

Identity and Access Management: Employee Lifecycles and Roles



HR departments can play a vital role in maximising the effectiveness and value of employee Identity and Access Management systems

Whilst many information security strategies have traditionally been based on a 'Keeping the bad guys out' paradigm, Identity and Access Management (IAM) approaches the subject from the opposite direction and focuses on how to securely let business *in* by controlling application access to internal employees, external customers and business partners.

Identity and Access Management systems seek to achieve this objective by combining two distinct sets of functions:

- *Identity Management* encompasses a broad, administrative area that deals with identifying individuals (identities) and controlling their access to resources, services and systems
- *Access Management* defines the sets of rules required to control and allow individual access to internal or external systems.

By integrating these functions, IAM systems allow organisations to introduce substantial improvements to security controls, achieve efficiency and budget savings, maintain data quality and, importantly, meet obligations to industry and regulatory compliance requirements.

Human Resources (HR) can play a vital role in the enablement of effective employee IAM solutions by utilising existing HR functions to provide benefits such as tighter application security, privilege entitlement and rapid user provisioning and de-provisioning.

Introducing an HR-led, role-based employee IAM solution can also help businesses to reduce administrative overheads, streamline business processes and help further enforce security policies for their IT systems. But are HR departments aware of these benefits?

Life-cycle management

Just like other business units, HR departments today face a range of operational challenges. Increasing the range and quality of services to employees at the same time as reducing operating costs are typical. Many are also tasked with meeting the changing, increasing demands – and expectations – of a diverse customer population that includes job applicants, new hires, contractors, management and retirees.

To help meet these demands, most HR systems today afford integral life-cycle

management capabilities that help businesses support employees through every phase of their service within the organisation – from recruitment through training, development and staff retention.

Some HR systems understand the concept of business roles and associate specific functions to them. A role is typically related to a job or business function within an organisation or a business relationship. Examples include Administrator, Sales Manager or Engineer.

An employee can then be associated to one, or more than one, business role throughout their employment. These would include changes in business roles, moves to different departments and promotion or demotion.

Most HR systems, however, consider roles as merely a one-to-one mapping to an employee's job title and never consider the value that they can introduce to other areas of the business.

implementing a comprehensive IAM solution. But is there a natural linkage between what HR know about an identity/role, and what electronic or asset resources and privileges that identity/role should have?

Life outside HR

A typical scenario that occurs in many companies starts when employees enter the HR system. A manual process or paper chase then commences whereby manual provision of desktop logins, server space, laptops, files systems, etc, is initiated. Employees eventually get the resources they require to fulfil their roles.

What then tends to happen, as *Figure One* depicts, is that as more life-event changes occur within HR, employees and non-employees never lose their electronic privileges (eg. open user accounts, group memberships) and assets (eg. mobile phone) when they should.

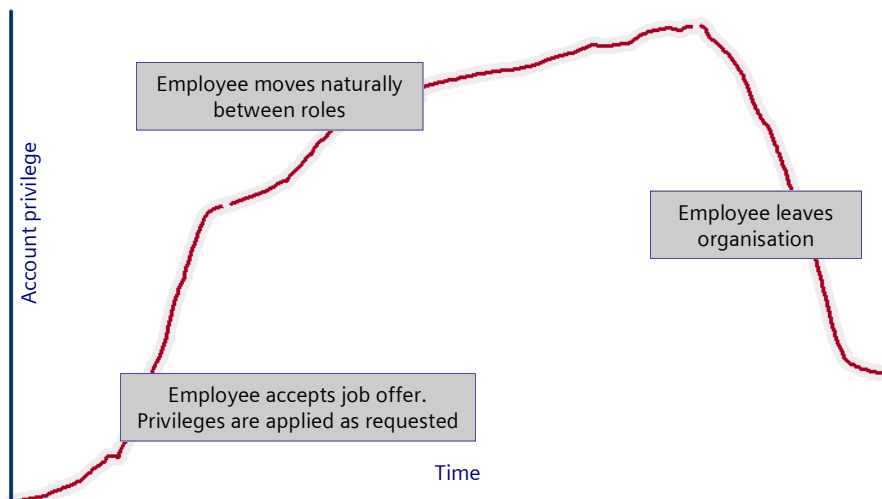


Figure One: Current Employee Life-cycle – Access to Accounts

HR systems can also distinguish between real employees and contractors. This is sometimes represented in a field called employee-type and has values of *employee* and *non-employee*.

Life-event changes

HR systems frequently support life-event or status values as well. Examples include *present* or *active* for current, employed personnel and, for those that have left, values of *removed* or *inactive*.

Picking up on these employee life-event changes, employee types and associated business roles is extremely useful when

In practice, an employee often gains more and more privileges throughout their corporate life and only ever relinquishes them (but not necessarily all) once they have left the organisation.

This results in many issues including:

- Open access to privileges that the user may no longer require
- Orphaned accounts in target systems
- Administrative overhead in cleaning up systems
- Assets not returned when users no longer require them

- IT roles and permissions have no relation to HR roles
- Difficulty in determining a common provisioning policy for employees and contractors.

By introducing an effective IAM solution based upon these HR events and role values, organisations can quickly eradicate a lot of the inefficiency in the current hand-off between HR and IT departments.

HR and IAM hand-in-hand

Role-based Access Control (RBAC) is the preferred solution for cross-platform access management. Since many employees need the same, or similar, authorisations to perform their tasks, this considerably reduces administration effort.

RBAC is a reference model for designing access control systems using a role-based approach and which adopts the following concept:

- Users are assigned roles based on their responsibilities in the organisation
- Roles are mapped to IT system-specific tasks through permissions
- Permissions comprise access modes and operations to one or more system resources.

Thus, through the chain *user–role–permission*, the user gains the access rights to system resources that are needed to perform the job function modelled through the role.

This use of roles permits access rights to be administered in business terms rather than in IT terms. Consequently, access management can be performed by people who understand which roles are necessary for a user – such as HR personnel – rather than by technical IT staff. This role-based approach to privilege management allows for the separation of user administration and access rights administration.

User administrators only need to know the users' roles (their job functions) – they do not need to know about each role's permissions and rights on the organisation's IT systems. Conversely, role administrators define permissions and IT system rights for each role - they

do not need to know which users actually have which roles.

Because roles evolve from business semantics, they are not limited to specific IT systems, but have a cross-platform meaning that combines users and permissions in many systems.

Using business semantics as the basis for granting access rights allows organisations to abstract away from a particular IT system's access model. Roles are derived from business processes in a top-down fashion. And, because they are based on business processes, they are not as likely to change as frequently as users do.

Role Hierarchy

A role can represent a single task in a business that has specific access rights. However, it is also useful to build roles that correspond to a user's job description, which can consist of many tasks. Some systems also support the concept of role hierarchies, where roles that correspond to job descriptions can, in turn, contain roles that correspond to single tasks and *aggregate* their access rights.

Senior roles with extended rights can be defined on the basis of existing roles. A hierarchy of junior roles and senior roles can be defined where the senior roles aggregate the permissions of their assigned junior roles. In this way, basic roles can be defined and used in more complex roles. This hierarchy helps to maintain clarity in the structure of roles and to simplify role assignment.

Employee Life-Cycle Scenario

A typical employee life-cycle scenario includes a number of distinct stages as described below:

Joiner: Steve joins Company X and is granted the role *Manager*. Within the role catalogue, the *Manager* role is allowed the permissions: application, desktop login, email account and access to the sales database. Based on his HR life-event status (eg. *active*), Steve will automatically be granted access to the appropriate systems.

Mover: Steve moves from the *Manager* role to the *Sales Manager* role. This automatically grants him additional privileges. Based on the role catalogue,

Steve could also lose other previously subscribed rights automatically.

Sabbatical: As Steve is on sabbatical for six months, he no longer needs access to resources. These should not be removed, however – simply locked to ensure access security.

Leaver: When Steve leaves the organisation, all accounts owned by him are immediately and automatically locked and removed at a later date. This enforces any security policy in place and prevents Steve from maliciously accessing those resources.

The key to map this example scenario to a business is as follows:

- Document and use the employee HR life-cycle as a trigger for creating and removing operations within the IAM space
- Document and use the employee HR life-event as a trigger for locking accounts that should not be open
- Document and use the employee HR roles within HR to build a role catalogue which can be used to assign and remove privileges (IT and non-IT).

Recommendations

For those currently thinking about implementing an employee IAM solution, the following recommendations – which are not exhaustive – will allow organisations to leverage existing HR business process to achieve successful project realisation:

- Gain HR buy-in from the start of any IAM project. The HR life-cycle process is key to effective employee Identity and Access Management
- Understand the HR life-cycle model including life-event and integrate this into the IAM solution – eg. simple *transparent* provisioning can be provided for all employees and *approval* provisioning for non-employees
- Look at mapping business roles to IT resources and assets either through role-mining or role-engineering to construct a role catalogue
- Introduce simple roles to start with, eg. employee and non-employee and assign common privileges to these roles
- Consider what resources may require approval, and those that do not, and build these into the role catalogue
- Consider introducing non-IT related resources, eg. assets into the role-permission model.

Employee IAM solutions need to identify the authoritative source for identity information. This is typically found within an HR department along with other useful data such as employee types, status values and role information.

By obtaining HR buy-in at the beginning of the project, and leveraging HR life-cycle and life-events, this can significantly reduce an IAM project life-cycle as the data and structures that are already used within the business can be re-used.

Key facts

- Many HR systems afford integral life-cycle management capabilities that can be integrated with IAM systems
- Role-based models ensure users only gain access rights to system resources that are needed
- Complex roles can be created by aggregating more basic roles
- IAM systems can help return assets no longer required when employees change roles or leave organisations

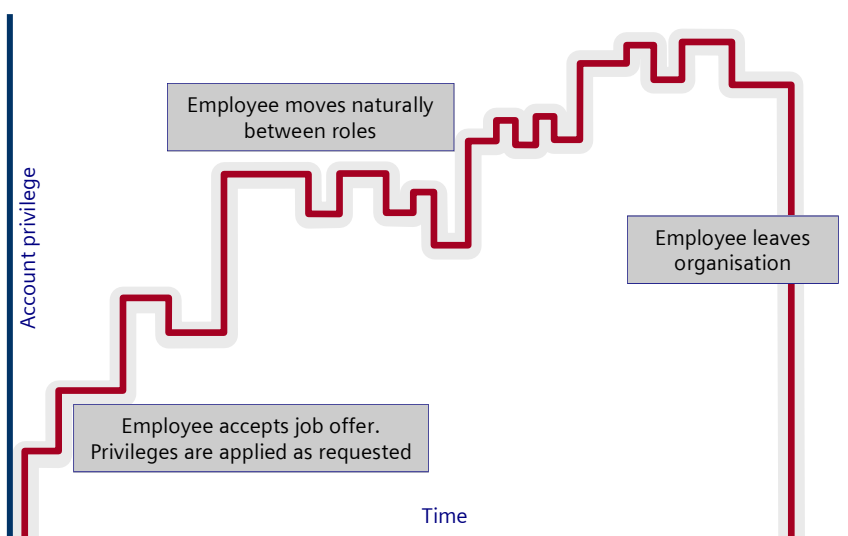


Figure Two: Role Based Access Management – Access to Accounts