**Compliance and Attestation**

Compliance is all about adhering to laws, regulations, and policies related to identity and access management.

1. **Why is compliance important in IAM/IGA?**

* Protects sensitive data from unauthorized access.
* Ensures adherence to regulations like GDPR, HIPAA, or SOX.
* Avoids penalties and security breaches.
* Simplifies audit processes with clear records.

1. **What is Attestation?**

Attestation is the process of reviewing and certifying that users have the appropriate level of access.

* Who performs Attestation?
  + Managers, application owners, or auditors.
* How often is it done?
  + Typically, periodic (e.g., quarterly, annually) or triggered by events like role changes.

1. **Key components of Attestation**
2. **Access Review:**
   * Regularly verify that users have appropriate access.
   * Example: ensure a terminated employee no longer has access.
3. **Certification:**
   * Managers or role owners certify (approve/reject) user access during reviews.
4. **Remediation:**
   * Actions taken to remove inappropriate access.

**Example Scenario for Attestation**  
Company: A financial organization needs to comply with SOX regulations.

Requirements: Quarterly reviews of all employee access to sensitive systems.

1. Access Review:

* List all employees with access to financial systems.
* Identify unnecessary or excessive permissions.

1. Certification:

* Managers approve or revoke access for their team members.

1. Remediation

* Revoke access for unauthorized users immediately.

Activity 4: Compliance and Attestation

Using the example above, answer these:  
1. What steps would you take to set up an attestation campaign for financial organization?

2. If a manager identifies unauthorized access during certification, what remediation steps should be taken?

***Solution:***

**1. Setting Up the Attestation Campaign**

1. **Prepare Data for Review**:
   * Gather a list of:
     + Employees.
     + Their roles and permissions.
     + Systems they have access to.
   * Include metadata like last access time and usage frequency (to spot dormant accounts).
2. **Define Scope**:
   * Focus on sensitive systems (e.g. financial apps, payroll systems).
   * Exclude general access (e.g., email or cafeteria booking) unless needed.
3. **Assign Reviewers**:
   * Managers for direct reports.
   * System/Application owners for technical resources.
4. **Set Up Notifications**:
   * Inform reviewers of their responsibilities.
   * Set a deadline for completing the review.
5. **Conduct the Review**:
   * Provide an intuitive dashboard for managers to:
     + Approve/retain valid access.
     + Revoke unnecessary access.
     + Mark anomalies for further investigation.

**2. Certification Process**

* Managers approve or revoke access based on need.
* Use tools like Saviynt to automate the presentation of data and decisions.

**3. Remediation for Unauthorized Access**

1. **Immediate Revocation**:
   * Disable access for the unauthorized user.
   * Log the action for audit purposes.
2. **Root Cause Analysis**:
   * Identify how unauthorized access was granted:
     + Was it an error during onboarding?
     + Was it due to role sprawl (overlapping permissions)?
3. **Preventive Measures**:
   * Update access policies to prevent recurrence.
   * Implement automated SOD (Segregation of Duties) checks.