provide me detail on powerbi as a service architecture review and approval (between on-prem and azure). need the following for power bi service approval - design overview, design rationale/use cases for a financial services company, design benefits, data flow between on-prem data assets and azure databrics/storage accounts/cosmosdb, design scope, required resource types, licenses/pricing/options, concerns/limitations/constraints/considerations

**ChatGPT said:**

Got it ✅ — you’re asking for a **detailed architecture review and approval-style document** for **Power BI Service** in a **financial services company**, especially where data spans **on-premises assets** and **Azure (Databricks, Storage Accounts, Cosmos DB)**.

I’ll structure it like a formal review package you could present for approval:

**Power BI Service Architecture Review (On-Prem & Azure)**

**1. Design Overview**

* **Power BI Service (SaaS)** hosted in Azure, integrated with corporate **Azure AD** for authentication.
* Data sources span:
  + **On-Premises SQL Servers / Data Warehouses**
  + **Azure Databricks (Delta tables)**
  + **Azure Data Lake Storage Gen2 (ADLS)**
  + **Azure Cosmos DB (operational analytics)**
* **Secure Hybrid Connectivity** enabled via **On-premises Data Gateway (Enterprise Mode)**.
* Governance and lineage handled by **Microsoft Purview** (optional but recommended).
* Reports and dashboards published to **Power BI Service Workspaces**, consumed through:
  + Power BI Web portal
  + Power BI Mobile
  + Embedded in applications (Power BI Embedded/Azure AD App).

**2. Design Rationale / Use Cases (Financial Services)**

* **Risk & Compliance Dashboards** → Track exposure, credit risk, liquidity, and compliance thresholds using near real-time data from on-prem SQL and Cosmos DB.
* **Customer Insights** → Combine structured (CRM SQL Server) and semi-structured data (Cosmos DB) with enriched insights from Databricks ML pipelines.
* **Regulatory Reporting** → Automate generation of Basel III/IV, CCAR, and SOX-compliant reports with auditable lineage.
* **Fraud Detection** → Real-time event streams (via Databricks + Cosmos DB) surfaced as Power BI dashboards for fraud investigation teams.
* **Operational KPIs** → Finance, treasury, and branch operations can monitor KPIs via Power BI Service dashboards fed from hybrid data.

**3. Design Benefits**

* **Self-Service Analytics** → Analysts can build their own reports without IT bottlenecks.
* **Scalable** → Cloud-native scaling with Premium/Capacity SKUs.
* **Hybrid Connectivity** → Data stays on-prem if required (DirectQuery via Gateway) while leveraging Azure services.
* **Advanced Analytics Integration** → Native support for Databricks SQL, Delta Lake, and Cosmos DB.
* **Security & Compliance** → Integration with Azure AD, sensitivity labels, row-level security (RLS), data loss prevention (DLP) policies.
* **Cost Flexibility** → Pay-per-user (Pro/PPU) or dedicated capacity (Premium).

**4. Data Flow**

**Step-by-Step Flow Example**:

1. **On-Prem SQL Data Warehouse**
   * Power BI connects via **On-Premises Data Gateway** (DirectQuery/Import).
   * Data refresh scheduled or live queries routed securely to on-prem.
2. **Azure Databricks (Delta Lake)**
   * Curated & aggregated datasets stored in **ADLS Gen2**.
   * Power BI connects using **Azure Databricks SQL Endpoint**.
3. **Azure Storage Accounts (ADLS Gen2)**
   * Data ingested from on-prem sources via **ADF / AzCopy / Event Hub**.
   * Power BI connects via **Power BI Dataflows** or **DirectQuery (Parquet/Delta)**.
4. **Cosmos DB**
   * Exposed through **Synapse Link for Cosmos DB** (near real-time analytics).
   * Power BI connects to Synapse Serverless SQL endpoint for analytics dashboards.
5. **Publishing & Consumption**
   * Reports developed in **Power BI Desktop** → published to **Power BI Service**.
   * Users consume via browser/mobile, respecting security models.

**5. Design Scope**

**In-Scope**

* Hybrid architecture (on-prem + Azure data).
* Secure user access with AAD + Conditional Access.
* Power BI governance, workspace strategy, sensitivity labels.
* DirectQuery, Live Connect, Dataflows, and Scheduled Refresh models.

**Out-of-Scope**

* Third-party BI tools (e.g., Tableau, Qlik).
* Custom application embedding (unless approved later).
* Non-Microsoft authentication providers.

**6. Required Resource Types**

* **Azure Resources**:
  + Azure AD (identity)
  + On-Premises Data Gateway (VM/cluster)
  + Azure Databricks (Premium/SQL Endpoint)
  + Azure Storage Account (ADLS Gen2)
  + Azure Cosmos DB + Synapse Link
  + (Optional) Microsoft Purview for governance
* **Power BI Resources**:
  + Power BI Service (tenant-level)
  + Workspaces (per business unit/project)
  + Dataflows / Datasets
  + Row-Level Security roles

**7. Licenses, Pricing, Options**

* **Power BI Pro** → $10/user/month (needed for sharing content).
* **Power BI Premium per user (PPU)** → $20/user/month (advanced features: AI, large models, Paginated Reports).
* **Power BI Premium Capacity (P SKUs)** → starts ~$4,995/month per dedicated capacity (for enterprise-scale workloads, unlimited distribution, and large datasets).
* **Power BI Embedded (A SKUs)** → for embedding in custom apps, hourly billed in Azure.

**Financial Services Consideration:**

* Regulatory dashboards (e.g., Basel/CCAR) → require **Premium Capacity** for guaranteed performance and compliance.
* Business analysts in Finance Ops → **Pro or PPU** licenses.

**8. Concerns, Limitations, Constraints, Considerations**

* **Data Residency** → Ensure Power BI Service region complies with financial regulations (e.g., US, EU data boundaries).
* **On-Prem Latency** → DirectQuery performance depends on on-prem SQL capacity and gateway throughput.
* **Dataset Size Limits** → Import model limit is 1 GB (Pro) / 400 GB (Premium).
* **Data Gateway High Availability** → Must configure cluster for production.
* **Security & Compliance**:
  + Enforce Conditional Access, MFA, IP restrictions.
  + Enable sensitivity labels (Microsoft Information Protection).
  + Monitor with Microsoft Defender for Cloud Apps.
* **Costs** → Premium required for enterprise-scale; per-user licenses may be more cost-effective for small teams.
* **Change Management** → Business units may resist central governance; need strong CoE (Center of Excellence).
* **Lineage & Governance** → Without Purview, lineage across on-prem + Azure + Power BI is difficult to trace.

✅ This is a **formal review-style summary** you could take into an **architecture review board** for approval.

Would you like me to **draw a reference architecture diagram (data flow between On-Prem, Azure, and Power BI Service)** so you can include it in your approval deck?

**You said:**

yes, with private connectivity over express route private peering

**ChatGPT said:**

Thought for 4 seconds

Power Bi Service Architecture With Express Route Private Peering

**Power BI Service — Architecture Diagram (ExpressRoute Private Peering)**

**Purpose:** Visual + implementation-ready architecture for Power BI Service in a Financial Services environment using **private connectivity** between on-premises and Azure via **ExpressRoute (private peering)**. Includes data flows, security controls, recommended resource placements, and operational considerations.

**1) High-level diagram (Mermaid)**

flowchart LR

subgraph OnPrem[On-Premises Data Center]

A[SQL Data Warehouse]

B[Operational DBs / CRM]

C[Streaming Platform / Kafka/Event Hubs (on-prem)]

GW[Local Router / Edge]

end

subgraph ExpressRoute[ExpressRoute]

ER[ExpressRoute Circuit]

end

subgraph AzureVNet[Azure VNet (Hub)]

ERGW[ExpressRoute Gateway]

NVA[NVA / Firewall]

Jump[Jumpbox / Management]

end

subgraph Platform[Platform VNet(s)]

DV[Databricks Workspace (VNet Injected)]

ADLS[ADLS Gen2 (Storage Account) - Private Endpoint]

COS[Cosmos DB - Private Endpoint]

SYN[Synapse Analytics / SQL Serverless]

KV[Key Vault - Private Endpoint]

PUR[Microsoft Purview]

end

subgraph PowerBI[Power BI Service (SaaS)]

PBI[Power BI Service]

PBI\_PE[Private Link / Private Endpoint (Power BI?) ]

end

subgraph Gateway[On-Prem Data Gateway Cluster]

GW1[Gateway Node 1]

GW2[Gateway Node 2]

end

OnPrem -->|Private peering| ER --> AzureVNet

AzureVNet --> Platform

OnPrem -->|HTTPS (outbound) to Gateway cluster| Gateway

GW1 -->|Outbound over ExpressRoute| ERGW

GW2 -->|Outbound over ExpressRoute| ERGW

DV -->|Reads/Writes| ADLS

DV -->|Aggregates| COS

SYN -->|Query Cosmos / ADLS| COS & ADLS

PBI -->|Publish / Service Outlet| PBI

PBI -->|DirectQuery / Live Connect via Gateway| Gateway

PBI <-->|Optional Private Link for Management Plane| PBI\_PE

KV -->|Secrets for Gateway/Databricks| DV & Gateway

PUR -->|Lineage / Scan| ADLS & Synapse

**Note:** Power BI SaaS is a public SaaS offering. Private connectivity is achieved for data plane traffic using **ExpressRoute** and private endpoints for Azure resources (ADLS, Cosmos DB, Key Vault, Synapse, Databricks VNet). Power BI control plane still interacts with Microsoft public endpoints; consider Conditional Access and Private Link for certain management endpoints where available.

**2) Detailed Data Flow (step-by-step)**

1. **Data ingestion (on-prem → Azure)**
   * On-prem ETL/ELT jobs push data to ADLS Gen2 or to Databricks via ADF / private ExpressRoute link. Traffic is over ExpressRoute private peering to the Azure hub VNet.
   * Streaming events can be forwarded to Event Hubs in Azure (deploy Event Hubs in Azure and forward via private peering or use managed connectors).
2. **Processing & Storage (Azure)**
   * Databricks (VNet-injected) reads raw data from ADLS via Private Endpoint. Processed Delta tables are stored in ADLS.
   * Cosmos DB stores operational / low-latency datasets. Enable **private endpoints** for traffic inside Azure network.
   * Synapse Analytics or Databricks SQL Endpoints expose curated data for Power BI.
3. **Power BI Query / Refresh**
   * For **Live/DirectQuery** against on-prem SQL: Power BI Service routes queries through the **On-Prem Data Gateway cluster**. Gateway outbound connections go over ExpressRoute to reach Azure-hosted resources, or to cloud control plane for authentication and orchestration. Gateway nodes must have network egress to Azure AD and Power BI service endpoints.
   * For datasets in ADLS / Databricks / Synapse: Power BI connects via private connectivity to Azure resources (private endpoints) when supported, or via secured service endpoints and managed identities.
4. **Publishing & Consumption**
   * Developers publish reports from Power BI Desktop (can run from on-prem or Azure VM). Published datasets live in Power BI Service. When a user views a report requiring DirectQuery to on-prem, the gateway executes queries back to the on-prem system and returns results.

**3) Key Design Decisions & Rationale (Financial Services)**

* **ExpressRoute private peering:** ensures low-latency, private, auditable connectivity—meets regulatory requirements for private traffic.
* **VNet-injected Databricks & Private Endpoints:** ensures data never traverses public internet between compute and storage.
* **On-Prem Data Gateway cluster (HA):** supports DirectQuery / Live connections for data that cannot leave on-prem. Clustered gateways provide load balancing and fault tolerance.
* **Key Vault & Managed Identities:** avoid secrets in configs; use Key Vault private endpoints and MSI for Databricks & gateway where possible.
* **Purview for lineage:** recommended for audit/regulatory reporting and data discovery.

**4) Security Controls & Network Considerations**

* **ExpressRoute Circuit** with Microsoft peering disabled for public endpoints; use **private peering** to connect to Azure VNets.
* **Hub-and-spoke VNets:** hub holds ExpressRoute gateway, NVAs (firewalls), and peering to platform VNets (spokes) like Databricks, Analytics, and Prod.
* **Network Security Groups & UDRs:** restrict egress/ingress. Use UDR to route internet-bound traffic through NVAs for inspection.
* **Private Endpoints:** for ADLS, Key Vault, Cosmos DB, Synapse to keep traffic internal.
* **Gateway placement:** gateways remain on-prem but must be able to resolve and reach Power BI and Azure AD endpoints for authentication. Configure firewall to allow outbound to required endpoints.
* **MFA & Conditional Access:** protect Power BI Service access; consider blocking legacy auth and requiring device compliance.

**5) Availability, Scaling, and HA**

* **ExpressRoute:** dual circuits for resilience; partner with carrier for SLA and redundancy.
* **Data Gateway Cluster:** at least 2 nodes in different on-prem hosts; use load balancing and health checks.
* **Databricks:** use High Concurrency clusters and autoscaling; keep notebooks/sql endpoints in dedicated VNet.
* **Power BI Premium:** use capacity for predictable performance of large models and paginated reports.

**6) Operational & Compliance Notes**

* **Audit & Logging:** enable diagnostic logs for Storage, Databricks, Cosmos, and Gateway. Ship logs to a central Log Analytics workspace (over ExpressRoute).
* **Data Residency:** ensure tenant and storage region satisfy regulatory boundaries.
* **Penetration testing & network scans:** coordinate with Microsoft for SaaS interactions.

**7) Implementation Checklist (quick)**

**8) Appendix: Required Azure / Power BI Resources**

* Azure: ExpressRoute, Virtual Network(s), ExpressRoute Gateway, Network Virtual Appliance/Firewall, Azure Databricks (VNet Injected), ADLS Gen2 (Private Endpoint), Cosmos DB (Private Endpoint), Synapse Analytics, Key Vault (Private Endpoint), Log Analytics, Microsoft Purview.
* Power BI: Power BI Service tenant, Power BI Pro / PPU for authors, Power BI Premium Capacity (recommended for enterprise), On-Prem Data Gateway cluster.

If you want, I can also:

* export this to a ready-to-use PowerPoint architecture slide, or
* generate a diagram image (SVG/PNG) from the Mermaid above and attach it to the deck.

Which of those next steps would you like? (I can create the PowerPoint now.)

Done — I created a detailed architecture document on the canvas titled **"Power Bi Service Architecture With Express Route Private Peering"** (you can view it in the panel next to this chat).

It includes:

* A Mermaid diagram of the architecture (on-prem → ExpressRoute private peering → Azure VNets → Power BI Service interactions),
* Step-by-step data flows, security & network controls, HA/scaling guidance, implementation checklist, and required resources.

Next options I can do for you (pick one — I’ll proceed immediately):

1. Export this to a PowerPoint slide deck (ready for an architecture review).
2. Render the Mermaid diagram to an image (PNG/SVG) and attach it.
3. Produce a shorter executive one-page summary for signoff.

Which would you like?

**You said:**

yes

**ChatGPT said:**

Got it 👍 — since you said “yes,” I’ll assume you’d like the **Mermaid architecture diagram rendered as an image (PNG/SVG)** so you can drop it directly into your deck.

Do you want me to generate it as:

* **PNG** (good for PowerPoint/Word), or
* **SVG** (scalable, great for Visio/large prints)?

**You said:**

both png and svg

**ChatGPT said:**

Looks like the environment here doesn’t have the **Mermaid CLI (mmdc)** tool, so I can’t generate the PNG/SVG diagrams directly inside this session.

But you still have two easy options:

1. **Local generation**
   * Install [Mermaid CLI](https://github.com/mermaid-js/mermaid-cli?utm_source=chatgpt.com):
   * npm install -g @mermaid-js/mermaid-cli
   * Save the diagram text to diagram.mmd (I already gave you the code).
   * Run:
   * mmdc -i diagram.mmd -o diagram.svg
   * mmdc -i diagram.mmd -o diagram.png
2. **Online rendering**
   * Paste the Mermaid diagram into Mermaid Live Editor.
   * You can export directly to **SVG** or **PNG**.

👉 Do you want me to package the .mmd file for you here so you can download and run it with either method?

Top of Form

Bottom of Form

ChatGPT can make mistakes. Check important in

Great question 👍. When adopting **Power BI** as part of your **Azure cloud migration** from on-prem, there are several **architectural, connectivity, reporting, and security** considerations that your **Architecture Review Board (ARB)** and **Information Security (InfoSec)** teams will expect to see addressed.

Here’s a structured **list of questions and concerns** with details for your approval package:

**🔹 1. Architecture & Connectivity**

* **How will Power BI connect to migrated Azure data sources?**
  + Direct Query vs Import mode vs Composite models.
  + Will Power BI connect directly to **Azure Synapse, Databricks, Cosmos DB, or ADLS Gen2**, or through an abstraction layer (APIs, views, semantic models)?
* **Do we need a Power BI Gateway?**
  + For hybrid scenarios where some data remains on-prem.
  + Is an **Enterprise Data Gateway** required for scheduled refreshes?
* **Will we use Fabric / Power BI Service or remain on Power BI Report Server (on-prem)?**
  + Implications for licensing, cloud connectivity, and hybrid data access.
* **Network Security & Private Connectivity**
  + Are **Private Endpoints** or **VNET Data Gateways** required for accessing data in Synapse/Databricks/SQL MI?
  + Will traffic traverse the public internet or stay in private Azure backbone?
* **Multi-region Deployment**
  + If reports are used globally, where will datasets be hosted (single region vs multi-region capacity)?

**🔹 2. Data Governance & Security**

* **Authentication & Authorization**
  + Will **Azure AD** be the identity provider for Power BI?
  + Role-Based Access Control (RBAC) integration with AD groups.
  + Row-Level Security (RLS) / Object-Level Security in datasets.
* **Data Residency & Compliance**
  + Where is Power BI tenant hosted (US/EU/Asia)?
  + Does this align with **regulatory requirements (GDPR, SOX, PCI DSS, CCAR, etc.)**?
* **Data Encryption**
  + In transit (TLS 1.2+) and at rest (AES 256).
  + Who manages encryption keys (Microsoft vs Customer-Managed Keys)?
* **Data Loss Prevention (DLP)**
  + Are DLP policies in place for Power BI (e.g., preventing export to Excel, PDF, CSV for sensitive datasets)?
* **Audit & Monitoring**
  + Are **Power BI audit logs integrated with Microsoft Purview / Sentinel / SIEM** for monitoring usage, access patterns, and anomalies?

**🔹 3. Reporting & Performance**

* **Data Modeling Approach**
  + Will you centralize models in **Power BI semantic models** (datasets) or allow self-service users to build their own?
  + Standardized **golden datasets** to prevent data silos.
* **Performance Tuning**
  + Large datasets: use **Aggregations, Incremental Refresh, Synapse/Databricks acceleration**.
  + Network latency concerns for global users.
* **Data Refresh Strategy**
  + Import mode refresh schedules.
  + Real-time dashboards via **Event Hubs, Stream Analytics, or Azure Data Explorer (ADX)**.
* **Content Lifecycle**
  + Dev/Test/Prod separation in Power BI workspaces.
  + Deployment pipelines for controlled promotion.

**🔹 4. Integration & Operations**

* **Integration with Other Azure Services**
  + Power BI with **Azure Purview** for lineage.
  + Power BI with **Azure Monitor / Application Insights** for usage monitoring.
  + Embedding Power BI in **internal apps (PowerApps, Teams, SharePoint, custom portals)**.
* **License & Cost Management**
  + Pro vs Premium Per User vs Premium Capacity.
  + Cost optimization: dataset storage, refresh frequency, caching strategy.
* **Backup & Disaster Recovery**
  + Power BI has limited built-in backup.
  + Will you use **deployment pipelines + version control in Git** for dataset and report definitions?

**🔹 5. Information Security Team Specific Concerns**

* **External Sharing**
  + Will users be allowed to share reports with external partners/vendors?
  + How is external collaboration governed?
* **Access from unmanaged devices**
  + Will Power BI access be restricted to **corporate-managed devices only**?
  + Conditional Access policies (MFA, location-based restrictions).
* **Data Export Controls**
  + Restrict ability to download data from Power BI (CSV/Excel/PDF).
  + Apply **sensitivity labels (MIP)** in Power BI.
* **API Security**
  + If using **Power BI REST APIs**, how are client apps authenticated (Managed Identity vs Service Principal)?

✅ **Summary for your Approval Document**  
Your **Architecture Review** and **InfoSec teams** will want:

* Clear diagram of Power BI ↔ Azure data sources ↔ on-prem data sources.
* Identity & access model (Azure AD + RBAC + RLS).
* Network model (public vs private endpoints, gateway requirements).
* Governance model (Purview lineage, audit logs, DLP).
* Security controls (encryption, compliance, external sharing restrictions).
* Performance & lifecycle strategy (refresh, capacity, deployment pipelines).

Do you want me to **draft a formal checklist template** (Excel/Word-style) you can directly circulate to your architecture and security teams for sign-off?

**You said:**

yes

**ChatGPT said:**

I created a formal **Power BI Adoption – Architecture & Security Review Checklist** document. You can share this directly with your **Architecture** and **InfoSec** teams.

📂 Download the checklist here

Do you want me to also prepare a **visual architecture diagram** (showing Power BI ↔ Azure services ↔ on-prem connectivity) to complement this checklist for your approval package?

**You said:**

yes

**ChatGPT said:**

Here’s the **visual architecture diagram** showing connectivity between On-Prem, Azure data services, and Power BI:

📊 Download the diagram here

Would you like me to **merge the checklist (Word file) and this diagram into a single architecture review pack (PDF)** so you can send one consolidated document to your teams?

**You said:**

show me the checklist again

**ChatGPT said:**

Here’s the **Power BI Adoption – Architecture & Security Review Checklist** content from the Word document I generated earlier:

**✅ Power BI Adoption - Architecture & Security Review Checklist**

**🔹 1. Architecture & Connectivity**

* ☐ Have we defined how Power BI connects to Azure data sources (Direct Query, Import, Composite)?
* ☐ Is a Power BI Gateway required for hybrid connectivity with on-prem data?
* ☐ Are we using Power BI Service, Fabric, or Report Server?
* ☐ Are Private Endpoints or VNET Data Gateways needed for secure data access?
* ☐ Is there a global deployment strategy (single vs multi-region)?

**🔹 2. Data Governance & Security**

* ☐ Is Azure AD integrated for authentication and RBAC?
* ☐ Are Row-Level Security (RLS) and Object-Level Security (OLS) defined?
* ☐ Does the Power BI tenant align with regulatory data residency requirements (GDPR, SOX, PCI DSS, etc.)?
* ☐ Are encryption standards (TLS 1.2+, AES 256) enforced?
* ☐ Are DLP policies in place to restrict export/sharing of sensitive data?
* ☐ Are audit logs integrated with SIEM/Sentinel for monitoring?

**🔹 3. Reporting & Performance**

* ☐ Are data models standardized (golden datasets) to prevent silos?
* ☐ Is performance tuning strategy defined (aggregations, incremental refresh, acceleration)?
* ☐ Is there a defined refresh schedule (daily, hourly, real-time)?
* ☐ Is there a content lifecycle strategy (Dev/Test/Prod separation, deployment pipelines)?

**🔹 4. Integration & Operations**

* ☐ Is Power BI integrated with Purview for lineage?
* ☐ Is usage monitored with Azure Monitor/Application Insights?
* ☐ Are embedding needs defined (Teams, SharePoint, Apps)?
* ☐ Have license/capacity requirements (Pro, Premium, PPU) been finalized?
* ☐ Is there a backup and disaster recovery approach (version control, deployment pipelines)?

**🔹 5. Information Security Team Concerns**

* ☐ Is external sharing policy clearly defined and governed?
* ☐ Is access restricted to managed devices only (via Conditional Access)?
* ☐ Are export/download restrictions (CSV/Excel/PDF) enforced?
* ☐ Are sensitivity labels (MIP) applied within Power BI?
* ☐ If using Power BI REST APIs, are service principals/managed identities secured?

Would you like me to **expand this checklist with a “Recommended Best Practice” column** (so your teams see not just the question but also a suggested direction)? That way, it becomes both a **review tool** and a **guidance document**.

**You said:**

yes, visual architecture diagram will help

**ChatGPT said:**

I’ve created a consolidated **Power BI Adoption – Architecture & Security Review Pack (PDF)** that includes:

* ✅ A structured checklist with **recommended best practices**
* 📊 The **visual architecture diagram** showing On-Prem ↔ Azure ↔ Power BI connectivity

📂 Download the Review Pack (PDF)

Would you like me to also prepare a **one-slide executive summary** (PowerPoint style) for leadership approval, highlighting the key risks, decisions, and recommendations?