Absolutely — let’s rewrite the **MongoDB Atlas Design & Connectivity Review** page in a **clear, professional, and human-friendly** tone that still matches how Confluence pages are usually written.

# **🧩 MongoDB Atlas – Design & Connectivity Review Process**

## **📝 Overview**

This page is meant to guide application teams through the **Design** and **Connectivity Review** process for MongoDB Atlas. Before onboarding Atlas to production or handling any sensitive data, teams must ensure proper controls are in place — covering account setup, data classification, access management, encryption, and network connectivity.

The process helps ensure alignment with internal tech risk policies and the shared responsibility model across application teams and the platform team (Middleware Engineering).

## **🛠️ Design Review**

The **Design Review** focuses on your intended use of MongoDB Atlas — what kind of data will be stored, how access will be managed, and whether security and compliance requirements are met.

### **✅ Key Areas Covered:**

#### **🔐 Account Setup**

* Set up your AWS account under the correct CFT community.
* Projects must be onboarded to MongoDB Atlas using the ME Portal UI/API.
* If a new business line is involved, the Platform Team will help set up a new Atlas organization.

#### **📊 Data Classification**

* Sensitive data (like DP20/DP30) **must not be stored in non-production environments**.
* If your use case involves sensitive data in lower environments, raise it with Tech Risk for an exception or further review.

#### **👤 User Access & Authentication**

* Application users access Atlas clusters through IAM roles or API keys — no username/password login is allowed.
* Console access is protected using **SSO + MFA** via GS SecurID.
* Teams should follow the **principle of least privilege** when giving access.

#### **🔑 Authorization**

* Non-production accounts **must not** have access to production data or clusters.
* If you're deploying to production, follow strict separation between environments.

#### **🔒 Encryption**

* All data must be encrypted **at rest** using GS CMK or BYOK.
* TLS/SSL is used for encryption **in transit**.
* Client-side encryption can be used optionally for extra protection of sensitive data.

#### **📈 Logging & Monitoring**

* MongoDB Atlas provides dashboards for real-time monitoring.
* App teams are responsible for setting up and maintaining logs at the project level.
* Alerts and metrics should be managed via Infrastructure-as-Code (IaC) — typically through Terraform.

#### **🌐 Multi-region Deployment**

* If your app is deployed across multiple regions, ensure the region setup follows our **multi-region deployment guidelines**.
* Order and region mapping must match the approved pattern.

#### **🏢 Tenancy**

* For production use, choose **M30 clusters or higher**.
* Shared clusters are only allowed for development or testing purposes.

## **🌐 Connectivity Review**

Once your design is reviewed, the next step is to review **how your app connects to MongoDB Atlas**, especially for production or privacy-sensitive use cases.

### **🔧 What You Need to Do:**

#### **🔒 Secure Ports**

* Only use approved ports:  
  + Port **443** for secure traffic
  + Ports **1024–65535** for Atlas PrivateLink (already approved)

#### **🔗 Private Networking**

* **Use AWS PrivateLink** and private endpoints in Atlas — this ensures no traffic flows through the public internet.
* All VPC endpoints should be provisioned from your CFT or SkyTransit account.
* If needed, work with your network team to allow outbound traffic to Atlas endpoints.

#### **🚫 Non-Prod to Prod Access**

* Access from **non-prod to prod environments is strictly prohibited**.
* If there's a specific case where cross-env access is needed, it must be reviewed and approved by Tech Risk.

#### **🔍 Inventory Scanning**

* The Platform team scans Atlas clusters every 2 hours and updates the internal inventory.
* If you're handling personal or sensitive data, make sure your collections are registered in the ME Privacy Inventory.

## **✅ Quick Checklist Before Submitting for Approval**

| **✅ Question** | **Your Answer** |
| --- | --- |
| Is your AWS account set up correctly under CFT? | Yes / No |
| Is the Atlas project onboarded via ME Portal? | Yes / No |
| Are you handling sensitive data? If yes, is it stored only in prod? | Yes / No |
| Are you using SSO + MFA for console access? | Yes / No |
| Are you using API keys/IAM roles for DB access (no passwords)? | Yes / No |
| Is encryption at rest enabled and CMK managed? | Yes / No |
| Have you disabled cross-environment access (e.g., non-prod to prod)? | Yes / No |
| Is network traffic going through PrivateLink only? | Yes / No |
| Are privacy-sensitive datasets registered in ME Inventory? | Yes / No |

## **🔁 How the Process Works**

1. **You (App Team)** document the design and connectivity details on this Confluence page.
2. **Tech Risk** reviews the use case and checks for:  
   * Proper security controls
   * Data classification
   * Network and environment separation
3. **Platform Team** (Middleware Engineering) assists with:  
   * Atlas organization setup
   * API key provisioning
   * Inventory and project-level support

Based on the screenshots and the structure shown in the last image (Snowflake Design & Connectivity Review Approval Process), here’s a clean **Confluence page draft** for **MongoDB Atlas Design Review & Connectivity Review Approval Process** modeled in a formal and readable structure.

# **MongoDB Atlas Design Review & Connectivity Review Approval Process**

## **Overview**

This document outlines the procedure for conducting **design** and **connectivity reviews** for MongoDB Atlas, ensuring all required controls are in place and aligned with Tech Risk requirements. This process is aligned with the Shared Responsibility Model and covers usage, data classification, access controls, encryption, and network connectivity.

## **Design Review**

Design review assesses the proposed use case for MongoDB Atlas, data classification, authentication models, and adherence to internal policies and security controls.

### **Design Aspects to be Validated**

1. **Account Setup**
   * AWS CFT account created under the CFT community.
   * Project onboarded via ME Portal UI/API.
   * Atlas organization setup by the Platform Team.
2. **Data Classification**
   * Ensure sensitive data (DP20/DP30) is not hosted in non-production environments.
   * If hosting sensitive data in lower environments is necessary, a Tech Risk review is required.
3. **User Access & Authentication**
   * Atlas control plane access via GS SSO + MFA (console login).
   * Database access via programmatic API keys or IAM roles (no password-based auth).
   * App teams manage user entitlements using SDLC pipelines.
4. **Authorization**
   * Least privilege principle enforced.
   * No elevated privileges in non-prod environments for prod clusters.
5. **Encryption**
   * Encryption-at-rest using GS CMK or BYOK via SDLC.
   * Encryption-in-transit using TLS 1.2+.
   * Client-side encryption is optional for sensitive data.
6. **Logging & Monitoring**
   * MongoDB Atlas dashboards to be leveraged by App Teams.
   * No centralized log aggregation (project-level monitoring only).
   * Alerts and failover must be managed through IaC.
7. **Tenancy**
   * M30 or above is recommended for production.
   * Shared clusters can be used for non-production use cases.
8. **Multi-region Deployment**
   * AWS regions and node deployments must follow the approved multi-region pattern.
   * Validate the requirements from Tech Risk documentation.

## **Connectivity Review**

Tech Risk reviews and approves **network connectivity** after ensuring technical validations are complete.

### **1. Secure Ports**

* **Allowed Ports:**
  + Port 443 (for data transfer)
  + Ports 1024–65535 (for MongoDB PrivateLink endpoints, already approved)

### **2. Private Network Connectivity**

* **PrivateLink (AWS) + Atlas Private Endpoints** to be enabled.
* VPCEs to be provisioned and managed via SkyTransit / Application SkyFoundry accounts.
* No public network traffic is permitted.
* Outbound traffic to MongoDB Atlas VPCE must be permitted via ConnMan.

### **3. NDS (Non-Digital Standard) Access**

* Not allowed for production clusters.
* If required for non-prod environments, it must be escalated and approved by Tech Risk.

### **4. Cross-Environment Access**

* **Strictly prohibited**:  
  + No read/write access from non-prod to prod environments.
  + No cross-account or cross-environment traffic unless explicitly reviewed and approved.

### **5. Inventory and Scanning**

* Platform team runs scans every 2 hours and updates Inventory Central.
* App teams must register privacy-related datasets in the ME Privacy Inventory.

## **Checklist for Review**

| **Question** | **Response (Y/N)** | **Details / Remarks** |
| --- | --- | --- |
| Is the AWS CFT account under the CFT community? |  |  |
| Is the Atlas project provisioned via ME Portal? |  |  |
| Are sensitive data classifications (DP20/DP30) respected? |  |  |
| Are control plane access mechanisms using GS SSO + MFA? |  |  |
| Are database access mechanisms using programmatic keys? |  |  |
| Are encryption keys rotated annually? |  |  |
| Are alerts configured for clusters? |  |  |
| Is cross-env access completely restricted? |  |  |
| Are data clusters registered in ME Privacy Inventory? |  |  |

## **Approval Flow**

1. **App Team** initiates design and connectivity review by populating the use case in Confluence.
2. **Tech Risk** reviews:  
   * Data classification
   * Connectivity paths
   * Port usage
   * Multi-region compliance
3. **Platform Team**:  
   * Approves creation of Atlas organizations
   * Manages inventory and project-level governance

## **MongoDB Atlas – Design Review & Connectivity Review Approval Process**

*(Patterned after the Snowflake example you shared)*

### **Overview**

Tech Risk uses this two‑step gate to make sure every MongoDB Atlas deployment that reaches production meets our security, data‑governance, and connectivity standards.

1. **Design Review** – confirms you’ve built the right controls into the architecture.
2. **Connectivity Review** – verifies the network path, firewall rules, and data‑classification rules before any traffic flows.

## **1. Design Review**

Design Review focuses on the use‑case, data classification, security controls, and separation of environments. Tech Risk checks the items below (self‑attestation by the App Team, validated by Middleware Engineering (ME) and Tech Risk):

1. **Network connectivity** from all non‑prod DIDs to both prod/non‑prod Atlas clusters is already open **only** via approved PrivateLink endpoints.
2. **Network connectivity** from Dev Workspaces to prod/non‑prod Atlas clusters is already open **only** via PrivateLink.
3. **Network connectivity** from non‑prod R&D labs to prod clusters is **not** opened. Any cross‑environment request still requires case approval.

**Additional controls (all must be true):**

* Only **API keys** are used for programmatic access to Atlas projects (no username/password).
* Console (Atlas UI) access uses **GS SSO + MFA** and is not used for day‑to‑day administration.
* All datasets on Production Atlas are registered in Inventory Central with proper **Data Governance / Privacy** classification.
* **Non‑production Atlas accounts must not** be leveraged for data beyond DP10 classification.
* No prod DID is ingesting data on non‑prod Atlas.
* No non‑prod DID is accessing a production Atlas cluster (R/W). If this control needs to be exempted, a Tech Risk review is required.
* Lower‑classified DIDs (e.g., dev) do not have R/W access to higher‑classified Atlas clusters.
* For projects holding privacy data, **business‑user access** is governed by Privacy Stewards & Tech Risk.

## **2. Connectivity Review**

Tech Risk reviews and approves connectivity requests after validating **source/destination, ports, environments, and data‑classification**.  
 Firewall rules are opened **only after** Connectivity Review is “green.”

Connectivity Review is triggered when:

* A new system needs to reach an Atlas project.
* For *every* production Atlas project, **Design Review approval** is a pre‑requisite.
* This is the **final enforcement point** – if controls are missing, connectivity is blocked.

### **2.1 Secure Ports**

* **Port 443** is allowed for data transfer.
* PrivateLink ports **1024 – 65535** are allowed for Atlas VPCE (already enforced for CFT connectivity).

### **2.2 Cross‑Environment Check**

* **No cross‑environment access** (e.g., non‑prod → prod, dev → prod).
* If a legitimate use case exists (e.g., controlled data migration), it must be reviewed and documented by Tech Risk.

### **2.3 Data‑Classification Check**

* **No cross‑classification access.**
  + Example: DP‑10 → DP‑20 (write) is disallowed.
  + **R/W to or from DP‑30** data is not allowed unless justified and reviewed inline with signing design review.

### **Non‑prod / Sensitive‑Data Access (DP 20 & DP 30)**

If you need to host DP 20 or DP 30 data in non‑prod, complete the Q&A below; Tech Risk will decide if compensating controls are enough or if access must be blocked.

| **#** | **Question** | **Your Answer** |
| --- | --- | --- |
| 1 | What’s the name of the Atlas account & database? |  |
| 2 | Is this Atlas set‑up just for testing? If yes, is the db name suffixed with **\_pp** to differentiate from real prod? |  |
| 3 | What is the data & privacy classification of the data being ingested by the non‑prod DID? |  |
| 4 | What’s the source of this non‑prod deployment’s data? |  |
| 5 | What are the deployment IDs and Application IDs of the non‑prod deployment and the prod deployment? |  |
| 6 | Are there any bulk‑export or reporting jobs scheduled against this dataset? |  |
| 7 | How will the App Team ensure the data is not copied or pulled by other non‑prod DIDs from the mentioned non‑prod DID? |  |

*If any answer is incomplete or risks remain, Tech Risk raises a finding and blocks connectivity until resolved.*

### **Summary Flow**

1. **App Team** completes the **Design Review** checklist in this Confluence page.
2. **ME reviewers** verify IaC, API‑key scope, PrivateLink setup, and inventory registration.
3. **Tech Risk** validates data classification & cross‑environment controls.
4. If Design Review ✅, App Team submits **Connectivity Review** request (Jira/ME Portal).
5. **Tech Risk** inspects source/destination, ports, and DP20/DP30 questionnaire.
6. When all checks are green, firewall rules are opened, and you can start traffic to MongoDB Atlas.

**Need help?** Ping **#atlas‑support** on Slack or raise a ticket in **ME Portal** under “Atlas Onboarding / Connectivity Review.”