Attestation and Compliance

Scenario Background

A departmental Human Resources employee has access to an application that grants her access to salary information for her department. Access to this application is controlled through group memberships in the Grouping Service and is provisioned and deprovisioned through the Provisioning Service.

The institution's Internal Audit group has established an auditing control that requires everyone with access to salary information to take sensitive data training on an annual basis, and to have their access re-approved by a supervisor once a year.

The Provisioning Service has two attestation rules configured:

1. Members of the 'Salary History' group must be in the group of users that have taken sensitive data training annually
2. Members of the 'Salary History' group must have an approved request that is less than one year old.

Scenario Walkthrough

1. The Provisioning Service evaluates whether or not the user is in the group that has taken sensitive data training within the last year. If so, the service moves on to the next attestation rule. If not, an institutionally defined workflow is fired that may inform the user about the need for training, remove the user from the group, notify the user's supervisor or take other action as appropriate.
2. The Provisioning Service evaluates the date of the last approved request. If the date is greater than one year, a new request is generated automatically and sent to the user's supervisor. If the request is approved, the approval is noted as a positive attestation that her access is still required. If it is not approved, her access is removed.
3. The Internal Audit group is able to verify that the required audit controls were met, and that the user had both taken sensitive data training and had a supervisory attestation that her access was still necessary.