

# Identity Management: Bringing the People Component to ITIL

This article appeared in *"INNOVATION: The Convergence of Information Technology and Business,"* published by BMC Software.



To receive a copy of *INNOVATION: The Convergence of Information Technology and Business*, go to [www.bmc.com/innovation](http://www.bmc.com/innovation).



## **Identity Management: Bringing the People Component to ITIL**

**By Rami Elron**

*Identity Management Worldwide Enablement Manager, BMC Software*

**Ken Turbitt**

*Global Best Practices Director, BMC Software*

**Christopher Williams**

*Identity Management Consultant*

The number of companies adopting IT Infrastructure Library (ITIL®) guidelines continues to grow as business leaders recognize the value of using best practices to improve IT service levels, reduce costs, increase business agility, and demonstrate regulatory compliance. ITIL speaks to a broad range of IT disciplines, including incident, problem, change, release, and configuration management, as well as IT service continuity and security management.

The latest release of ITIL, version 3, now has security and access management, which reflects identity management activities and processes. It focuses on the people component of the IT environment. As a result, many practices within identity management intersect directly with ITIL disciplines. This level of synergy is undeniably strong. Identity management solutions maintain comprehensive information about users, which can be leveraged to support ITIL processes. Organizations that integrate identity management solutions with applications to support ITIL processes are finding that ITIL best practices are easier to implement. They are also discovering that the resulting environment delivers far greater efficiency than would be possible without this integration.

### **What Identity Management Brings to the Table**

An identity management system manages the entire lifecycle of digital identities and maintains a wealth of user information — the user's role in the enterprise, access privileges to enterprise applications, authentication data, and more. Through such a system, IT can implement, enforce, and audit identity-related procedures in accordance with business policies. That aligns directly with the central role of ITIL, which is to provide greater efficiency through standardization of process and nomenclature.

**Organizations that integrate identity management solutions with applications to support ITIL processes are finding that ITIL best practices are easier to implement. They are also discovering that the resulting environment delivers far greater efficiency than would be possible without this integration.**

Identity management and ITIL disciplines are tightly intertwined. Their relationship is especially evident in change management and the related release and configuration management disciplines. To understand this concept, let's look at the intersection of identity management with change, release, and configuration processes.

### **Incorporating Best Practices**

Improperly planned or poorly executed changes cause disastrous system outages in many organizations. Improperly planned changes can also lead to noncompliance with government mandates. To prevent this, businesses must implement and enforce best-practice processes for change, release, and configuration management. Identity information is a necessary ingredient for each.



It is an important imperative to ensure that only authorized people approve and implement changes, and that people approve and implement only those changes for which they are authorized. Change privileges are based on an employee's role — and it's the identity management system that maintains role information. The change management application can use role information to determine who is authorized to approve and implement changes. It can also use the information to create an audit trail that indicates who approved each change and when, as well as who implemented each change and when. This auditing capability enables accurate and timely regulatory compliance reporting.

Identity information also gives the change management team visibility into who uses which applications. With this insight, the team can easily determine who will be affected by planned changes to critical business applications, notify them in advance, and keep them informed of change status.

**Change privileges are based on an employee's role — and it's the identity management system that maintains role information.**

Finally, identity information enables the configuration management application to ensure that only standard configurations, based on employee roles, are deployed in client machines. Operating in concert with automatic discovery tools, the configuration management application can determine the configurations of client machines and compare them with standard configurations to uncover inconsistencies. The application can also restore the offending machines to standard configurations by triggering the change management application to reprovision the machines with the appropriate software.

**Facilitating Automatic Provisioning**

The user base in most organizations changes continually as employees come on board, change roles, and leave. In response, IT must provision new and reassigned employees with properly configured client computers and appropriate access to enterprise applications, and must also deprovision terminated employees. In a large organization, the number of changes each day can be in the thousands. By integrating identity management with ITIL change and release processes, the IT organization can automate provisioning, saving valuable staff time and ensuring greater accuracy.

Here's an example of an automated approach: The entry of a new employee record in the human resources (HR) system is detected by the identity management system, which, based on configurable policies, determines the appropriate employee data, including role and group membership, and adds it to the identity database. The identity management system subsequently provisions user account data (corresponding to the new employee) to each system. This is where the employee may be granted access rights, and the change management system is triggered to initiate change processes associated with the event. The change management application, in concert with the release management application, allocates and provisions a client computer with the appropriate software and access to applications. Corporate policies based on the employee's role in the enterprise guide the provisioning task.

**By integrating identity management with ITIL change and release processes, the IT organization can automate provisioning, saving valuable staff time and ensuring greater accuracy.**

Likewise, when an employee is reassigned or leaves the company, an update to the HR system is detected by the identity management system. This system, which is based on configurable policies, determines how to deprovision employee-related data. As a result, the employee's ability to gain access to system resources is disabled. Additionally, the identity management system prompts the change management application to initiate any actions determined relevant to this event.

Visit [www.bmc.com/idm](http://www.bmc.com/idm) for more information.

### **Final Thoughts**

While ITIL does not specifically address identity management, ITIL processes and identity management are tightly intertwined. Integrating an identity management solution with ITIL process management applications leverages the strong synergy between them. The result is increased process automation and effectiveness, which delivers business benefits well beyond those that ITIL process management applications and the identity management solution could deliver individually.



#### **About the Author**

*Rami Elron, identity management worldwide enablement manager, BMC, is responsible for design aspects of the BMC Identity Management solution, including the solution's next-generation architecture and features.*



#### **About the Author**

*Ken Turbitt is the global best practices director for BMC. He is focused on best practices for IT services, such as ITIL, COBIT, and eTom, among others, and presents this information to clients, partners, and analysts. Turbitt has held an ISEB ITIL Manager/Masters qualification for more than 12 years and has been a Gartner-qualified TCO consultant for more than 10 years.*



#### **About the Author**

*Christopher Williams, identity management consultant, has been associated with IT organizations for the past 25 years in a variety of industries. He currently works with consulting firms on ITIL-related computing disciplines.*