**Defining IAM Governance Policies**

IAM governance policies are the backbone of a secure and compliant identity management system. They establish the rules and processes to manage identities, access, and compliance effectively.

1. **What Are IAM Governance Policies?**

IAM governance policies are written rules that define:

* Who can access systems and data.
* What level of access they are granted.
* When and how access should be reviewed and modified**.**

1. **Key Governance Policy Areas**

* **Access Control Policy:**
  1. Defines how access is granted, modified, and revoked.
  2. Example:

“All access requests must be approved by the user’s manager.”

* **Role Management Policy**:
  1. Establishes guidelines for creating, assigning, and updating roles.
  2. Example: “Roles must follow the least privilege principle and be reviewed every 6 months.”
* **Password Policy**:
  1. Sets rules for creating and managing passwords.
  2. Example: “Passwords must be at least 12 characters long and include uppercase, lowercase, numbers, and special characters.”
* **SOD Policy**:
  1. Prevents users from having conflicting roles or permissions.
  2. Example:

“No user should have access to both create and approve financial transactions.”

* **Audit and Compliance Policy**:
  1. Ensures all access and changes are logged and reviewed.
  2. Example:

“Quarterly audits must be conducted to verify user access.”

1. **Example IAM Governance Policy Framework**

Here’s a simple framework to define your policies:

|  |  |  |
| --- | --- | --- |
| **Policy Name** | **Purpose** | **Key Rules** |
| Access Control | Ensure secure and appropriate access | Manager approval required; periodic access reviews |
| Role Management Policy | Simplify access management through roles | Roles are reviewed every 6 months; least privileged principle enforced |
| Password Policy | Strengthen account security | Passwords must be complex and changed every 90 days |
| SOD Policy | Prevent conflicts in permissions | Automated SOD checks for all provisioning actions |
| Audit Policy | Maintain records for compliance and monitoring | All changes logged; access reviews conducted quarterly |

1. **Implementing Governance Policies**

* **Define policies:**
  1. Write clear, concise, and enforceable policies.
  2. Use tools like Saviynt to automate enforcement
* **Communicate Policies:**
  1. Train employees and managers on the importance of governance policies.
  2. Share quick-reference guides or dashboards for key rules.
* **Monitor and Improve**:
  1. Use analytics to track compliance.
  2. Refine policies based on audit findings or organizational changes.

**Activity 7: Design a Governance Policy**

Imagine you’re creating a policy for **Access Reviews**. Define:

1. The **frequency** of reviews.
2. The **stakeholders** responsible.
3. The **action steps** for remediation.

Access Review Policy:

1. Frequency: Quarterly is a great choice for balancing regular checks without overburdening the team.
2. Stakeholders Responsible:

Managers:

* Review access for their direct reports.

Application Owners:

* Review access to critical systems.

Compliance/Audit Team:

* Oversee the process and ensure adherence to policies.

1. Action Steps for Remediation:

* Preparation:
  1. Generate access review reports from the IAM tool (e.g., Saviynt).
  2. Include details like:
     1. User id
     2. Roles/Permissions
     3. Last Accessed Date
     4. Justification for Access
* Review Process:
  1. Managers:
     1. Approve or revoke access based on team members’ responsibilities.
  2. Application Owners:
     1. Confirm access for external or shared resources (e.g., APIs, external contractors).
* **Remediation**:
  1. Revoke unnecessary permissions immediately.
  2. Flag exceptions for further investigation (e.g., dormant accounts with sensitive access.)
* **Audit and Documentation**:
  1. Log all approvals, revocations, and exceptions.
  2. Generate a compliance report for stakeholders and auditors.

**Example Workflow for Access Reviews**

