DITY™ Weekly Newsletter
itSM Solutions®
IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself
Vol. 5.38 • September 24, 2009

6 Steps to Making Your Security Policies Work - ITIL v.3 Access Management

By Janet Kuhn

We have all been in this situation. We know that managing security is a mandate in today's IT environment, but calls are swamping the Service Desk. "I've been on vacation. I've forgotten my password." "I have a new employee starting today. She needs to be able to log into X application." "I've been promoted. How do I get Manager privileges?"

And, the dreaded "Some unauthorized changes were made. Who has access to the system?" It is like herding cats to stay current on who is who in the corporate structure, and who should have which level of authority. Access Management, one of the Service Operation processes, provides key guidance to help rein in those Security lions lying in the bushes.

One of the outstanding features in the ITIL V.3 Service Lifecycle is that it separates operational and execution activities from strategic and design ones. For example, the Service Operation volume clearly defines the boundaries around Access Management, the operational process that grants users' right to use a particular service, versus the security policies defined and established in Security and Availability Management.

ITIL V3 is adamant about it. Access Management does not define security standards; it solely and exclusively executes the Security and Availability policies and actions that are in place. As such, it performs six key activities – requesting access, verification, providing rights, monitoring identity status, logging and tracking access, and removing or restricting rights.

The following paragraphs take a closer look at each of these areas. You will see that bringing each one of these under control will help avoid the morass of issues depicted above.

#1 Requesting Access

This is an excellent place to start defining your Access Management procedures, as requests to change an access level generally emanate from only a few, well-defined areas. For instance, the Human Resources system could generate a standard request for access whenever someone is hired, promoted or transferred or leaves the company.

Other entry points for a request for access could be a Request for Change (RFC) into the Change Management System (Service Transition) or a Service Request from the Request Fulfillment System (Service Operation).

You can include the procedure for requesting access as part of the Service Catalog (Service Design).

In general, the Security policies will define which areas and departments may request access, and the Access Management process will design the mechanisms to carry out that request.

2 Verification

The verification activity verifies a request for access to ensure that the user requesting the access is who he/she says he/she is, and that the user has a legitimate requirement for the service.

There are many methods for verifying the user's identity, ranging from low-tech personal recognition to high-tech biometric data. Establishing the legitimacy of the request requires a few more verification steps. For instance, you may require the Human Resources department or the appropriate manager to co-sign requests to add new users.

The Change Management process should include a review of Access Management rights as it evaluates RFCs to specify

who should have access to the service and whether existing users are still valid.

Depending on the levels of risk to the organization, the Security policies may define different levels of verifications to access different services. For example, a request to access the banking system may carry a much higher level of verification than a request to add a new employee to the internal network.

#3 Providing Rights

Once it has verified a user, Access Management provides the appropriate rights to him/her.

However, Access Management should also be on the lookout for any role conflicts that might occur. For example, two separate accesses might be granted by different requesters to a single contract worker – one authorizing him to log time sheets for a project and the other authorizing him to approve all payment on work for the same project. In addition, large organizations may have many roles and groups, and sometimes a user may end up with mutually exclusive roles.

Access Management does not fix role conflicts or duplications itself, but it informs the originators of the access requests about the issues.

Again, the Security policy defines the rights that should be available to an individual, and Access Management grants rights based on this information. The Security team and the Access Management team must work together to build awareness within Access Management regarding potential role conflicts and mutual exclusions.

#4 Monitoring Identity Status

One of the problems with many manual Access Management systems in use today is that there is no easy way to monitor when a user changes roles or Identity Status. Typical events that trigger a change in Identity Status are job changes, promotions or demotions, transfers, resignation or death, retirement, disciplinary action, dismissals.

By identifying trigger events similar to the above, it is possible to seek Access Management tools that will automate the Access Management process and provide an audit trail.

Security policies define such trigger events, and Access Management builds ways to capture them.

#5 Logging and Tracking Access

All Technical and Application Management monitoring activities should include reviews of Access rights and utilization to ensure that the rights are being properly used. The review should direct all exceptions to Incident Management for investigation. Of course, it may be necessary to restrict the view of the Incident Record to only those people with a right to know as it could reveal vulnerabilities in the organization's security tools or policies.

Furthermore, Access Management may provide access records to assist corporate investigations into user activity.

The Security group develops the requirements for monitoring and tracking, and Access Management develops the pursuant capabilities.

#6 Removing or Restricting Rights

Users do not stay in the same jobs or roles forever, and neither should their access rights. This is another place to set up standard procedures and policies to more easily identify events requiring the removal or restriction of rights. Some examples are death, resignation, dismissal, changed user roles, and physical moves to areas with different access rights.

Based on such changes in User status or access requirements, Access Management adjusts access rights according to Security policy.

Concluding Thoughts

The key take-away from this DITY should be that Access Management holds responsibility solely for executing the security procedures that the organization's Security policies define elsewhere in the organization. As a corollary, the six activities defined above provide a solid framework for building your own Access Management implementation plan.