Enhancing Access Governance: LE-Specific Approval Enforcement for Global Entitlements

RSAM + ServiceNow + JIT Hybrid Approach for Compliance and Control

111111111111111111111111111111111111111111111

This is a governance and compliance issue where a global entitlement allows access to country-specific data without additional approvals, raising concerns from the respective countries. Since modifying the **RSAM structure** is not an option and strict timelines are in place, here are some possible solutions:

**1. Conditional Access Based on User Attributes (Recommended)**

* **Implement Attribute-Based Access Control (ABAC)**: Instead of modifying RSAM, apply a policy-based access layer that checks additional attributes (e.g., user role, location, or approval status) before granting access.
* **Example**: Even if the entitlement allows access, a middleware layer checks if the user is in an allowed region or has a specific tag before allowing access.

**2. Dynamic Approval at Data Access Level**

* Introduce a mechanism where **certain countries' data require a one-time approval** (without altering RSAM).
* **Example**: If a user with a global entitlement tries to access Malaysia or India data, an inline approval request is triggered.

**3. Country-Specific Access Logs & Review Mechanism**

* Implement a **real-time access logging and review mechanism** where countries can monitor who accessed their data.
* **Example**: A dashboard shows Malaysia/India teams all accesses via global entitlement, ensuring transparency.

**4. Hybrid Role-Based Access Control (RBAC) with Global Entitlement Override**

* Keep the global entitlement but introduce **country-level override roles** where:
  + If a user needs Malaysia/India access, an additional flag or approval is required.
  + Global entitlement remains unchanged but is **restricted dynamically** based on user context.

**5. Just-in-Time (JIT) Access for Country Data**

* Allow **temporary access grants** for sensitive country data via a JIT mechanism.
* Users with global entitlement would need to **request short-term access** for Malaysia/India data.

**6. API Gateway Rule Enforcement**

* If access is via APIs, an **API gateway layer** can introduce extra validation before allowing data retrieval.
* This allows **RSAM to remain untouched** while enforcing additional security at runtime.