Omada

Auditing

IdentityPROCESS+

Audits are performed to assess the measures in place to safeguard an organization's data, infrastructure, and other assets. Successfully completing audits is a top priority for IT, Security, and IAM teams. A failed audit can result in fines, personnel changes, reputational damage, and more. Consequently, significant effort goes into compiling the necessary data and documentation during an audit.

Identity Governance & Administration (IGA) solutions are meant to support the creation and evaluation of business policies, rules and governance controls, and essentially provide assurance to auditors and executive stakeholders that proper security controls are enforced. IGA solutions should also enable the organization to demonstrate that the IT environment is under control and managed properly.

Audit reports allow visibility on controls such as orphaned accounts, entitlement creep, Segregation of Duty (SoD) violations, and visibility into privileged user accounts. Advanced auditing processes deliver comprehensive views of access rights based on identity intelligence from data collected across business-critical systems and applications. Identity and access data is compared against policies and any violations automatically identified to enable instant remediation. Reporting delivers answers to 'who has access to what' and 'who approved the access.' However, without defining a process for audits, it is easy to waste time, energy, and resources, without necessarily achieving enhanced security.

As outlined in Omada IdentityPROCESS+, there are several auditing best practices that are critical for optimizing efficiency, tightening security, and ensuring compliance.

Audit Trail

Audit trail functionality enables auditors to gain insight into why access exists, who authorized it, and how that access originated. Organizations should operate with scheduled and ad hoc security assessments to constantly monitor and alert the responsible teams if policies are violated, or if security is potentially compromised. IdentityPROCESS+ ensures that security policies are followed and that there is available and automated documentation for how sensitive data is being protected. This includes repeatable processes for documenting all decisions made to determine why access was granted (and who authorized it) as well as any entitlements that were granted despite policy violations - so as to determine who authorized them and why. Audit trails are useful for generating detailed reports on decisions that have affected and entitlements and can drill down to detailed specific resource assignment reports through filtering, searching, and sorting. Audit trail data should include information on object changes, changes to permissions, access requests, approvals and custom objects.

Audit History

History processes ensure that all process data across all systems within Omada is stored for a potential audit. Audit findings should be presented via a dashboard and exportable in multiple reporting formats for identities, accounts, access and entitlements, policies, and systems. Audit logs and histories should also provide date and time-stamp functionality for documentation. Advanced historical auditing features point in time, changes within period, historical development, and change log reporting. Auditors are able to define the search scope and the parameters on any and all objects in Omada which include effective times, validity dates, status, categories, and usage patterns. These are based on selected values such as identities, context, accounts, resources, access, orphan objects, account usage, data quality and systems. Data is also extracted from the Omada Data Warehouse and archives to generate reports when called.

Audit Log

All certification campaigns must be logged as an assurance mechanism for the auditor to validate that appropriate controls are in place. The auditor, system administrator, and relevant system owners can view assigned certification campaign questions and update them in real-time. They can also review the reports within Omada for continuous evaluation of key controls, business rules, data integrity, and performance. IdentityPROCESS+ also enables auditors to verify and prove that a certification campaign has taken place with a date and time log of any remediation actions.

Audit Policies

Audit policies evaluate business rules and controls against the actual state of identities and associated access rights. IdentityPROCESS+ helps organizations implement a method to alert control owners and includes the option to perform remediation if inconsistencies or violations are discovered. Processes include performing policy management through the audit dashboard that displays all policies for which a user is authorized. This should be configured to constantly review all active identities and compare the actual versus desired states. This can reveal inconsistencies to the proper support teams so that they can be remedied.

Control policies should also be used on an ongoing basis to detect and react to inconsistencies across policies. Potential issues might include objects that do not have an owner, circularities in the role hierarchy, and roles without proper descriptions and/or mandatory fields defined. Control policies are used to detect conflicts or problems within Segregation of Duty (SoD) policies. The policy owner should have the ability to override and accept violations after providing a justified reason for the need to implement compensating controls. SoD control policies are evaluated every time the access rights for an identity are re-evaluated within Omada. Risk scoring can also be used to define risk for improperly configured control and constraint policies. Every improperly applied policy and override of a constraint policy contributes to the risk score and can easily be bubbled up to auditors, security, or IT team members.

Audit Response

If violations have been detected, it is crucial to enable the organization to ensure that exceptions are detected and handled by the responsible policy owner. IdentityPROCESS+ provides guidance for organizations to continuously evaluate policies, either on defined schedules or triggered ad hoc by the audit policy owner. When a policy exception is detected, Omada automatically triggers an automated workflow to alert the policy owner, the user's manager or the security team. Depending on the type of policy violation and any exceptions required, the reviewer can allow, correct, or mitigate the incident. IdentityPROCESS+ outlines the need to first load data from target systems into the Omada Data Warehouse, where Key Performance Indicator (KPI) improvements and history are monitored.

Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Identity Security Breach Management, the following teams must be involved in the following capacities:

Executive Team

- Establish vision for Audit efforts
- Review results to ensure Audit requirements are addressed

Policy Owners

- Ensure that policies are aligned with business needs
- Participate in reporting and certification campaign scoring and follow-up

Auditors

- Define audit parameters
- Conduct the audits
- Participate in testing audit functions
- Analyze and remediate exceptions

IGA Team

- Configure and monitor Omada

Key Best Practices

Define effective audit processes

It is essential that audit policies are aligned with the business and deliver the expected results. The audit processes should always provide answers to the questions of "who has access to what, who approved that access or policy exception?" Use control policies to detect and react to inconsistency within the policies. Provide a remediation workflow to address any issues discovered within the policies. Leverage constraint policies to detect conflicts or problems within segregation of duty policies and provide a way to document policy exceptions and overrides (compensating controls). Assign each policy object a weight/score and include a risk scoring control to understand the exposure of policies not being implemented or enforced properly. Provide auditors governance dashboards and the ability to report the status of the various policies, and for continuous evaluation of key controls, business rules, data integrity, and performance to ensure each policy object is being historically documented and stored properly.

Establish effective SoD audits

The lifecycle of permissions and roles can be very dynamic. As a result, segregation of duty policies (SoD) can over time become highly complex and difficult to manage. This also can lead to the policies becoming stale or dated, resulting in the generation of false policy application results. Without a business-oriented approach the organization will struggle to deliver effective SoD audits. Therefore, it is recommended to define segregation of duties (SoD) policies based on business processes, supporting the standard approach of roles and permissions.

The list of business processes can be hierarchical, allowing the organization to define both fine-grained SoD but also broader operational constraints. The organization can rapidly introduce new SoD constraints without needing to rebuild their role catalogue, since the SoD policy is based on business process that changes much less frequently.

Ensure ongoing compliance

Some organizations implement scheduled security assessments once or twice a year or quarterly, an approach that has the potential to create gaps in security that can go undiscovered for months at a time. In regulated industries and for mission-critical systems, it is highly recommended to conduct audits more frequently. To constantly monitor and alert if policies are violated or security is compromised, policy auditing processes can be set to run as a continuous activity to achieve the following:

- Establish constant controls of access to business-critical data and IP
- Identify and resolve SoD issues
- Ensure that all relevant access rights are identifiable
- Review policies quarterly for effectiveness
- Refine and apply granular reporting and analysis

?

Auditing Questions to consider

- Do we have business alignment?
- Who are the designated policy owners?
- How often should the auditing processes be scheduled to run?
- What is the frequency for policy review?

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to maximize efficiency, reduce risk, and meet compliance. requirements. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our leading technology, proven best practice process framework, and best-in-breed deployment approach.

For more information, go to **omadaidentity.com**