Publishing & Sharing Reports in Power BI

Easy Level

Q1. Explain why publishing and sharing reports is considered more important than just building dashboards
in Power BI Desktop.

> Building in Power BI Desktop is for development; it's a solo activity. Publishing is vital because:
Accessibility: It moves the data from a local file (.pbix) to the cloud, allowing stakeholders to access it via web browsers or mobile apps.

Collaboration & Automation: Only in the Service can you set up scheduled refreshes, data alerts, and collaborative dashboards that update automatically for the whole team.

Q2. Define Power BI Service and explain its role in comparison to Power BI Desktop in the reporting lifecycle.

> Power BI Desktop: A free Windows application used to connect to, transform, and model data. It is the "Authoring Tool."

Power BI Service: A cloud-based SaaS **(Software as a Service)**. It is the **"Consumption/Sharing Tool"** where reports are hosted, shared, and monitored.

Q3. What does publishing a report mean in Power BI? List any two outcomes that occur after a report is published.

> Publishing means uploading the .pbix file from my computer to the Power BI cloud.
Two outcomes:
A **Report** is created in the Service for people to view.
A **Dataset** is created, which can be reused to build other reports or set up for scheduled refreshes.

Medium Level

Q4. List and explain the steps involved in publishing a report from Power BI Desktop to Power BI Service in the correct sequence.

> Steps to publish a report:

1. Save the report in Power BI Desktop.
2. Click the Publish button on the Home tab.
3. Sign in with my work or school account if prompted.
4. Select the Workspace where I want the report to live (like 'My Workspace' or a team folder).
5. Wait for the success message and click the link to open it in the browser.

Q5. Differentiate between Report and Dashboard in Power BI based on structure and usage

>

Feature	Report	Dashboard
Pages	Can have many pages of detailed visuals.	Only one single page.
Data	Uses data from a single dataset.	Can pin tiles from many different reports.
Goal	Used for deep-dive analysis and filtering.	Used for a quick, high-level status glance.

Q6. Explain the difference between the following three sharing methods in Power BI Service:
Direct Report Sharing
Workspace Access
Power BI Apps
Also mention one use case for each.

> Direct Report Sharing: Sending a specific report to one person.

- Use Case: Sending a weekly sales update to my manager.

Workspace Access: Giving people a role (like Member) in a folder.

- Use Case: Working with two other analysts to build a project together.

Power BI Apps: Bundling several reports into one package for a large group.

- Use Case: Distributing the company-wide HR portal to all 500 employees.

Q7. Describe the four workspace roles available in Power BI and explain how access control is managed using these roles.

> Access control in Power BI is managed by assigning users specific Workspace Roles. This ensures that people only have the permissions they need to do their jobs, which keeps the data and reports secure.

The four roles are:

Admin: This is the highest level of access. Admins can add or remove users, delete the entire workspace, and update all reports. They are essentially the "owners" of the workspace.

Member: Members are the primary collaborators. They can add, edit, or delete reports and dashboards. They can also share items with others and add other people to the "Member" or "Viewer" roles.

Contributor: This role is for people who need to build and edit reports but cannot share them with others or manage who has access to the workspace. It's perfect for a developer who should focus on the technical work without worrying about permissions.

Viewer: This is the most restricted role. Viewers can see and interact with the reports (like using slicers or filters), but they cannot change the visuals or see the underlying data settings.

How access is managed:

Access is managed by following the "Principle of Least Privilege." For example, if someone only needs to see the data to make decisions, I would give them the Viewer role. If I am working with a teammate to design the report, I'd give them Member or Contributor access so they can actually make changes.

Hard Level

Q8. Why are Power BI Apps considered more secure and scalable than direct sharing? Explain this from a governance and enterprise usage perspective.

> From a governance and enterprise perspective, Apps are the gold standard for distributing content to large groups of end-users.

Decoupling Development from Consumption: Direct sharing often happens within a workspace where "too many cooks in the kitchen" can lead to accidental edits. Apps allow developers to work on a "Draft" in the workspace while users only see the "Published" version.

Granular Access Control: Apps allow you to bundle multiple reports and dashboards into one package with a single set of permissions. This is much easier to audit than checking 50 individual reports for unique sharing permissions.

Scalability: Direct sharing is manual and prone to "permission creep." Apps can be distributed to entire Active Directory (AD) groups, ensuring that as people join or leave the company, their access is handled automatically via IT protocols rather than manual report tweaks.

Read-Only Integrity: Users of an App cannot inadvertently change the underlying dataset or report structure, preserving a "single source of truth."

Q9. Explain Row-Level Security (RLS) in Power BI. How does RLS ensure that different users see different data using the same report?

> Row-Level Security (RLS) is a security feature that restricts data access for given users. Instead of creating different reports for different departments, you create one report that filters its data based on who is viewing it.

How it ensures different users see different data:

DAX Filters: You define "Roles" in Power BI Desktop using DAX (Data Analysis Expressions). For example, a role named "Sales_North" might have a filter: [Region] = "North".

Identity Mapping: Once the report is published to the Service, you map users or security groups to these roles.

Dynamic Filtering: When a user logs in, Power BI identifies their email. If they belong to "Sales_North," the engine silently applies the DAX filter to every query sent to the database. The user only sees rows where the region is North; to them, it's as if the rest of the data doesn't exist.

Q10.Assume an organization shares reports without using Apps, workspace roles, or RLS. Discuss any three risks or issues that may arise related to security, governance, or data misuse, and explain how Power BI best practices help prevent them.

>

Risk/issue	**Detailed Impact**	**Best Practice Prevention**
1. Data Leakage & Privacy Breaches	Without RLS, every user with access to the report can see the entire dataset. This leads to unauthorized viewing of sensitive info like salaries or private client lists.	Row-Level Security (RLS) restricts data at the database level so users only see rows they are permitted to see based on their login.
2. Lack of Version Control (Data Integrity)	If you share directly from a workspace without Apps, users see "live" changes. If a developer is mid-edit, the user might make a business decision based on broken or unfinished data.	Power BI Apps separate the "Dev" environment from the "Prod" environment. Users only see the stable, published version, never the "work-in-progress."
3. Administrative Overload & Human Error	Sharing individual reports to individual emails is not scalable. It’s easy to forget to remove an ex-employee, leading to "permission creep" and security gaps.	Workspace Roles & AD Groups allow you to manage permission at a group level. Using viewer roles ensures consumers can’t accidentally break the report logic.