

Large organizations have to manage high staff mobility and turnover. Access requirements of employees and contractors change rapidly as they are re-assigned from one job to another. When users try to access something that they need to do their job, and get an “access denied” error message, they call the help desk, figure out what’s missing, and get it fixed.

In other words, processes for granting new privileges to users may not be friendly or timely, but they are always reliable. The same cannot be said of privilege deactivation. When was the last time a user in your organization called the security administration desk and asked that an old ID or group membership be removed? In reality, users may forget that they have the old privilege, may not understand the security infrastructure or may simply hoard old privileges, “just in case.”

The net result of unreliable and/or untimely access termination processes is that users accumulate inappropriate security rights.

The obvious artifacts of privilege accumulation are orphan accounts, whose owners have left the organization and dormant accounts, whose owners haven’t signed on in months or years. More subtle effects include inappropriate privileges on systems that users do still log into, and violations of policies regarding separation of duties or access to sensitive data.

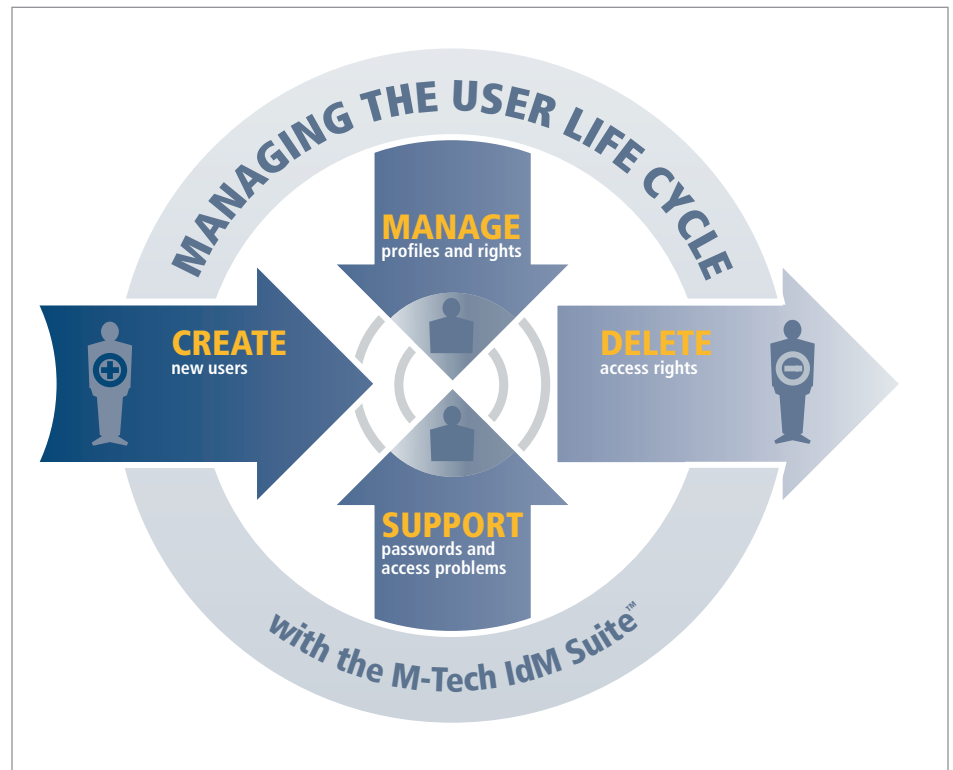
Until recently, many organizations were reluctant to invest in timely and reliable access termination processes, due to cost and complexity. Today, regulations such as SOX, HIPAA, the EU Privacy Directive and others have changed that: all these rules call for stronger internal controls, which includes timely and reliable processes to terminate inappropriate user rights.

### Solution Approaches

One approach to access termination is to develop a privilege model, using roles and rules, to predict what rights every user should have. It is then possible to measure variance between the model and reality, and either clean up privileges or document and approve exceptions.

Privileges models can be complicated to implement and maintain, so planning is essential: Who will develop the privilege model? How long will it take? How much will it cost? Who will maintain the model? This is a large project, likely taking person-years to implement and multiple skilled FTEs to maintain.

A simpler approach is to engage the user community to find out what’s appropriate and what’s not. Every manager can be invited to look over a list of her direct subordinates and spot



When do users lose old privileges? This might seem like a simple question, but in a large organization, the answer is probably anything but.

# Addressing OUTDATED USER PRIVILEGES

those who no longer work for the organization. At a more fine-grained level, managers can review their subordinates’ accounts and security rights, accepting most as appropriate and flagging the few exceptions for further review and deletion.

In practice, large financial institutions have been using managerial access reviews for years.

This approach can be extended to other kinds of stake-holders. Application or data owners can perform a similar review, so long as the number of users within their scope of authority is reasonable. Pharmaceuticals have asked application owners to perform micro-audits of clinical systems for years.

By engaging the user community, stale privileges can be identified and removed in months, not years. In fact, this process may well precede a role engineering project, as a way to scrub the data, to make role mining easier.

### ID-Certify

Engaging stake-holders to review and clean up user privileges is exactly what M-Tech automates with its ID-Certify product.

*Idan Shoham is the CTO of M-Tech.*

To learn more about ID-Certify, please visit: <http://ID-Certify.com>. To learn more about M-Tech and our suite of identity management products, please visit: <http://MTechIT.com>.