Here’s a high-level architecture diagram that integrates Azure AD, Active Directory (AD), SailPoint MyID, and AWS IAM roles and policies:

### IAM Architecture Diagram

┌─────────────────────────────────────┐

│ User Layer │

│ - Employees, Partners, Customers │

│ - User Roles and Groups │

│ - User Provisioning and Deprovisioning │

└─────────────────────────────────────┘

▲

│

┌─────────────────────────────────────┐

│ Authentication Layer │

│ - Azure AD │

│ - Active Directory (AD) │

│ - Multi-Factor Authentication (MFA)│

└─────────────────────────────────────┘

▲

│

┌─────────────────────────────────────┐

│ Authorization Layer │

│ - Azure AD Roles and Policies │

│ - AD Groups and Permissions │

│ - SailPoint MyID │

└─────────────────────────────────────┘

▲

│

┌─────────────────────────────────────┐

│ Access Management │

│ - Single Sign-On (SSO) │

│ - Federated Identity Management │

│ - Access Requests and Approvals │

└─────────────────────────────────────┘

▲

│

┌─────────────────────────────────────┐

│ Audit and Monitoring │

│ - Azure AD Logs │

│ - AD Logs │

│ - SailPoint MyID Logs │

│ - AWS CloudTrail Logs │

│ - Compliance and Reporting │

└─────────────────────────────────────┘

```

### Explanation:

1. \*\*User Layer\*\*: This layer includes all users, their roles, and groups, as well as the processes for provisioning and deprovisioning users.

2. \*\*Authentication Layer\*\*: This layer handles user authentication using Azure AD, AD, and multi-factor authentication methods.

3. \*\*Authorization Layer\*\*: This layer manages access controls, including Azure AD roles and policies, AD groups and permissions, and SailPoint MyID for identity governance.

4. \*\*Access Management Layer\*\*: This layer includes single sign-on (SSO) and federated identity management, ensuring seamless access to resources.

5. \*\*Audit and Monitoring Layer\*\*: This layer involves logging and monitoring activities across Azure AD, AD, SailPoint MyID, and AWS CloudTrail to ensure compliance and detect any suspicious activities.

This architecture ensures a robust and secure identity and access management system for your bank, integrating various tools and services to provide comprehensive governance and control.

Does this architecture meet your requirements?

Here’s an expanded table with the **Risk Addressed** and **Risk for Each Control** columns:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control** | **Central Level** | **Application Level** | **Risk Addressed** | **Risk for Each Control** |
| **Role-Based Access Control (RBAC)** | Defined in Azure AD/AD | Mapped to app-specific roles | Mitigates **over-privileged access**, **insider threats**, and **privilege escalation**. | **Misconfigured roles** leading to excessive privileges or lack of access for critical functions. |
| **Authentication (MFA, SSO)** | Managed centrally via Azure AD | Integrated at app-level | Addresses **compromised credentials**, **phishing attacks**, and **weak authentication**. | **Failure to enforce MFA** or weak SSO configurations may allow unauthorized access. |
| **Logging and Monitoring** | Centralized in SIEM | Detailed app-level logging | Mitigates risks of **undetected breaches**, **unauthorized access**, and **compliance failures**. | **Incomplete logging** or **delayed monitoring** can result in missed security incidents. |
| **Policy Enforcement** | Managed via Azure AD/AWS IAM | Custom policies per app | Prevents **misconfigurations**, **policy deviations**, and **non-compliance**. | **Policy gaps** or inconsistent enforcement could lead to security and regulatory issues. |
| **Access Request Workflow** | SailPoint MyID workflows | Application-specific approvals | Reduces risks of **unauthorized access** and **orphaned accounts**. | **Weak approval processes** or bypassing workflows could allow unauthorized access. |
| **Privileged Access** | Managed via PAM (e.g., Azure PIM) | App-specific elevated roles | Protects against **privilege escalation** and **insider threats**. | **Overly broad privileged roles** or weak PAM configurations can lead to abuse of elevated access. |
| **Compliance Reporting** | Centralized (SailPoint/Azure) | App-specific dashboards | Ensures compliance with regulations and reduces **regulatory non-compliance risks**. | **Inaccurate reporting** or lack of traceability could lead to regulatory penalties. |
| **Conditional Access Policies** | Managed in Azure AD | Specific app rules enforced | Mitigates **location-based threats** and access from **untrusted devices**. | **Weak or overly permissive policies** could allow risky access from untrusted sources. |
| **Password Policies** | Enforced in Azure AD/AD | N/A | Prevents risks of **weak credentials** and **credential compromise**. | **Poor password hygiene** or inability to enforce policies leads to higher credential risks. |
| **Federated Identity Management** | Managed via Azure AD and AWS | Integrated at app-level | Mitigates risks of **token misuse** and **weak SSO configurations**. | **Improper token handling** or lack of federation monitoring can expose identity-related risks. |
| **User Behavior Analytics (UBA)** | Central monitoring in SIEM | App-level anomaly detection | Addresses **insider threats** and **compromised credentials** by identifying suspicious behaviour. | **False negatives** or inability to detect subtle anomalies could lead to undetected breaches. |
| **Deprovisioning Orphaned Accounts** | Automated via SailPoint MyID | Managed for app-specific users | Mitigates risks of **orphaned accounts** being exploited. | **Delayed deprovisioning** or failure to detect orphaned accounts can leave access vulnerabilities. |
| **AWS IAM Role Reviews** | Centralized reviews | Application-specific policies | Prevents **over-permissioning** and **policy misconfigurations** in AWS. | **Incomplete reviews** or failure to address risky permissions could lead to unauthorized access. |
| **Audit Trails** | Centralized in Azure AD/AD and AWS logs | App-specific logs maintained | Reduces risks of **compliance failures** and provides traceability for **security incidents**. | **Incomplete or tampered logs** reduce visibility and hamper incident investigations. |
| **Just-in-Time Access (JIT)** | Enabled for admin roles | Temporary app-specific access | Mitigates risks of **privileged role misuse** and **over-permissioning**. | **Failure to monitor JIT access** or improper expiration can leave elevated permissions exposed. |
| **Data Encryption and Masking** | Central policies in Azure/AWS | Enforced at data level | Protects against **data breaches** and ensures **confidentiality of sensitive information**. | **Encryption misconfigurations** or lack of masking can expose sensitive data to unauthorized users. |
| **Segregation of Duties (SoD)** | Enforced via role definitions | Specific workflows per app | Reduces risks of **fraud** and **conflicting privileges**. | **Conflicting roles** or inadequate SoD checks could lead to fraudulent activities. |
| **Incident Response** | Centralized SOC monitoring | App-specific incident rules | Mitigates risks of **delayed breach detection** and **escalating attacks**. | **Delayed response** or lack of incident-specific playbooks can increase attack impact. |
| **API Security** | Centralized API policies | Scoped permissions per app | Prevents **API exploits**, **unauthorized access**, and **data exposure**. | **Unsecured APIs** or excessive permissions can expose critical systems to threats. |
| **Vendor and Third-Party Access** | Centrally governed policies | Monitored for specific apps | Mitigates risks of **supply chain attacks** and **unmonitored vendor activities**. | **Unmonitored vendor activities** or lack of time-bound access may lead to data and system misuse. |

**Highlights of Risk Management**

* **Central Level**: Controls aim to address governance, standardization, and monitoring but must be validated regularly to avoid misconfigurations or lapses in policy enforcement.
* **Application Level**: Controls address specific operational requirements but must integrate effectively with central governance to avoid fragmentation or misalignment.

Would you like a deeper dive into any specific risk-control pair or further examples?

**Key Components of IAM:**

1. **Identification**:
   * Assigning unique identifiers (e.g., usernames, employee IDs) to individuals or entities.
2. **Authentication**:
   * Verifying the identity of users through methods such as passwords, biometrics, or multi-factor authentication (MFA).
3. **Authorization**:
   * Granting or restricting access to resources based on policies, roles, and user permissions.
4. **Account Management**:
   * Managing the lifecycle of user accounts, including provisioning, de-provisioning, and regular reviews.
5. **Access Control**:
   * Enforcing rules and permissions to ensure users access only what they are authorized to.
6. **Auditing and Monitoring**:
   * Tracking and logging user activities for compliance, troubleshooting, and security analysis.

When conducting a Privileged Access Management (PAM) audit, it’s essential to consider accounts with elevated privileges or those that have access to sensitive systems or data. The following types of accounts should be included in the audit:

1. **Administrator Accounts**: These are accounts with system-wide privileges. This includes accounts such as root (Linux/Unix) or Administrator (Windows).
2. **Service Accounts**: These accounts are used by applications or services to interact with other systems and are often granted elevated privileges for automation purposes.
3. **Database Accounts**: Accounts with access to database management systems (DBMS) that are critical to the organization’s operations. These accounts often require strict control due to the sensitive nature of the data they access.
4. **Network Accounts**: Accounts that have elevated access to network infrastructure, such as routers, switches, firewalls, etc. These are highly privileged and should be carefully monitored.
5. **Cloud Administrator Accounts**: Accounts with administrative access to cloud platforms like AWS, Azure, Google Cloud, or any other third-party cloud services.
6. **Third-Party Access Accounts**: Accounts granted to third-party vendors, contractors, or external users that have access to the organization's systems. This could include access to infrastructure, software, or data.
7. **Privileged User Accounts**: These are accounts used by employees or contractors that require elevated access to perform certain tasks, such as security personnel, system administrators, or senior developers.
8. **Domain Accounts**: Accounts with domain-wide access in Windows environments, which could be used for cross-system access.
9. **Superuser Accounts**: Special accounts on Unix/Linux systems with unrestricted access, such as "root," "sudo," or other similar accounts.
10. **Audit Accounts**: These are accounts used to monitor, log, and audit system activity. While they don’t directly grant access to systems, they should be protected to ensure their integrity.
11. **Backup Accounts**: Accounts that are used to back up critical data or systems, as they typically have broad access to data and systems across the network.
12. **Application Admin Accounts**: Accounts used to manage critical applications, including internal or external business applications. These accounts often require additional monitoring and auditing due to the sensitive nature of the data they manage.
13. **End User Elevated Access Accounts**: Accounts where users are granted elevated privileges for specific tasks (e.g., installing software, modifying configurations).
14. **Remote Access Accounts**: Accounts used for remote access to the corporate network or systems, such as VPN accounts or Remote Desktop Protocol (RDP) access.

When auditing these accounts, ensure you review:

* Account creation, modification, and deletion logs.
* Access permissions and roles.
* Session logging and monitoring.
* Multi-factor authentication (MFA) status.
* Periodic access reviews and certifications.

Additionally, enforcing the principle of least privilege and ensuring that only necessary access is granted is vital in minimizing potential risks.