BEST PRACTICES FOR MANAGING ACCESS RE-CERTIFICATIONS

Whitepaper I 2022

avancercorp.com

INTRODUCTION

To maintain your system's security on a continuous basis, it is best to audit user access to all applications, and what they can do in those applications, networks, and other enterprise assets periodically. It is imperative to review all accesses to find any unauthorized access or over access, validate accesses as certified or revoked, and ensure the availability of an audit trail. Such an access re-certification exercise is undertaken on annual basis in almost all organizations nowadays to ensure that only enough access is provided to a user, based on their requirements, and the said user is not given excess access than needed.

Further, certain industries, especially healthcare and financial services, have mandatory regulatory compliances, which mandate information security departments to certify users and apps on a regular basis for remaining compliant. For e.g. the NYDFS Cybersecurity Requirements took effect on March 1, 2017 as defined under 23 NYCRR Part 500 that each covered entity, such as banking and other financial institutions, insurance companies that do business in New York stat shall limit user access privileges to information systems that provide access to nonpublic information and shall periodically review such access privileges.

TYPES OF CERTIFICATION

- User Certification
- Role Certification
- Account Certification
- Entitlement Certification
- Information Owner certification
- Physical Server Certification
- Privileged Access Certification

> At Avancer, our Identity experts have analyzed numerous use cases and scenarios while helping medium to large size organizations on their Access re-certification needs at periodic intervals.

Similarly in Healthcare industry, being compliant through access certifications enable these organization to ensure that security standards challenges, and insider threats are mitigated. Applications like Cerner, Epic, Allscripts, McKesson nowadays require a robust compliance program to ensure employees and providers have correct access into these EMR systems.

Identity security solutions built on a solid IAM platform enables the organizations with an annual or on-demand certification campaign approach to validate user access to organizational resources, or to revoke access as needed. Through Access re-certification campaigns, enterprises may allow certain people, such as system owners or department managers, to review the identity footprint and system access assigned to them.

At Avancer, our Identity experts have analyzed numerous use cases and scenarios while helping medium to large size organizations on their Access re-certification needs at periodic intervals. While working through these challenges for almost last two decades, our experts have been able to formulate certain best practices for managing Access reviews in an IAM platform.

We are sharing some of our learning to help other similar organization in their Access Recertification journey. Let us review some of these Best Practices for **Managing Access-Recertification.**

BEST PRACTICES FOR MANAGING ACCESS-RECERTIFICATION

No. 1: Generate app certification campaign

In this campaign, all users for a specific application or resource will be validated to ensure that their access, rights, and privileges are correct and appropriate. IAM platform will allow admins to create a certification campaign for reviewing user access for a particular application or group of applications. Once the admin creates such a campaign, the reviewer is provided with a notification that the certifications are ready to be reviewed and validated.

After the reviewer has taken an action, the certifications are routed to application owners to ensure that the reviewer has taken correct action followed by a stamp from Information security department (ISD) for final approval. Many times, organization can change this behavior of certification review steps depending on their needs. For e.g., in case of privileged users' certifications, the application owners can review the access and ISD can do the final approval.

No. 2: Ensure reviewing of entire user base

Before starting the certification process, the list of reviewers needs to be compiled by the security team to ensure that the user base from all the departments is also covered and no user is missed from the access review. The reviewers should be in line with the organizational hierarchy, maintained by the organization's HR. This is undertaken at the initial stage when a certification admin defines the certification campaign requirements. All of this information needs to be matched between the application and IAM platform so that there is no discrepancy.

No. 3: Provide specific guidance to the reviewers

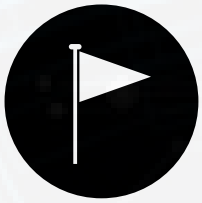
This best practice helps the reviewers to understand the review process and take access decisions by following the instructions that are specific to the organization's policies, practices, and familiarity with IAM platform User interfaces. If reviewers are not up to date on their knowledge of IAM platform and its user interfaces, the reviewers may lack the will to take on access reviews tasks.

A continuous training and adoption are very much required for the reviewers to use IAM platform. It is imperative to create enough documentation with screenshots, and/or video clips, to reflect the look and feel of the instance of IdM tool, the organization's policies, and the specific options available for the certifications and access reviews. Many Identity solutions provide an easy-to-use interfaces and dashboard that quickly enables the reviewers about the whole certification process.

No. 4: Encapsulate access into entities such as roles

It is a good practice to encapsulate accesses into entities such as roles. Since roles can include many entitlements, a good role model can help reduce the number of individual access items a reviewer needs to process.

- One can include user-friendly descriptions with the roles to help reviewers understand what access is appropriate for and granted by the role. However, these roles need to be certified before Certifying User Access. This helps to ensure that roles include the right permissions and entitlements.
- Roles should be certified by business experts, to validate that they provide correct and expected access. Further, the certification should focus on reviewing if the organization has consistent and meaningful names for roles and entitlements. This helps reviewers to quickly grasp important information about the access under review.
- Through IAM platform, reviewers may choose various roles or entitlements that need to be certified from the list of roles provided in the platform.
- Reviewers may also validate the associated access profiles and other details related to a particular role.



No. 5: Flag high-risk access

It's a given that some access carries higher risk than others. Elevated administrator privileges and access to sensitive financial or personal data are common examples of high-risk accesses. This is the type of access enterprises need to be very sure that the reviewers are paying particular attention. Flagging high-risk access is a simple way to alert reviewers to which access items need an especially closer look.

- Further, it is a good practice to Certify High-Risk Access more frequently than Low-Risk Access. To minimize risk, high-risk access should be monitored more frequently than low-risk access, and with particular care to avoid the rubber-stamp approving that can come with certification fatigue.
- Multiple phase reviews are recommended for reviewing applications & entitlements that has high-risk access.
- In any IAM platform when a reviewer an access an item for a certification, a high-risk indicators should be displayed, which helps in alerting the reviewer of the information they should consider while approving accesses.

No. 6: Use recommendations and automatic approvals

Nowadays, IAM tools come with Predictive Identity Recommendation Engine, such as SailPoint identity solutions, that use artificial intelligence (AI) and machine learning to give a deeper visibility into managing risks associated with user access. For example, when certifying access, AI-based recommendations appear as thumbs-up or thumbs-down icon to help reviewers determine whether it's safe to allow access.

Recommendations are made based on peer group analysis, identity attributes and access activity. These can help one identify outliers to the norm and therefore potential points of risk, and predictive modeling helps surface abnormal access that can be hard to identify with a manual approach. In identity services, tagging helps to flag high-risk access, so that one can identify, which access may need more frequent certification.

The recommendations engine allows the reviewers to decide whether an access request should be approved or denied. Such recommendations are based on peer group analysis and identity attributes.

No. 7: Stagger certifications to manage workload

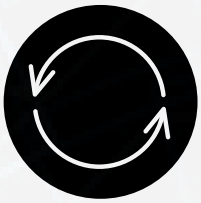
To avoid certification fatigue, it is a good practice to stagger certifications to manage workload. Consider grouping certifications by department, by population (such as specific geographies, risk profiles, or management levels), or roles, then schedule the certifications so that the workload for the reviewers is spread out in a manageable way.

- Certification campaigns can be scheduled to run on specific cadences - daily, weekly, monthly, quarterly, and yearly.
- While creating a campaign, an admin may set the deadline in IAM platform for completing the said task. Using the deadline field, admin may select a deadline for reviewers to complete their certification reviews.

No. 8: Understand what you may not need to certify

Most organizations have some kind of “birthright” access – access that every employee has simply by virtue of being an employee. An email address with an account on the company’s email system, a login to the payroll application, or a standard Active Directory account are all examples of common birthright access. In the real world, birthright access may not be so simple.

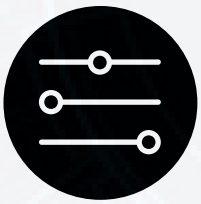
- Companies may have one set of birthright access for permanent employees, and a different set for contractors or seasonal workers.
- Different job families or departments may have unique birthright access profiles – perhaps remote workers have VPN access as a birthright, while the engineers have access to a code repository by birthright.
- Further, using Sunrise and Sunset dates can also help in managing temporary accesses. Sunrise and Sunset dates determine when access becomes active, and when it is automatically deactivated.
- Automating temporary access can be an efficient alternative to relying on certifications to remove access.



No. 9: Conduct automatic access remediation like closed loop remediations

This best practice is to ensure that access gets revoked immediately once a reviewer reviews the access and deems it not viable or required to give that level of access to the user. IAM platform should enable admins to verify remediation for ensuring that the revoked items in the campaign have been removed.

Further, archiving old certification definition is a recommended practice. Certification definition that is no longer in use should be archived, as this will be needed to show if the organization has been compliant or not and is needed to satisfy certain regulatory requirements.



No. 10: Create custom certification

Admins may create custom certifications based on different queries through IAM platform, in order to enable reviewers, certify specific users of a particular application or for fulfilling different specific compliance requirements.

Additionally, admins may trigger certifications based on certain predetermined events. For instance, a certification trigger should be generated automatically whenever a user undergoes a role or department change. Administrators nowadays have the ability to set up such custom triggers and workflows through IAM platform.

HOW AVANCER HELPS?

Enterprises need to undertake certification to review the accesses that they have provided to their users, employees, vendors and others on a periodic basis, depending on the criticality of the data accessed by the users. In order to ensure creating an accountable, compliant and holistic enterprise, Avancer's security experts help in undertaking such access certification, which includes reviewing critical applications. Our experts also aid in enhancing the accuracy of access validation, while providing a formal process for audit purposes.

Some of our clients reaches out to us from the audit failures due to Access recertification or looking for assistance in launching their Access reviews process. Based on this, Avancer is continuing to innovate newer approaches and solutions to assist our customers.

AVANCER'S EXPERTISE IN IAM

At Avancer, we understand that one of the compelling factors for organizations to bring in technical solutions is to adhere by existing compliances. However, there is so much more to technical solutions, and these add on benefits help in bringing efficiency, security and operational automation. We add an edge to solutions in Identity and Access Governance, IT Security and Big Data by closing any loopholes, and tailoring the solutions as per the needs of the business, industrial standards and regulatory considerations.

For more information on how we can make a difference in your organization, drop us a request here or directly contact our IT Security Leaders

Contact Us

Avancer Corporation

30 N Main Street

Suite 201 Cranbury

NJ 08512, USA

Tel: +1 (609) 632-1285

Fax: +1 (877) 843-8594

Email: info@goavancer.com

Website: avancercorp.com