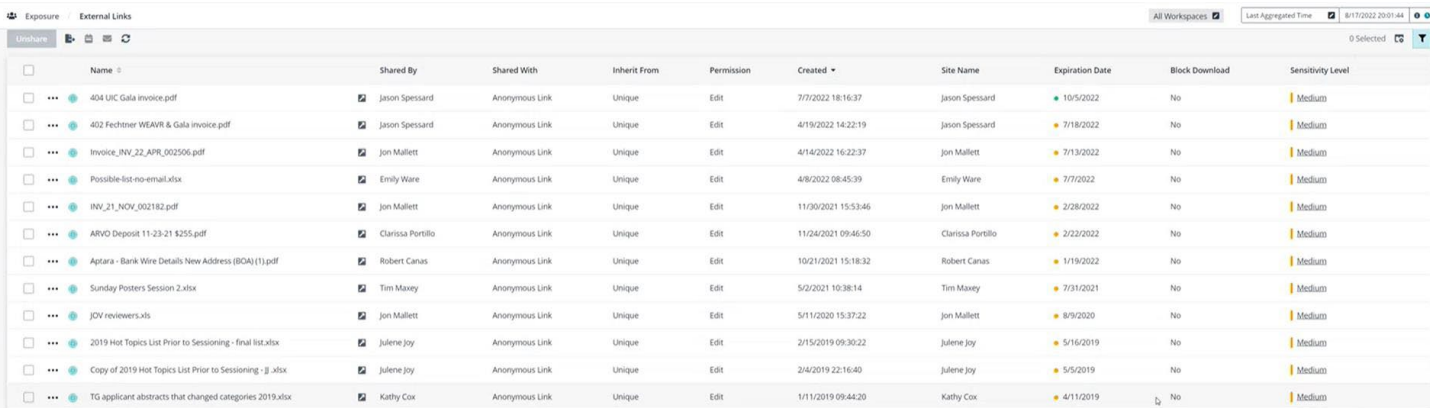
## Health Check Details Results and Recommendations

This section walks through the results of the Insights Health Check. Each risk metric in the report is explained along with the reasons why a business needs to care about the metric and recommendations on how to mitigate the risks associated with the metric. The report starts with metrics at the tenant level and breaks down each metric for each of the M365 workload (Teams, SharePoint Online, OneDrive for Business and M365 Group). Where similar metrics appears at the workload level, the explanation and recommendations given at the tenant level will not be repeated. Only risk metrics specific at the workload level will be expounded.

### Tenant Wide

#### High and Medium Risk Contents

The Health Check scan has identified a total of 3,580 high-risk contents and 9 medium-risk contents in the M365 environment. The high-risk contents identified are considered medium sensitive but highly exposed. The screenshot below shows an example of these high-risk contents. The objects in the screenshot have a medium sensitivity level with high exposure (shared as anonymous link).



Name	Shared By	Shared With	Inherit From	Permission	Created	Site Name	Expiration Date	Block Download	Sensitivity Level
404 LIC Gala Invoice.pdf	Jason Spessard	Anonymous Link	Unique	Edit	7/7/2022 18:16:37	Jason Spessard	10/5/2022	No	Medium
402 Fechner WEAR & Gala Invoice.pdf	Jason Spessard	Anonymous Link	Unique	Edit	4/19/2022 14:22:19	Jason Spessard	7/18/2022	No	Medium
Invoice_INV_22_APR_002506.pdf	Jon Mallett	Anonymous Link	Unique	Edit	4/14/2022 16:22:37	Jon Mallett	7/13/2022	No	Medium
Possible-list-no-email.xlsx	Emily Ware	Anonymous Link	Unique	Edit	4/8/2022 08:45:39	Emily Ware	7/7/2022	No	Medium
INV_21_NOV_002182.pdf	Jon Mallett	Anonymous Link	Unique	Edit	11/30/2021 15:53:46	Jon Mallett	2/28/2022	No	Medium
ARVO Deposit 11-23-21 \$255.pdf	Clarissa Portillo	Anonymous Link	Unique	Edit	11/24/2021 09:46:50	Clarissa Portillo	2/22/2022	No	Medium
Aptara - Bank Wire Details New Address (BOA) (1).pdf	Robert Canas	Anonymous Link	Unique	Edit	10/21/2021 15:18:32	Robert Canas	1/19/2022	No	Medium
Sunday Posters Session 2.xlsx	Tim Maxey	Anonymous Link	Unique	Edit	5/2/2021 10:38:14	Tim Maxey	7/31/2021	No	Medium
JDV reviewers.xls	Jon Mallett	Anonymous Link	Unique	Edit	5/11/2020 15:37:22	Jon Mallett	8/9/2020	No	Medium
2019 Hot Topics List Prior to Sessioning - final list.xlsx	Julene Joy	Anonymous Link	Unique	Edit	2/15/2019 09:30:22	Julene Joy	5/16/2019	No	Medium
Copy of 2019 Hot Topics List Prior to Sessioning - J.xlsx	Julene Joy	Anonymous Link	Unique	Edit	2/4/2019 22:16:40	Julene Joy	5/5/2019	No	Medium
TG applicant abstracts that changed categories 2019.xlsx	Kathy Cox	Anonymous Link	Unique	Edit	1/11/2019 09:44:20	Kathy Cox	4/11/2019	No	Medium

Below are recommendations on how to mitigate the risks with these contents.

- Identify the business owners of these contents and discuss the business need for these contents with the business owners
- Implement a regular process for the business owners to review the high and medium-risk objects in their workspace – assessing the necessity of the sensitive contents, whether the business contents can be redacted, and review who has access to the contents and whether access can be trimmed. Cloud Governance renewal feature can be used to automate and enforce this review process.

## ***Empowering Technology. Powered by People.***

### **Sensitive Contents**

There are 5,760 items considered sensitive (low, medium or high) in the M365 environment. 3,580 of the high and medium risk contents are considered high risk (as identified and discussed in the previous section), the rest of these sensitive items are considered medium or low risk because these contents are assessed to have low exposure.

Working with sensitive information is unavoidable and is oftentimes a necessary part of doing business. It is not realistic to ask business users to stop storing sensitive information in M365. Organizations that have done so end up finding their business users storing and sharing this sensitive information some other ways – oftentimes in less secure fashion.

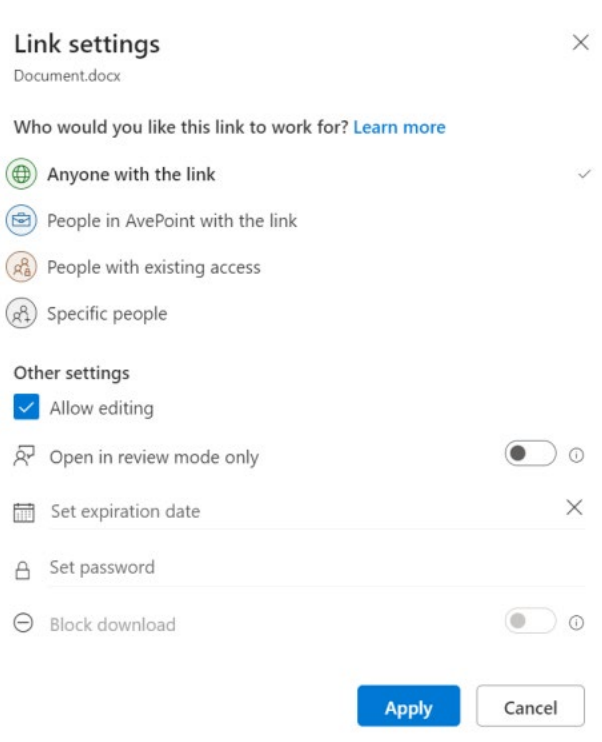
Below are recommendations on how to mitigate the risks with these sensitive contents.

- Recognize the need for users to work with sensitive information and develop a guideline in how business users should do so safely
- Leverage native M365 DLP capability to control access to sensitive contents
- Use tools like Insights to monitor that business users are following these guidelines and use Insights to apply sensitivity labels which can be used to trigger DLP controls
- Implement a regular process for the business owners to review the sensitive contents in their workspace – assessing the necessity of the sensitive contents, whether the business contents can be redacted, and review who has access to the contents and whether access can be trimmed. Cloud Governance renewal feature can be used to automate and enforce this review process.

### **External Links**

There are a total of 732 items in the M365 environment that is directly shared with a user outside of the organization via a direct shared link or via an anonymous link. This is normally done by an end user via the “Share” button in a Microsoft Office application (see screenshot below). Direct shared link still requires the external user to create and authenticate via a Microsoft account whereas anonymous link provides access to the content to anyone inside and outside the organization with just the URL link (no authentication required).

**Empowering Technology. Powered by People.**



It is best practice that anonymous sharing be disabled at the tenant level. If there is a business need for anonymous sharing, it is recommended that any anonymous link be set to expire automatically after a period of time, and the anonymous link only be enabled for specific SharePoint sites. Refer to screenshots below.

**Choose expiration and permissions options for Anyone links.**

These links must expire within this many days

These links can give these permissions:

Files:

Folders:

Below are additional recommendations on how to mitigate the risks with anonymous links.



## *Empowering Technology. Powered by People.*

- Disable anonymous links in OneDrive for Business and enable it only for specific SharePoint Sites. Cloud Governance can enable/disable anonymous links for requested SharePoint Sites. Policies can monitor SharePoint sites regardless of whether it's provisioned through Cloud Governance or via native M365 to ensure that anonymous link are disabled.
- Use tools like Insights to monitor where anonymous links exists and use the tool to remove the link or set expiration for the link
- Review the SharePoint Sites where anonymous links are enabled on a more frequent basis (compared to regular SharePoint Sites) by the business owner and by the administrator or security team. Cloud Governance renewal feature can be used to automate and enforce this review process.
- Implement an automated process that identify when sites with anonymous links enabled are inactive for a period of time (i.e. 30 days). Have an automated decommissioning process defined when these sites become inactive. Cloud Governance have these automated processes built in.
- Implement a regular process for the business owners to review any anonymous links in their workspace. Cloud Governance renewal feature can be used to automate and enforce this review process.

External direct shared link is more secure alternative to anonymous links. However, ungoverned external direct sharing can become a huge risk over time as it is not practical to monitor these activities at the content level.

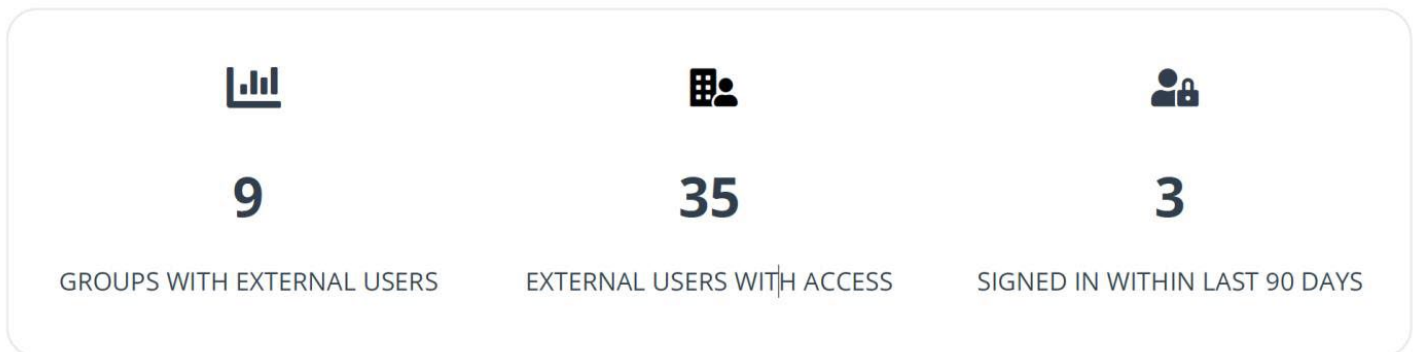
Below are additional recommendations on how to mitigate the risks with external direct shared links.

- Enable external direct shared links only for specific SharePoint Sites. Cloud Governance can enable/disable external direct shared links for requested SharePoint Sites. Policies can monitor SharePoint sites regardless of whether it's provisioned through Cloud Governance or via native M365 to ensure that external direct shared links are disabled.
- Use tools like Insights to monitor where external links exists and use the tool to remove the link
- Implement a policy that requires the business user to invite the external user to the workspace as opposed to sharing specific contents for the more sensitive workspaces. It's hard for business users to identify, manage and keep track of explicitly shared contents over time. Policies can help enforce this rule.
- Implement a regular process for the business owners to review any external direct shared links in their workspace. Cloud Governance renewal feature can be used to automate and enforce this review process.

## Empowering Technology. Powered by People.

### External Users

There are currently a total of 44 external users in your Azure Active Directory, 35 of these users currently have access to some information in your M365 environment. There are 9 M365 groups with external users as members. Only 3 of these external users have signed in the past 90 days.



One of the more popular features with M365 is the ability for business users to easily collaborate with external partners and vendors. At the same time, external users accessing their M365 environment is one of the biggest security concerns for organizations. Collaborating with external partners and vendors are a normal part of doing business. Shutting down the ability to collaborate with external users in M365 pushes your business users to collaborate in some other, potentially less secure, fashion such as email or shadow IT system (like personal Dropbox).

Below are recommendations on how to mitigate the risks with allowing external guest users in your M365 environment.

- Use tools like Insights to monitor external users and use the tool to remove the users if needed
- Enable guest users only in specific workspaces. Cloud Governance can enable/disable guest users for requested SharePoint Sites. Policies can monitor SharePoint sites regardless of whether it's provisioned through Cloud Governance or via native M365 to ensure that the ability to add guest users are disabled.
- Implement lifecycle management for these workspaces where the business owners of the workspaces review if the guest users still need access to their workspace. Cloud Governance workspace renewal feature can be used to automate and enforce this review process.
- Identify a sponsor for each of the guest users and implement a regular process for the sponsor to review the workspaces the guest users have access to. Cloud Governance service request process can ensure that a business sponsor is assigned for every guest user. Cloud Governance guest renewal feature can be used to automate and enforce this review process.

**Empowering Technology. Powered by People.**

- Identify “ghost” and inactive guest users (ghost guest users are guests who are in the tenant but do not belong to any workspaces) and have a process that removes these users from the tenant. Policies can automate the process of identifying these guest users and removing them from Azure AD.
- Further reduce risk by whitelisting specific external domains for each workspace that has guest access. Policies can enforce a rule that business users can only invite guests from a specific domain in specific workspaces.

**Top Sensitive Information Types**

The following is a list of the top 5 Sensitive Information Types identified by MSFT’s compliance scan. Note that not all these Sensitive Information Types are used to classify contents in Insights as sensitive (refer to the Configuration and Definition: Sensitivity Level section for sensitivity definition). It is recommended that business reviews this list on a regular basis using a tool like Insights to identify newly found Sensitive Information Types that may need to be added to the definition of sensitivity.

Top 5 Sensitive Info Types	
NAME	SENSITIVE ITEMS
ABA Routing Number	4.19K
U.S. Bank Account Number	716
Drug Enforcement Agency (DEA) Number	538
U.S. Individual Taxpayer Identification Number (ITIN)	321
U.S. Driver's License Number	282

**Top Sensitivity Labels**

Sensitivity Labels are not being used in [Sample Company]’s tenant.

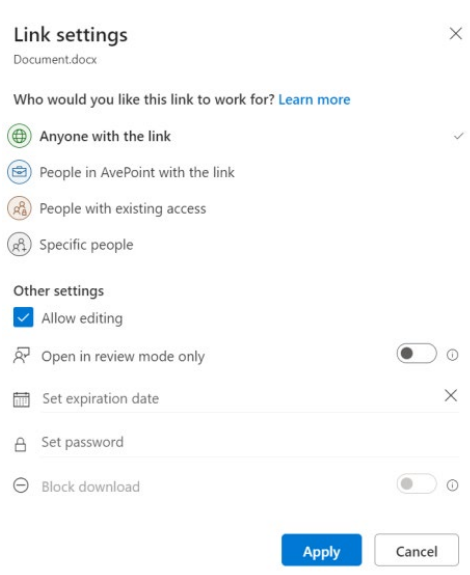
**Empowering Technology. Powered by People.**

**Direct Sharing Links to Sensitive Contents**

This section of the report shows the number of sensitive objects (low, medium, or high) that is directly shared (item/document level permission). The count is broken down by the type of direct sharing. Note that there is an overlap between this metric and the External Links metric. The objects counted for the direct share type of “Anonymous Link” and “Link for Specific External Users” are a subset of the External Links metric (it’s the subset of External Links that are sensitive).

<b>Direct Access Sharing</b>	
<b>SHARED WITH</b>	<b>SENSITIVE ITEMS</b>
Everyone	0
Everyone except External Users	3.51K
External Users	0
Anonymous Link	8
Link for Specific External Users	0
Organization Link	531

As with External Links, Direct Sharing Links is normally done by an end user via the “Share” button in a Microsoft Office application (see screenshot below). Direct Sharing can also be achieved the traditional way of creating unique SharePoint permission for the specific document. Doing the aforementioned direct sharing via the “Share” button results in the same unique document level permission. It used to be that only business users that has enough SharePoint technical skills know how to create these unique document level permissions. However, Microsoft’s introduction of the “Share” button has made this more rampant.



Link settings ×  
Document.docx

Who would you like this link to work for? [Learn more](#)

- Anyone with the link ✓
- People in AvePoint with the link
- People with existing access
- Specific people

Other settings

- Allow editing
- Open in review mode only
- Set expiration date ×
- Set password
- Block download

The security risks and concerns with directly shared contents is similar to external direct shared links – namely the sprawl and proliferation of contents with unique permissions. Not only is it not practical to monitor all these risks at the content level as the number of contents with unique permissions grows, it’s also almost impossible to meet chain of custody compliance requirements that comes with some of the regulated sensitive contents.

To mitigate the risks associated with directly shared sensitive contents, [Sample Company] recommends:

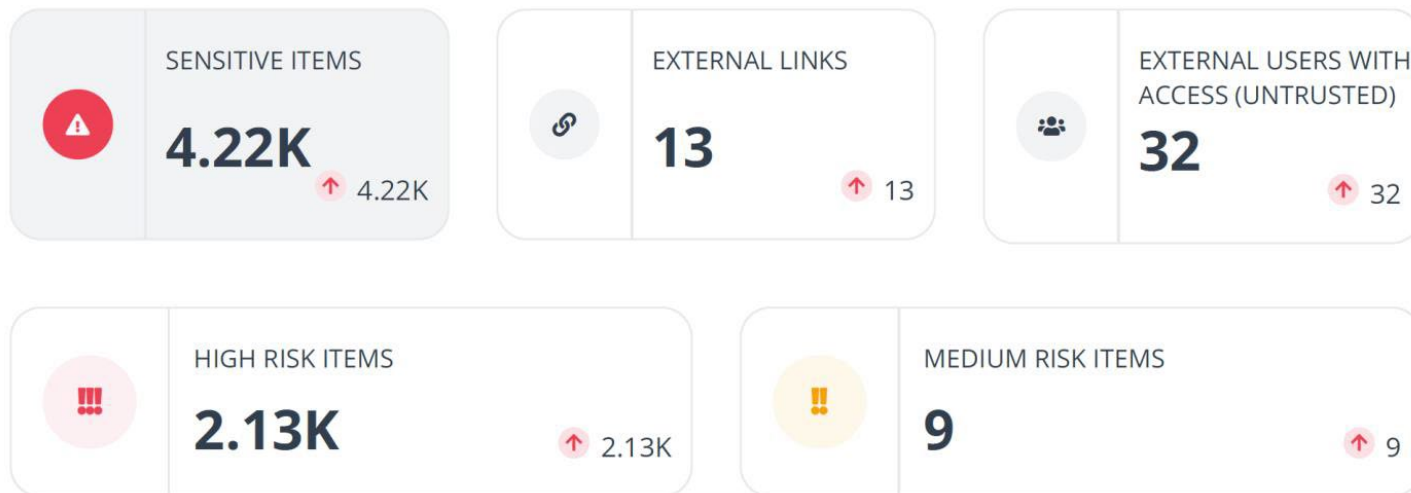
- Implement a regular process for workspace owners to review contents in their workspace that have unique permissions. Cloud Governance renewal feature can be used to automate and enforce this review process.
- Use a tool like Insights on a regular basis to identify sensitive contents that are directly shared and work with the business owners to validate business necessity. Insights can also be used to remove the link or set expiration for the link.
- Identify workspaces that are expected to contain highly sensitive or regulated contents and use a tool like [Sample Company] Policies to disable the ability to directly share contents and set unique document level permission



**Empowering Technology. Powered by People.**

**Microsoft Teams**

There are 4,220 sensitive items, 2,130 high risk items and 9 medium risk items in the Teams. There are a total of 32 external users spread out over 8 Teams. There are 32 contents in Teams that are directly shared with an external user.



**Risk Summary**

TYPE	COUNT
Total Teams	Public <b>20</b> Private <b>12</b> <b>32</b>
Teams with Guest Users Guest users may unintentionally have access to confidential data distributed by your users.	<b>8</b>
Teams with Shadow Users/Groups Shadow users may have access to your Teams data through direct sharing links without actually having been added to the membership of Team channels.	<b>12</b>
Teams with High Risk Items The Teams that contain both sensitive information and out of policy exposure levels per defined policies.	<b>10</b>
Teams without Available Owners Teams with no designated owners or no available owners may allow any user to have unchecked access to view or distribute sensitive data.	<b>0</b>
Teams with Private Channels Teams that have private channels.	<b>6</b>

## ***Empowering Technology. Powered by People.***

### **Teams with Shadow Users/Groups**

There are 12 Teams with shadow users/groups. Shadow users and groups occurs when one of the Team owners manually gives specific users and/or groups access to the SharePoint team site connected to the Team. Shadow users/groups can become problematic as access to the Team's contents (stored in the connected SharePoint Team Site) is not defined anymore by membership to the Team. This can result in confusion by the business users, and the potential for inadvertent data leak.

To mitigate the risks associated with shadow users/groups, [Sample Company] recommends:

- Implement a regular process for workspace owners to review the security configuration in their workspace. Cloud Governance renewal feature can be used to automate and enforce this review process.
- Use a tool like Policies to detect and remove shadow users/groups ensuring that access to the connected SharePoint site is always defined by the Team membership

### **Teams without Available Owners**

There are no Teams without available owners. When a team has no active owner, it is considered as an orphaned team or ownerless team. Orphaned teams are created in the following scenarios.

- When the only/last team owner left the organization
- When the team owners' sign-in blocked in Microsoft 365

### **Teams with Private Channels**

There are 6 Teams with private channels in the environment. Private channels are a very useful feature by providing the ability to create a channel with a more restricted membership (only a subset of the Team member can access that particular channel and the contents in the private channel). However, private channels provide additional complexity that can introduce risk and make governance harder because of the following reasons:

- The Team Owner may not be a member of the private channel and are not able to provide the necessary oversight to the private channel
- Each private channel spins up its own SharePoint Team Site. Each additional team site is another opportunity for business users to introduce complexity (i.e. shadow users/groups) and another container for the admins to monitor

## Empowering Technology. Powered by People.

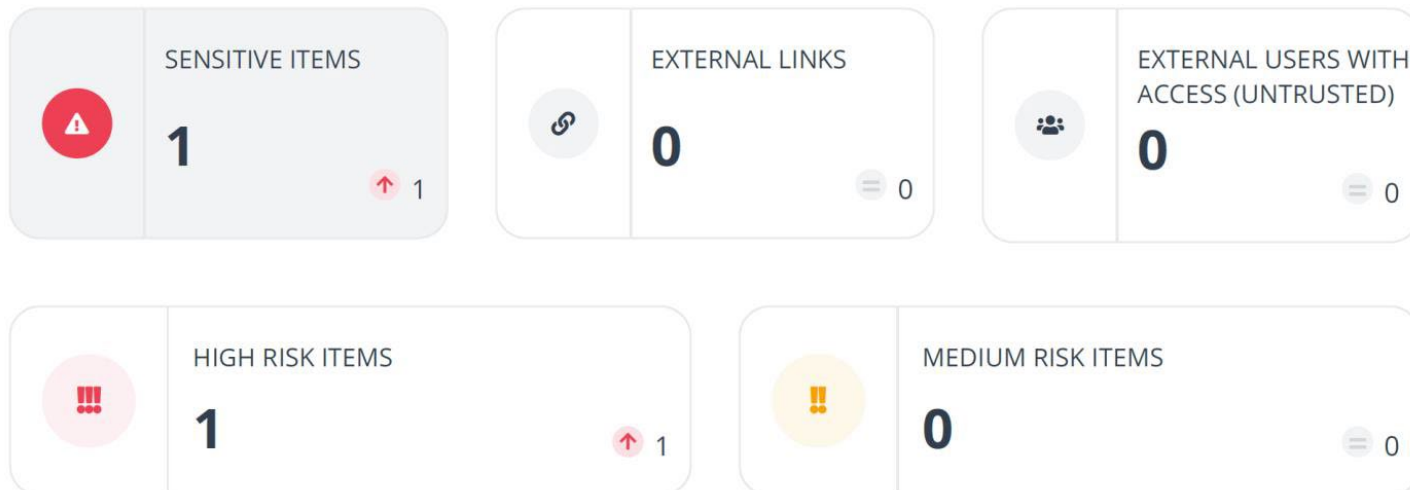
Proliferation of private channels results in the same governance headache that proliferation of directly shared contents does and increases the risk in the environment.

To mitigate the risks associated with Teams with Private Channels, [Sample Company] recommends:

- Use a governance and provisioning tool like Cloud Governance to disable, restrict and/or control the ability to create private channels
- Implement a regular process for workspace owners to work with private channel owners in reviewing the private channels in their workspace. Cloud Governance renewal feature can be used to automate and enforce this review process.

### SharePoint Online

There is 1 sensitive item and 1 high/medium risk items in the SharePoint Online environment. There are no external users and no content in SharePoint that is directly shared with an external user.



**Empowering Technology. Powered by People.**

**Risk Summary for SharePoint Online**

TYPE	COUNT
Total Site Collections	5
Site Collections Shared with External Users Guest users may unintentionally have access to confidential data distributed by your users.	0
Site Collections with High Risk Items The site collections that contain both sensitive information and out of policy exposure levels per defined policies.	0

**With Unique Permissions**

TYPE	QUANTITY
Site	1
Library/List	0
Folder	0

There is 1 subsite that has unique permissions. By default, any container created within or below a site (subsites, lists, libraries, or folders within a library) inherits the permissions of the parent container. However, SharePoint allows the ability to break the inheritance and configure a unique permission to the specific container.

There are valid business reasons for breaking inheritance. However, it is best practice to avoid unnecessarily breaking permission inheritance and to keep unique permissions at a minimum as proliferation of unique permissions increases the complexity of the security structure. The security risks and concerns with unique permissions are similar to external direct shared links. It becomes quickly unfeasible for a workspace owner to keep track of the security of a workspace if there are numerous objects within the workspace with unique permissions – thus increasing the risk of unintended data leak.

To mitigate the risks associated with unique permissions, [Sample Company] recommends:

- Implement a regular process for workspace owners to their workspaces that have sub containers with unique permissions. Cloud Governance renewal feature can be used to automate and enforce this review process.
- Use a tool like Insights on a regular basis to identify containers with unique permissions and work with the business owners to validate business necessity
- Identify workspaces that are expected to contain highly sensitive or regulated contents and use a tool like [Sample Company] Policies to disable the ability to break permission inheritance to sub containers in the workspace



**Empowering Technology. Powered by People.**

**OneDrive for Business**

There are 30 sensitive items and 2 high/medium risk item in the OneDrive for Business environment. There are 3 external users spread out over 2 OneDrives. There are 719 contents in OneDrive for Business that are directly shared with an external user.

**SENSITIVE ITEMS**

**30**

↑ 30

**EXTERNAL LINKS**

**719**

↑ 719

**EXTERNAL USERS WITH ACCESS (UNTRUSTED)**

**3**

↑ 3

**HIGH RISK ITEMS**

**2**

↑ 2

**MEDIUM RISK ITEMS**

**0**

= 0

**Risk Summary for OneDrive for Business**

TYPE	COUNT
Total OneDrives	<b>58</b>
OneDrives Shared via Anonymous Link Guest users may unintentionally have access to confidential data distributed by your users.	<b>37</b>
OneDrives Shared with External Users Shadow users may have access to your OneDrives' sensitive files through direct sharing links without appearing as a visitor or member.	<b>2</b>

**Built-in Folders with High Exposure**

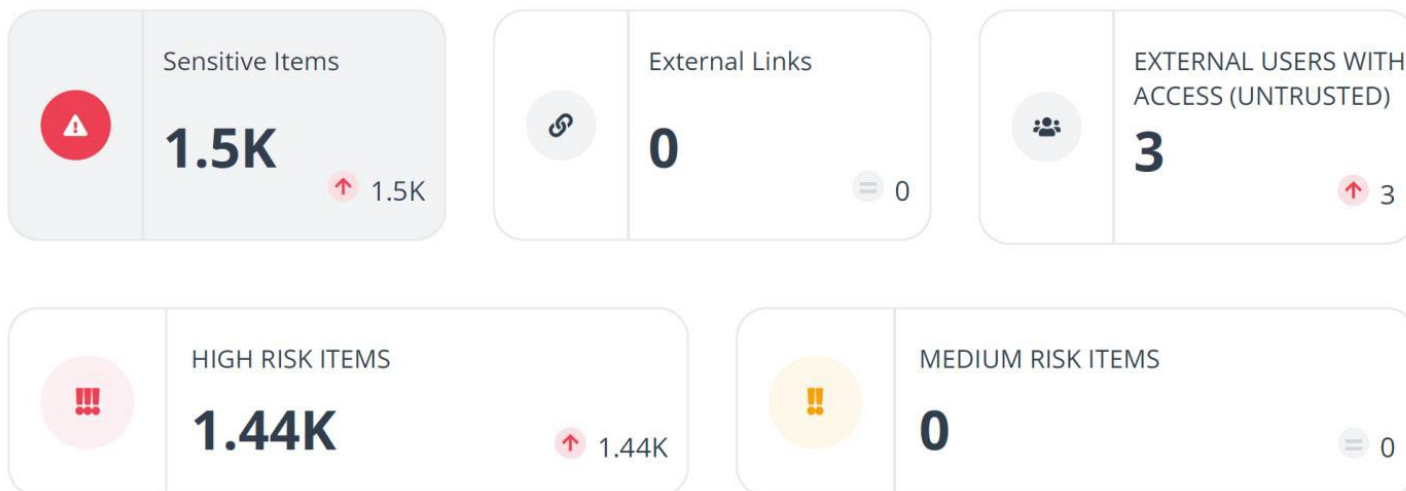
FOLDER TYPE	COUNT
Microsoft Teams Chat Files	0
Attachments	0



**Empowering Technology. Powered by People.**

**Microsoft 365 Group**

There are 1,500 sensitive items and 1,440 high/medium risk items in M365 Group enabled SharePoint Sites. There are 3 external users in 1 M365 Group. There are no contents in M365 Groups that are directly shared with an external user.



**Risk Summary for Microsoft 365 Groups**

TYPE	COUNT
Total Microsoft 365 Groups	Public <b>18</b>   Private <b>7</b>   <b>25</b>
Microsoft 365 Groups with Guest Users Guest users may unintentionally have access to confidential data distributed by your users.	<b>1</b>
Microsoft 365 Groups with Shadow Users/Groups Shadow users may have access to your Groups' sensitive data through direct sharing links without being part of the Microsoft 365 Group membership.	<b>22</b>
Microsoft 365 Groups with High Risk Items The Microsoft 365 Groups that contain both sensitive information and exposure levels beyond the defined policies.	<b>11</b>
Microsoft 365 Groups without Available Owners Microsoft 365 Groups with no designated owners or no available owners may allow any user to have unchecked access to view or distribute sensitive data.	<b>0</b>

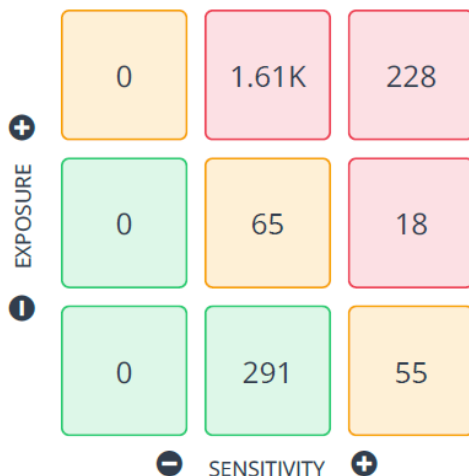
## Risk Summary

Generated Time: 2022/07/20 11:33:29(UTC-10:00)

### What does risk mean for your organization?

The Overall Risk analyzes your organization external risk by looking at guests or the content shared outside against potential sensitive or confidential information as set by your administrator according to rules for Microsoft 365 usage. This helps to prioritize your risk to focus on what is important to your business.

### Overall Risk



*Empowering Technology. Powered by People.*



SENSITIVE ITEMS

**2.25K**

↓ 5 in the last 7 days



EXTERNAL LINKS

**20**

No changes in the last 7 days



EXTERNAL USERS IN AZURE AD  
(UNTRUSTED)

**26**

No changes in the last 7 days



HIGH RISK ITEMS

**1.85K**

↓ 6 in the last 7 days



MEDIUM RISK ITEMS

**105**

No changes in the last 7 days



**42**

GROUPS WITH EXTERNAL USERS



**35**

EXTERNAL USERS WITH ACCESS



**3**

SIGNED IN WITHIN LAST 90 DAYS

*Empowering Technology. Powered by People.*

### Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	64
Everyone except External Users	1.39K
External Users	264
Anonymous Link	3
Link for Specific External Users	0
Organization Link	5

### External Users with Highest Risk

NAME	HIGH RISK OBJECTS
Murugan Balaji	97
antoine.snow	86
Murugan Balaji	68
Stephen Hines	7

### Top 5 Sensitive Info Types

NAME	SENSITIVE ITEMS
Credit Card Number	649
U.S. Social Security Number (SSN)	605
EU Debit Card Number	335
Coffee	310
Telephone Number	283


### Top 5 Sensitivity Labels

NAME	FILES
Restricted	25
Confidential	11
Internal	5
Client Data	4
Sensitive	3

## Microsoft Teams




↓ ↑ denote changes over the last 7 days  
 Generated Time: 2022/07/20 11:33:29(UTC-10:00)



SENSITIVE ITEMS

327


↓ 1



EXTERNAL LINKS

4


= 0



EXTERNAL USERS WITH ACCESS (UNTRUSTED)

28


= 0



HIGH RISK ITEMS

247

↓ 1



MEDIUM RISK ITEMS

33

= 0

### Risk Summary

TYPE	COUNT
Total Teams	<div style="display: flex; justify-content: space-around; border: 1px solid #ccc; border-radius: 5px; padding: 5px;"> <span>Public 93</span> <span>Private 507</span> </div> <b>600</b>
Teams with Guest Users <small>Guest users may unintentionally have access to confidential data distributed by your users.</small>	<b>36</b>
Teams with Shadow Users/Groups <small>Shadow users may have access to your Teams data through direct sharing links without actually having been added to the membership of Team channels.</small>	<b>178</b>
Teams with High Risk Items <small>The Teams that contain both sensitive information and out of policy exposure levels per defined policies.</small>	<b>49</b>
Teams without Available Owners <small>Teams with no designated owners or no available owners may allow any user to have unchecked access to view or distribute sensitive data.</small>	<b>0</b>
Teams with Private Channels <small>Teams that have private channels.</small>	<b>53</b>



### Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except External Users	204
External Users	147
Anonymous Link	0
Link for Specific External Users	0
Organization Link	3

### Teams with Highest Risk

NAME	HIGH RISK OBJECTS
2019 Marketing Wei Office	28
2022MarketingWeiOffice	28
MarketA	11

High risk Teams contain sensitive information and have exposure levels that are beyond the defined policies.

### Top 5 Sensitive Info Types

NAME	SENSITIVE ITEMS
Credit Card Number	141
U.S. Social Security Number (SSN)	82
EU Debit Card Number	63
Salary Information	54
EU Tax Identification Number (TIN)	37




### Top 5 Sensitivity Labels



NAME	FILES
Restricted	13
Confidential	5
Sensitive	2
Public	2
Internal	1

### Team Site Sensitivity Labels

LABEL NAME	TEAM SITES
Internal	4
Confidential	1
Restricted	1
Sensitive	1
None	593

## SharePoint Online

   denote changes over the last 7 days  
Generated Time: 2022/07/20 11:33:29(UTC-10:00)

 SENSITIVE ITEMS  
**1.43K**  4

 EXTERNAL LINKS  
**1**  0

 EXTERNAL USERS WITH ACCESS (UNTRUSTED)  
**2**  0

 HIGH RISK ITEMS  
**1.18K**  5

 MEDIUM RISK ITEMS  
**60**  0

### Risk Summary for SharePoint Online

TYPE	COUNT
Total Site Collections	158
Site Collections Shared with External Users Guest users may unintentionally have access to confidential data distributed by your users.	2
Site Collections with High Risk Items The site collections that contain both sensitive information and out of policy exposure levels per defined policies.	24

### With Unique Permissions

TYPE	QUANTITY
Site	38
Library/List	40
Folder	37

### Direct Access Sharing

SHARED WITH	SENSITIVE ITEMS
Everyone	64
Everyone except External Users	1.04K
External Users	3
Anonymous Link	0
Link for Specific External Users	0
Organization Link	1

### Site Collections with Highest Risk

NAME	HIGH RISK OBJECTS
AvePoint, Inc Team Site	337
Intranet 2016	204
AvePoint, Inc Team Site	147

### Top 5 Sensitive Info Types

NAME	SENSITIVE ITEMS
U.S. Social Security Number (SSN)	393
Credit Card Number	350
Coffee	262
EU Debit Card Number	187
Telephone Number	168

### Top 5 Sensitivity Labels



NAME	FILES
Restricted	7
Internal	4
Confidential	2
Client Data	2

### Site Collection Sensitivity Labels


LABEL NAME	TEAM SITES
Internal	4
Public	2
None	115

## OneDrive for Business





 denote changes over the last 7 days  
 Generated Time: 2022/07/20 11:33:29(UTC-10:00)


**SENSITIVE ITEMS**

 **436** = 0

**EXTERNAL LINKS**

 **15** = 0


**EXTERNAL USERS WITH ACCESS (UNTRUSTED)**

 **3** = 0

**HIGH RISK ITEMS**

 **375** = 0

**MEDIUM RISK ITEMS**

 **7** = 0

### Risk Summary for OneDrive for Business

TYPE	COUNT
Total OneDrives	47
OneDrives Shared via Anonymous Link Guest users may unintentionally have access to confidential data distributed by your users.	5
OneDrives Shared with External Users Shadow users may have access to your OneDrives' sensitive files through direct sharing links without appearing as a visitor or member.	6

### Built-in Folders with High Exposure

FOLDER TYPE	COUNT
Microsoft Teams Chat Files	2
Attachments	7



**Empowering Technology. Powered by People.**

**Direct Access Sharing**

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except External Users	108
External Users	93
Anonymous Link	3
Link for Specific External Users	0
Organization Link	1

**OneDrives with Highest Risk**

NAME	HIGH RISK OBJECTS
Eric Krusi	74
Ray Hill	65
Murugan Balaji	50

High risk OneDrives contain sensitive information and have exposure levels that are beyond defined policies.

**Top 5 Sensitive Info Types**

NAME	SENSITIVE ITEMS
Credit Card Number	137
U.S. Social Security Number (SSN)	110
Telephone Number	88
EU Debit Card Number	74
EU Tax Identification Number (TIN)	57

**Top 5 Sensitivity Labels**

NAME	FILES
Client Data	1



## Microsoft 365 Group



↓ ↑ denote changes over the last 7 days  
 Generated Time: 2022/07/20 11:33:29(UTC-10:00)

Sensitive Items

57

= 0

External Links

0

= 0

EXTERNAL USERS WITH ACCESS (UNTRUSTED)

1

= 0

HIGH RISK ITEMS

52

= 0

MEDIUM RISK ITEMS

5

= 0

### Risk Summary for Microsoft 365 Groups

TYPE	COUNT
Total Microsoft 365 Groups <div style="float: right; border: 1px solid #ccc; padding: 2px;">             Public <b>26</b>    Private <b>40</b> </div>	<b>66</b>
Microsoft 365 Groups with Guest Users <small>Guest users may unintentionally have access to confidential data distributed by your users.</small>	<b>2</b>
Microsoft 365 Groups with Shadow Users/Groups <small>Shadow users may have access to your Groups' sensitive data through direct sharing links without being part of the Microsoft 365 Group membership.</small>	<b>45</b>
Microsoft 365 Groups with High Risk Items <small>The Microsoft 365 Groups that contain both sensitive information and exposure levels beyond the defined policies.</small>	<b>9</b>
Microsoft 365 Groups without Available Owners <small>Microsoft 365 Groups with no designated owners or no available owners may allow any user to have unchecked access to view or distribute sensitive data.</small>	<b>0</b>

**Empowering Technology. Powered by People.**

**Direct Access Sharing**

SHARED WITH	SENSITIVE ITEMS
Everyone	0
Everyone except External Users	34
External Users	21
Anonymous Link	0
Link for Specific External Users	0
Organization Link	0

**Microsoft 365 Groups with Highest Risk**

NAME	HIGH RISK OBJECTS
Accounting NA	15
Contoso Intranet	14
ATS Collaboration	7

High risk Microsoft 365 Groups contain sensitive information and have exposure levels that are beyond defined policies.

**Top 5 Sensitive Info Types**

NAME	SENSITIVE ITEMS
Credit Card Number	21
U.S. Social Security Number (SSN)	20
EU Debit Card Number	11
EU Tax Identification Number (TIN)	6
IP Address	5

**Top 5 Sensitivity Labels**

NAME	FILES
Restricted	5
Confidential	4
Sensitive	1
Public	1

**Group Team Site Sensitivity Labels**

LABEL NAME	TEAM SITES
None	66