Microsoft Power BI

M365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

V0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Table of Contents

This page is intentionally blank.

1. Introduction

Power BI is a Software as a Service (SaaS) offering from Microsoft that facilitates self-service business intelligence dashboards, reports, datasets, and visualizations. Power BI can connect to multiple different data sources, combine and shape data from those connections, then create reports and dashboards to share with others.

The Power BI service is built on Azure. The Power BI service architecture is based on two clusters: the Web Front End (WFE) cluster and the Back-End cluster. End users neither control nor have visibility into these underlying clusters, as they are part of the underlying SaaS architecture. The WFE cluster manages the initial connection and authentication to the Power BI service, and once authenticated, the Back-End handles all subsequent user interactions. Power BI uses Azure Active Directory (AAD) to store and manage user identities and manages the storage of data and metadata using Azure Binary Large Object (BLOB) and Azure Structured Query Language (SQL) Database, respectively. (For additional detail, please refer to the Power BI Security documentation page.)

1.1 Scope

This baseline focuses on the Power BI SaaS service that comes integrated with Microsoft 365 (M365), noting that there is also a desktop version of Power BI that can be installed locally. Users who are developing business intelligence products and analytics in Power BI desktop can push content to either the Power BI Report Server or to the Power BI SaaS service previously described. If required for a given environment or use case, a separate Power BI desktop baseline with tailored security requirements and considerations should be developed by security and end user operations staff.

1.2 Resources

License Compliance and Copyright

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The United States Government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

1.3 Assumptions

- Agencies using Power BI have a data classification scheme in place for the data entering Power BI.
- Agencies may connect more than one data source to their Power BI tenant.
- All data sources use a secure connection for data transfer to and from the Power BI tenant; the agency disallows non-secure connections.
- The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level. Therefore, only licenses not included in E3/G3 are listed. Additionally, M365 G5 is required for Power BI Pro. Power BI Premium is available as an add-on to G5 and provides dedicated capacity-based BI, self-service data prep for big data, and simplification of data management and access at enterprise scale.

2. Baseline

2.1 External Sharing SHOULD be Disabled

External sharing can represent a potential security risk; therefore, disabling it is a best practice unless specific, approved use cases make it a necessity. As with the other collaboration capabilities within the Power BI tenant, the agency must evaluate whether its use case requires allowing external sharing.

When sharing with users outside an agency, the external users receive an email with a link to the shared report or dashboard. The recipient must sign into Power BI to view the shared content.

After the shared-to user signs into the Power BI service, they see the shared report or dashboard in its own browser window, not in the usual Power BI portal.

People outside the agency can't edit content in the shared report or dashboard. They can interact with the charts and change filters or slicers, but changes are not saved.

Only direct recipients see the shared report or dashboard. For example, if a sharing invite is sent to powerbiuser1@contoso.com, only powerbiuser1 sees the dashboard. No other user can see the dashboard, even if powerbiuser1 forwards them the link. Powerbiuser1 must use the same email address to access it: if powerbiuser1 signs in with any other email address, they will not have access to the dashboard.

People outside the tenant agency cannot see any data if role or row-level security is implemented on on-premises Analysis Services tabular models.

2.1.1 Policy

- External sharing SHOULD be disabled unless the agency mission requires the capability.
- If external sharing is deemed appropriate, the agency SHOULD limit the sharing ability to a security group instead of the entire agency.

2.1.2 Resources

- Power BI Tenant settings | Microsoft Docs

2.1.3 License Requirements

- N/A

2.1.4 Implementation

1. In the **Power BI tenant admin portal**, go to **Export and Sharing Settings.**
2. Disable the **External sharing** toggle.
3. If the agency approves external sharing, select a specific security group that includes users who should be able to share data and reports externally.

2.2 Publish to Web SHOULD be Disabled

Power BI has a capability to publish reports and content to the web. This capability creates a publicly accessible web URL that does not require authentication or status as an AAD user to view it. While this may be needed for a specific use case or collaboration scenario, it is a best practice to keep this setting off by default to prevent unintended and potentially sensitive data exposure.

If it is deemed necessary to make an exception and enable the feature, admins should limit the ability to publish to the web to only specific security groups, instead of allowing the entire agency to publish data to the web.

2.2.1 Policy

- The Publish to Web feature SHOULD be disabled unless the agency mission requires the capability.

2.2.2 Resources

- Power BI Tenant settings | Microsoft Docs
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.2.3 License Requirements

- N/A

2.2.4 Implementation

Confirm Publish to web is disabled

The **Publish to web** setting in the admin portal gives options for users to create embed codes. It is recommended that agencies disallow publishing to the web pending further justification reviews by information security.

1. Administrators can set **Publish to web** to **Disabled.**
2. However, if **Publish to web** is set to **enabled**, admins can **Choose how embed codes work** to **Allow only existing embed codes**. In that case, users can create embed codes, but they must contact the tenant's Power BI admin to allow them to do so.

2.3 Power BI Guest Access SHOULD be Disabled

A best practice is to disallow guest user access. Disallowing guest access also aligns with zero trust principles. The agency with potentially shareable Power BI resources and data in its tenant must evaluate its unique sharing requirements and whether an exception should be granted to allow external guests to access content in the agency's tenant.

Enabling this setting allows AAD Business-to-Business (AAD B2B) guest users to access Power BI. If this setting is disabled, guest users receive an error when trying to access Power BI. Disabling this setting for the entire agency also prevents users from inviting guests to the agency. Using the specific security groups option allows admins to control which guest users can access Power BI.

The types of users are defined as follows (**Note**: These terms vary in use across Microsoft documentation):

- **Internal users**: members of the agency's M365 tenant.
- **External users**: members of a different M365 tenant.

- **Business to Business (B2B) guest users**: external users that are formally invited to view and/or edit Power BI workspace content and are added to the agency's AAD as guest users. These users authenticate with their home organization/tenant and are granted access to Power BI content by virtue of being listed as guest users in the tenant's AAD.

Note: Guest users are subject to restrictions to their experience that are controlled by the AAD administrator. If the Power BI tenant's guest users will need to own and share Power BI content with others and manage workspaces as Power BI workspace Admins, Microsoft recommends changing the **Guest user permissions are limited** setting in AAD to allow these users to use people pickers within the Power BI UX. Since Power BI integrates natively with AAD, the AAD Baseline should be consulted for additional guidance on managing guest users.

2.3.1 Policy

- Guest user access to the Power BI tenant SHOULD be disabled unless the agency mission requires the capability.

2.3.2 Resources

- Power BI Tenant settings | Microsoft Docs
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.3.3 License Requirements

- N/A

2.3.4 Implementation

1. In the **tenant admin portal**, go to **Export and Sharing Settings**.
2. Disable the **Allow Azure Active Directory guest users to access Power BI** toggle.

2.4 External Invitations SHOULD be Disabled

This setting controls whether Power BI allows inviting external users to the agency's organization through Power BI's sharing workflows and experiences. After an external user accepts the invite, they become an AAD B2B guest user in the organization. They will then appear in user pickers throughout the Power BI user experience.

If this setting is disabled:

- Existing guest users in the tenant organization continue to have access to any items they already had access to and continue to be listed in user picker experiences.
- An external user who is not already a guest user in the agency cannot be added to the agency through Power BI.

For maintaining least privilege, a best practice is to disable this setting unless dictated by the mission need.

Note: To invite external users to the tenant, a user also needs the AAD Guest Inviter role. The setting in this baseline statement only controls the ability to invite guest users through Power BI. See the *AAD Minimum Viable Secure Configuration Baseline* for more information on roles.

2.4.1 Policy

- The **Invite external users to your organization** feature SHOULD be disabled unless agency mission requires the capability.

2.4.2 Resources

- Power BI Tenant settings | Microsoft Docs
- Distribute Power BI content to external guest users with AAD B2B | Microsoft Docs
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.4.3 License Requirements

- N/A

2.4.4 Implementation

1. In the tenant admin portal, go to **Export and Sharing Settings**.
2. Disable the **Invite external users to your organization** toggle.

2.5 The External Editing Capability SHOULD be Disabled

It is possible to give external guest users the ability to edit and manage Power BI content; however, this could have considerable data security implications.

Microsoft notes that Power BI comes with this setting disabled.

If there is a mission need to allow external users to edit and manage Power BI content, the recommended best practice is to assign these entities to a security group.

2.5.1 Policy

- The external editing capability SHOULD be disabled unless agency mission requires the capability.

2.5.2 Resources

- Power BI Tenant settings | Microsoft Docs
- Azure AD B2B Guest users can now edit and manage content in Power BI to collaborate better across organizations | Microsoft Docs
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.5.3 License Requirements

If this setting is enabled, an AAD B2B guest user must have a Power BI Pro license in a workspace other than the “My workspace” area to edit and manage content within the inviting organization’s Power BI tenant.

2.5.4 Implementation

1. In the tenant admin portal, go to **Export and Sharing Settings**.
2. Disable the toggle labeled **Allow Azure Active Directory guest users to edit and manage content in the organization**.

2.6 Service Principals SHALL be Allowed to be Used to Securely Manage Application Identities

Power BI supports the use of service principals to manage application identities. Service principals can use application programming interfaces (APIs) to access tenant-level features, which are controlled by Power BI service admins and enabled for the entire agency or for agency security groups. Access of service principals can be controlled by creating dedicated security groups for them and using these groups in any Power BI tenant level-settings. If service principals are employed for Power BI, it is recommended that service principal credentials used for encrypting or accessing Power BI be stored in a Key Vault, with properly assigned access policies and regularly reviewed access permissions.

Several high-level use cases for service principals:

- Power BI interactions with data sources. There will be some cases where a service principal is not possible from Power BI to a data source (e.g., Azure Table Storage).
- A user's service principal for accessing the Power BI Service (e.g., app.powerbi.com, app.powerbigov.us).
- Power BI Embedded and other users of the Power BI REST APIs to interact with PBI content.

Best Practices for Service Principals:

- Evaluate whether certificates or secrets are a more secure option for the implementation. Note that Microsoft recommends certificates over secrets.
- Use the principle of least privilege in implementing service principals; only provide the ability to create app registrations to entities that require it.
- Instead of enabling service principals for the entire agency, implement for a dedicated security group.

2.6.1 Policy

- Service Principals SHOULD be allowed for Power BI where applicable.
- Service Principal credentials used for encrypting or accessing Power BI SHALL NOT be stored in scripts or config files and SHALL be stored in a secure vault such as Azure Key Vault.

2.6.2 Resources

- Automate Premium workspace and dataset tasks with service principal | Microsoft Docs
- Embed Power BI content with service principal and an application secret | Microsoft Docs
- Embed Power BI content with service principal and a certificate | Microsoft Docs
- Enable service principal authentication for read-only admin APIs | Microsoft Docs
- Microsoft Power BI Embedded Developer Code Samples | Microsoft GitHub
- Microsoft Power BI Security Baseline, Baseline Statement IM-2 | Microsoft Docs

2.6.3 License Requirements

- N/A

2.6.4 Implementation

Standardize on a single authoritative identity and access management source (note that AAD integrates natively for Power BI).

1. In the **tenant settings**
   a. Confirm that service principals are enabled in the **Allow service principals to use Power BI APIs** option.
   b. Confirm that the service principal is restricted to a security group related to Power BI, rather than open to the entire agency. (**Note:** Service principals have access to any tenant settings for which they are enabled. Depending on the agency's admin settings, this includes specific security groups or the entire agency.)

To restrict service principal access to specific tenant settings, it is recommended to allow access only to specific security groups. Alternatively, one can create a dedicated security group for service principals and exclude it from the desired tenant settings.

2.7 ResourceKey Authentication SHOULD be Blocked

This setting pertains to the security and development of Power BI embedded content. The Power BI tenant states that "for extra security, block using resource key-based authentication." This baseline statement recommends, but does not mandate, setting ResourceKey-based authentication to the blocked state.

For streaming datasets created using the Power BI service user interface, the dataset owner receives a URL that includes a resource key. This key authorizes the requestor to push data into the dataset without using an AAD OAuth bearer token, so please keep in mind the implications of having a secret key in the URL when working with this type of dataset and method.

This setting applies to streaming and PUSH datasets. If Resource Key-based authentication is blocked, users will not be allowed to send data to streaming and PUSH datasets using the API with a resource key. However, if developers have an approved need to leverage this feature, an exception to the policy can be investigated.

2.7.1 Policy

- ResourceKey Authentication SHOULD be blocked unless a specific use case (e.g., streaming and/or PUSH datasets) merits its use.

2.7.2 Resources

- Power BI Tenant settings | Microsoft Docs
- Real-time streaming in Power BI | Microsoft Docs

2.7.3 License Requirements

- N/A

2.7.4 Implementation

1. Under **Developer Settings** in the Power BI tenant admin portal, toggle **Block ResourceKey Authentication** to an enabled state.

2.8 Python and R Visual Sharing SHOULD be Disabled

Power BI can interact with Python and R scripts to integrate visualizations from these languages. Python visuals are created from Python scripts, which could contain code with security or privacy risks. When attempting to view or interact with a Python visual for the first time, a user is presented with a security warning message. Python and R visuals should only be enabled if the author and source are trusted, or after a code review of the Python/R script(s) in question is conducted and deems the scripts free of security risks.

2.8.1 Policy

- R and Python interactions SHOULD be disabled.

2.8.2 Resources

- Power BI Visuals and Python | Microsoft Docs

2.8.3 License Requirements

- N/A

2.8.4 Implementation

1. In the **Power BI tenant**, go to **R and Python Visuals Settings**.
2. Toggle off the **Interact with and share R and Python visuals** option.

2.9 Data Stewards and Power BI Admins SHOULD Discover, Classify, and Label Sensitive Data

There are multiple ways to secure sensitive information, such as warning users, encryption, or blocking attempts to share. Use Microsoft Information Protection sensitivity labels on Power BI reports, dashboards, datasets, and dataflows to guard sensitive content against unauthorized data access and leakage. This can also guard against unwanted aggregation and commingling.

Note: At this baseline's time of writing, data loss prevention (DLP) profiles are in preview status for Power BI. Once released for general availability and government, DLP profiles represent another available tool for securing Power BI datasets. Refer to the *Defender for Office 365 Minimum Viable Secure Configuration Baseline* for more on DLP.

2.9.1 Policy

- Sensitivity labels SHOULD be enabled for Power BI and employed for sensitive data per enterprise data protection policies.

2.9.2 Resources

- Enable sensitivity labels in Power BI | Microsoft Docs
- Data loss prevention policies for Power BI (preview)

- Data Protection in Power BI
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.9.3 License Requirements

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view Microsoft Information Protection sensitivity labels in Power BI. Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See Azure Information Protection pricing for detail.
- Azure Information Protection sensitivity labels need to be migrated to the Microsoft Information Protection Unified Labeling platform to be used in Power BI.
- To be able to apply labels to Power BI content and files, a user must have a Power BI Pro or Premium Per User (PPU) license in addition to one of the previously mentioned Azure Information Protection licenses.
- Before enabling sensitivity labels on the agency's tenant, make sure that sensitivity labels have been defined and published for relevant users and groups. See Create and configure sensitivity labels and their policies for detail.

2.9.4 Implementation

Enable Sensitivity Labels in Power BI:

Sensitivity labels must be enabled on the tenant before they can be used in both the Power BI service and in Desktop. This section describes how to enable them in the tenant settings.

To enable sensitivity labels on the tenant:

1. Navigate to the **Power BI Admin portal**->**Tenant settings** pane-> **Information protection** section.
2. In the **Information Protection** section, perform the following steps:
   a. Open **Allow users to apply sensitivity labels for Power BI content.**

   b. Enable the toggle.

   c. Define who can apply and change sensitivity labels in Power BI assets. By default, everyone in the agency will be able to apply sensitivity labels; however, one can choose to enable setting sensitivity labels only for specific users or security groups. With either the entire agency or specific security groups selected, one can exclude specific subsets of users or security groups.
      i. When sensitivity labels are enabled for the entire agency, exceptions are typically security groups.

      ii. When sensitivity labels are enabled only for specific users or security groups, exceptions are typically specific users.

   This approach makes it possible to prevent certain users from applying sensitivity labels in Power BI, even if they belong to a group that has permissions to do so.
3. Click **Apply**.

2.10 Audit Logs SHALL be Enabled in Power BI Tenant

The Power BI tenant has a setting for audit log generation to monitor internal activity and compliance. Users within the agency can use auditing to monitor actions taken in Power BI by other users in the agency. Power BI audit logs are always available for tenants that have enabled recording user and admin activity in the Office 365 Admin Portal, in which case this setting appears enabled but greyed out in the tenant settings.

2.10.1 Policy

- Power BI audit log generation SHALL be enabled in the Power BI tenant.

2.10.2 Resources

- Power BI Tenant settings | Microsoft Docs
- National Cybersecurity Protection System-Cloud Interface Reference Architecture Volume 1
- National Cybersecurity Protection System - Cloud Interface Reference Architecture Volume 2
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.10.3 License Requirements

- N/A

2.10.4 Implementation

1. In the **Power BI tenant**, go to **Audit and Usage Settings.**
2. Enable **Create audit logs for internal activity auditing and compliance.** This setting may already be enabled and greyed out if audit recording has been turned on in the M365 admin portal.

3. Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership

Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors

Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors

Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).

Appendix A. Implementation Considerations

A.1 Information Protection Considerations

Several best practices and approaches are available to protect sensitive data in Power BI.

- Leverage sensitivity labels via Microsoft Information Protection.
- Power BI allows service users to bring their own key to protect data at rest.
- Customers have the option to keep data sources on-premises and leverage Direct Query or Live Connect with an on-premises data gateway to minimize data exposure to the cloud service.
- Implement Row Level Security in Power BI datasets.

Implementation Steps:

Apply sensitivity labels from data sources to their data in Power BI

When this setting is enabled, Power BI datasets that connect to sensitivity-labeled data in supported data sources can inherit those labels, so the data remains classified and secure when brought into Power BI. For details about sensitivity label inheritance from data sources, see Sensitivity label inheritance from data sources (preview).

To enable sensitivity label inheritance from data sources:

1. Navigate to the Power BI tenant settings.
2. Select **Information protection** -> **Apply sensitivity labels from data sources to their data in Power BI (preview).**
3. Enable **Restrict content with protected labels from being shared via link with everyone in your agency**.

When this setting is enabled, users can't generate a sharing link for people in the agency for content with protection settings in the sensitivity label.

Sensitivity labels with protection settings include encryption or content markings. For example, the agency may have a "Highly Confidential" label that includes encryption and applies a "Highly Confidential" watermark to content with this label. Therefore, when this tenant setting is enabled and a report has a sensitivity label with protection settings, then users can't create sharing links for people in the agency.

Information Protection Prerequisites Specific to Power BI

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view Microsoft Information Protection sensitivity labels in Power BI. Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See Azure Information Protection pricing for detail.
- Azure Information Protection sensitivity labels need to be migrated to the Microsoft Information Protection Unified Labeling platform in order for them to be used in Power BI.
- To be able to apply labels to Power BI content and files, a user must have a Power BI Pro or Premium Per User (PPU) license in addition to one of the previously mentioned Azure Information Protection licenses.

- Before enabling sensitivity labels on the agency's tenant, make sure that sensitivity labels have been defined and published for relevant users and groups. See Create and configure sensitivity labels and their policies for detail.

High-Level Steps to Use Bring Your Own Key (BYOK) Feature in Power BI

First, confirm having the latest Power BI Management cmdlet. Install the latest version by running Install-Module -Name MicrosoftPowerBIMgmt. More information about the Power BI cmdlet and its parameters is available in Power BI PowerShell cmdlet module.

Follow steps in Bring Your Own (encryption) Keys for Power BI | Microsoft Docs.

Row Level Security Implementation

Row Level Security (RLS) involves several configuration steps, which should be completed in the following order.

1. Create a report in Microsoft Power BI Desktop.
    a. Import the data.
    b. Confirm the data model between both tables.
    c. Create the report visuals.
2. Create RLS roles in Power BI Desktop by using DAX.
3. Test the roles in Power BI Desktop.
4. Deploy the report to Microsoft Power BI service.
5. Add members to the role in Power BI service.
6. Test the roles in Power BI service.

- ➢ Reference Microsoft Power BI documentation for additional detail on Row Level Security configuration.

Related Resources

- Sensitivity labels in Power BI | Microsoft Docs
- Bring your own encryption keys for Power BI | Microsoft Docs
- What is an on-premises data gateway? | Microsoft Docs
- Row-level security (RLS) with Power BI | Microsoft Docs
- Power BI PowerShell cmdlets and modules references | Microsoft Docs

A.2 *Source Code and Credential Security Considerations*

Exposure of secrets via collaboration spaces is a security concern when using Power BI.

For Power BI embedded applications, it is recommended to implement a source code scanning solution to identify credentials within the code of any app housing embedded Power BI report(s). A source code scanner can also encourage moving discovered credentials to more secure locations, such as Azure Key Vault.

Store encryption keys or service principal credentials used for encrypting or accessing Power BI in a Key Vault, assign proper access policies to the vault and regularly review access permissions.

For regulatory or other compliance reasons, some agencies may need to bring their own keys (BYOK), which is supported by Power BI. By default, Power BI uses Microsoft-managed keys to encrypt the data. In Power BI Premium, users can use their own keys for data at-rest that is imported into a dataset (see Data source and storage considerations for more information).

- For Power BI embedded applications, a best practice is to implement a source code scanning solution to identify credentials within the code of the app housing the embedded Power BI report(s).
- If required under specific regulations, agencies need a strategy for maintaining control and governance of their keys. The bring your own key (BYOK) functionality is one option.

Prerequisites

- Implementers must do their own due diligence in selecting a source code scanner that integrates with their specific environment. Microsoft documentation provides a link to third-party scanners at the Open Web Application Security Project (OWASP). This baseline does not endorse or advise on the selection or use of any specific third-party tool.
- If BYOK is deemed to be a requirement:
    - ➢ Power BI Premium is required for BYOK.
    - ➢ To use BYOK, the Power BI tenant admin must upload data to the Power BI service from a Power BI Desktop (PBIX) file.
    - ➢ RSA keys must be 4096-bit.
    - ➢ Enable BYOK in the tenant.

BYOK Implementation High-Level Steps

Enable BYOK at the tenant level via PowerShell by first introducing the encryption keys created and stored in Azure Key Vault to the Power BI tenant.

Then assign these encryption keys per Premium capacity for encrypting content in the capacity.

To enable bringing the agency's key for Power BI, the high-level configuration steps are as follows:

1. Add the Power BI service as a service principal for the key vault with wrap and unwrap permissions.
2. Create an RSA key with a 4096-bit length (or use an existing key of this type) with wrap and unwrap permissions.
3. To turn on BYOK, Power BI Tenant administrators must use a set of Power BI Admin PowerShell Cmdlets added to the Power BI Admin Cmdlets.

Follow detailed steps from Microsoft.

Related Resources:

- Bring your own encryption keys for Power BI | Microsoft Docs
- Microsoft Source Code Analysis Developer Frequently Asked Questions
- For GitHub, the agency can use the native secret scanning feature to identify credentials or other form of secrets within code at About secret scanning | GitHub docs
- Announcing General Availability of Bring Your Own Key (BYOK) for Power BI Premium

A.3 *File Export and Visual Artifact Considerations*

Exporting data from Power BI to image files and comma-separated value (.csv) file format has data security implications. For example, if row-level security (RLS) features are in use in Power BI, an export to image or .csv could allow a user to inadvertently decouple that setting and expose data to a party who does not have permissions or a need to know that previously secured data. A similar scenario applies for information protection sensitivity labels.

A message regarding this condition is provided in the Power BI tenant settings for the particular types of exports.

In contrast to this, Power BI applies these protection settings (RLS, sensitivity labels) when the report data leaves Power BI via a supported export method, such as export to Excel, PowerPoint, or PDF, download to .pbix, and Save (Desktop). In this case, only authorized users will be able to open protected files.

Copy and Paste Visuals:

Power BI can allow users to copy and paste visuals from Power BI reports as static images into external applications. This could represent a data security risk in some contexts. The agency must evaluate whether this represents risk for its data artifacts and whether to turn this off in the Export and Sharing Settings.

Related Resources:

- Sensitivity labels in Power BI | Microsoft Docs
- Say No to Export Data, Yes to Analyze in Excel
- Power BI Governance – Why you should consider disabling Export to Excel

Implementation settings:

1. In the **Power BI tenant** settings, under **Export and sharing settings**, admins can opt to toggle off both **Export reports as image files** and **Export to .csv**.
2. In the **Power BI tenant** settings, under **Export and sharing settings**, admins can opt to toggle off **Copy and paste visuals**.

A.4 *Establishing Private Network Access Connections Using Azure Private Link*

When connecting to Azure services intended to supply Power BI datasets, agencies should consider connecting their Power BI tenant to an Azure Private Link endpoint and disable public internet access.

In this configuration, Azure Private Link and Azure Networking private endpoints are used to send data traffic privately using Microsoft's backbone network infrastructure. The data travels the Microsoft private network backbone instead of going across the Internet.

Using private endpoints with Power BI ensures that traffic will flow over the Azure backbone to a private endpoint for Azure cloud-based resources.

Within this configuration, there is also the capability to disable public access to Power BI datasets.

High-Level Implementation Steps

Note: It is imperative that the VNET and VM are configured before disabling public internet access.

1. Enable private endpoints for Power BI.
2. Create a Power BI resource in the Azure portal.
3. Create a virtual network.
4. Create a virtual machine (VM).
5. Create a private endpoint.
6. Connect to a VM using Remote Desktop (RDP).
7. Access Power BI privately from the virtual machine.
8. Disable public access for Power BI.

Related Resources:

- Private endpoints for accessing Power BI | Microsoft Docs
- Microsoft Power BI Security Baseline, Baseline Statement NS-3 | Microsoft Docs