let’s walk through a **realistic scenario** of how **RSAM + SNOW + JIT** would work together for **multi-legal-entity data access** (Malaysia, India, Singapore) using a **hybrid layered approach**. This approach balances **control**, **scalability**, **security**, and **auditability**.

**🔁 End-to-End Workflow: RSAM + SNOW + JIT**

**🎯 Scenario:**

A user, *Ravi*, from the UK team needs to access **global data**, including sensitive datasets from Malaysia, India, and Singapore.

**✅ Step-by-Step Breakdown**

**1️⃣ Request Initiation — via RSAM**

* Ravi logs into RSAM and requests access to GLOBAL\_DATA\_ACCESS entitlement.
* RSAM collects metadata (justification, region impact, etc.).
* **RSAM doesn’t handle approval logic**; it simply **routes to SNOW** via integration.

**2️⃣ Workflow Kickoff — ServiceNow Workflow Begins**

* RSAM sends request payload to SNOW.
* Based on the entitlement (GLOBAL\_DATA\_ACCESS) and metadata (data regions: Malaysia, India, Singapore):
  + SNOW dynamically **routes approval to 3 legal entity approval groups**:
    - Malaysia InfoSec/Compliance
    - India Security Officer
    - Singapore Legal/Compliance

**3️⃣ Conditional Multi-Entity Approvals**

* Each country LE group reviews:
  + Business need
  + Risk
  + Timeframe
* If **any country rejects**, access is **denied or restricted to approved scopes only**.
* If **all approve**, SNOW logs this and sends confirmation to **Identity Governance platform** (or RSAM/SailPoint/Okta).

**4️⃣ Entitlement Provisioning**

* Identity Governance system grants **baseline GLOBAL\_DATA\_ACCESS role** to Ravi.
* This role **does not include full data visibility** by default.

**5️⃣ Enforcement via JIT (Just-In-Time Access)**

* Ravi logs into a data dashboard and tries to query **Malaysia data**.
* System performs **real-time access check**:
  + Is Ravi authorized for Malaysia data?
  + Has he passed JIT approval for today?
* Since Ravi has the entitlement and prior approval, he:
  + Submits a **JIT request** (e.g., via in-app form or API call).
  + Gets **temporary access (e.g., 2 hours)** to Malaysia data.
* JIT system logs:
  + Who accessed, what was accessed, when, and why.
  + Auto-revokes access after 2 hours.

**6️⃣ Audit & Monitoring**

* SNOW logs are available for access approvals.
* JIT logs show **usage patterns**, timeframes, and anomalies.
* Reports can be auto-sent to:
  + Country compliance teams
  + Global audit group
  + InfoSec leaders

**🧠 What Problems Does This Solve?**

| **Concern** | **Addressed By** |
| --- | --- |
| No LE approvals? | SNOW dynamic routing to legal entities |
| Global access too broad? | JIT enforces per-country usage |
| Auditing need? | SNOW + JIT logs provide granular traceability |
| Future LE onboarding? | SNOW routing rules scalable to new LEs |
| Security risk? | JIT ensures no standing access |
| RSAM dependency? | RSAM stays as intake layer, no structural changes needed |

**🏗️ Bonus: System Architecture View (Layered)**

pgsql

CopyEdit

+-----------------------------+

| User (e.g., Ravi) |

+-----------------------------+

|

v

+-----------------------------+

| RSAM Portal |

| (Request Intake + Logging) |

+-----------------------------+

|

v

+-----------------------------+

| SNOW Workflow Engine |

| (Multi-LE Dynamic Approval)|

+-----------------------------+

|

v

+-----------------------------+

| Identity Governance Tool |

| (SailPoint / Okta / Oracle) |

+-----------------------------+

|

v

+-----------------------------+

| JIT Access Enforcement |

| (Proxy, ABAC, Gateway, App) |

+-----------------------------+

|

v

+-----------------------------+

| Target Data Platform |

| (App, Dashboard, Database) |

+-----------------------------+