



Leveraging the Synergy between Identity Management and ITIL Processes

Ken Turbitt, best practices director, BMC Software

Rami Elron, senior system architect, Identity Management, BMC Software

Chris Williams, director, Consulting Services, ILANTUS Technologies

Table of Contents

- EXECUTIVE SUMMARY 1

- IDENTITY MANAGEMENT BUSINESS CHALLENGE 2
 - The Importance of Federation 2

- INTEGRATING ITIL PROCESSES WITH IDENTITY MANAGEMENT 3
 - ITIL Overview 3
 - Service Desk 3
 - Incident and Problem Management 3
 - Change, Release, and Configuration Management 4
 - IT Service Continuity Management 5
 - Security Management 5

- A FOUNDATION FOR INTEGRATION..... 5

- CONCLUSION 6

Executive Summary

Businesses today are striving to manage IT from a business perspective to improve service, reduce costs, increase business agility, and achieve regulatory compliance — all while protecting profits. To help them in this quest, they are turning to standardized industry frameworks of best practice processes. One of these frameworks, the IT Infrastructure Library (ITIL®), has been adopted by companies interested in applying best practice IT processes. At the same time, identity management solutions are providing companies with convenient, yet controlled, access to IT resources by people inside and outside the organization — employees, business partners, and customers.

There is a strong synergy between identity management and ITIL processes. Identity management solutions maintain comprehensive information about users that can be leveraged to support ITIL processes. By integrating identity management solutions with applications that support ITIL processes, an organization can facilitate and enhance the implementation of ITIL.

This paper:

- > Provides overviews of identity management and ITIL
- > Examines the synergy between identity management and ITIL processes, focusing on those ITIL processes most relevant to identity management
- > Describes an approach to integrating identity management solutions with applications that support ITIL processes
- > Discusses the business value this approach delivers

Identity Management Business Challenge

IT must permit access to IT resources to users who reside both inside and outside the walls of the organization — employees, business partners, and customers — at any time, from anywhere. At the same time, IT has to maintain tight control of that access by:

- > Preventing unauthorized people from gaining access
- > Permitting authorized people to access only the assets they are authorized to use
- > Permitting access only at the user's authorized access privilege level, such as "read-only" or "read/write"

A major requirement is that user authentication must not be intrusive or it will adversely impact productivity. Providing convenient, yet controlled, access presents a challenge. There are many users who need access, especially in large organizations. Some of these users, such as business partners in the supply and distribution chains, are outside the walls of the organization, but still require access to sensitive information. There are also a large number of IT resources, many of which are often distributed worldwide. Some may even be located outside the walls of the organization. What's more, the user base is in a constant state of flux, and the IT infrastructure changes continually as components are added, updated, or removed.

As if that weren't enough, IT has to ensure that access control meets internal policies and external regulations. That requires IT to be prepared to answer such questions as:

- > Who are the users?
- > Who has access to what?
- > Who approved that access?
- > How is that access being used?

Answering these questions requires comprehensive monitoring, logging, reporting, and auditing. IT can no longer rely on traditional user account management processes, as they are cumbersome and introduce delays. In addition, they are error prone, costly, and difficult, if not impossible, to audit. What the IT staff needs is a comprehensive, system-based identity management solution. This solution should provide a single system of record that understands who users are, the resources they should be able to access and when, and the type of access they should have.

Identity management encompasses the processes, practices, and tools utilized to govern the complete lifecycle of digital identities. It combines access authentication, access administration, and access auditing. Identity management provides the means for modeling, implementing, enforcing, and auditing identities and identity-related procedures in accordance with business policies. A well-designed solution provides a number

of important capabilities that facilitate business management, simplify administration, and improve user experience. That solution offers:

- > *A comprehensive, consolidated view of users* that encompasses people both inside and outside the organization and permits IT to answer the question "Who are the users?"
- > *Access management across the enterprise* that enables IT to control and enforce access privileges from a central point, permitting IT to answer the question "Who has access to what?" It also allows IT to delegate access control to responsible groups, permitting these groups to retain control of authoritative data sources.
- > *Automated user administration and provisioning* that facilitates security management (primarily through automated rule-based and role-based management of user accounts on enterprise systems), thus reducing errors and lowering administrative costs. These capabilities also maintain information about user relationships, roles, and access rules that can be leveraged to drive automated IT processes.
- > *Automated password management* that permits IT to define and enforce password policies, minimize the number of passwords users have to remember (through mechanisms such as password synchronization and single sign on), and allow user self-service in such areas as password change.
- > *Audit and compliance management* that automatically monitors, logs, and reports access events and generates appropriate notifications, including automatic notification of suspicious activities. It also maintains an audit trail to validate compliance, permitting IT to answer the question "How is that access being used?"

To deliver these capabilities, an identity management solution must maintain comprehensive information about users — their locations and roles; their relationships to IT resources, such as desktop and laptop computer configurations; authentication information, such as IDs and passwords; and access privileges to enterprise applications and data.

The Importance of Federation

A well-designed identity management solution supports federation. In the context of identity management, federation involves a combination of processes, agreements, and technologies that together facilitate management of identities across separate security domains.

Federation brings important capabilities to identity management. It permits federation of the management of identity data within an enterprise, data that may reside in multiple diverse sources, such as network directories, applications, and management systems. It also permits federation of the management of identities across security domain boundaries by establishing trust relationships among multiple enterprises.

Federation delivers significant advantages. It facilitates the implementation of the identity management solution, facilitates interaction between independent parties, and permits delegation of authority to allow responsible groups to retain control of authoritative data sources, while still making the data available to the identity management system.

Integrating ITIL Processes with Identity Management

Identity management deals primarily with the people component of the IT environment, while ITIL focuses on the process component. ITIL provides a framework of best practice processes that ensures delivery of high-quality business services. Although ITIL does not deal specifically with identity management, it does have a focus on the people component of the IT environment. As a result, many of the practices within identity management directly intersect with ITIL disciplines.

This section briefly describes ITIL and how an organization can leverage an identity management system to support ITIL processes. The section focuses on those ITIL processes most relevant to identity management.

ITIL Overview

ITIL provides a comprehensive, consistent, and coherent framework of best practices for IT processes. It promotes a quality approach for achieving business effectiveness and efficiency in the use of information systems.

First developed in the 1980s by the Office of Government Commerce (OGC), a branch of the British Government, ITIL has become a de facto standard worldwide as organizations adopt it as their framework for establishing IT processes. What's more, ITIL adoption is the foundation of ISO 20000, which is now an international standard for service management.

ITIL consists of many books, seven of which are considered core books. These core books define seven sets of processes covering seven different IT areas: ICT Infrastructure Management, Applications Management, Service Support Management, Service Delivery Management, Business Perspective, and Security Management. Two areas deal specifically with IT Service Management:

- > Service Support — Service Desk, Incident Management, Problem Management, Change Management, Configuration Management, and Release Management
- > Service Delivery — Service Level Management, Capacity Management, Availability Management, Financial Management for IT Services, and IT Service Continuity Management

Many ITIL processes can benefit significantly from integration with an identity management system. Of special interest

are those processes in the ITIL Service Support, Service Delivery, and Security areas.

The applications that support ITIL processes can leverage the people data maintained by the identity management system to enhance ITIL processes. In addition, integration of ITIL process management with identity management can enhance IT process automation by enabling bidirectional interaction between ITIL process management applications and the identity management system.

The following examples illustrate the synergy between identity management and IT processes.

Service Desk

The service desk is typically the first point of contact for users. The service desk application can leverage the comprehensive, consolidated user view made available by the identity management system to provide service desk agents with a wealth of people-related information that facilitates and speeds response when users call.

- > *User entitlement.* Quickly determine the user's entitlement to service, knowing right away, for example, if a user is calling with an issue on an application that he or she is not authorized to access.
- > *User role.* Distinguish between employees, business partners, and customers; tailor responses accordingly; and quickly identify senior management users for appropriate business impact response.
- > *Status of entitled services.* Immediately see the services to which a user is entitled and quickly determine the status of these services or if other users have reported problems against these services. This information can help speed incident resolution or forwarding to Problem Control.
- > *Source of support.* Determine who supports the IT resource in question and immediately and seamlessly transfer the user to the proper support source, such as the internal help desk, second-tier support, or an external service supplier's help desk.

Incident and Problem Management

Through integration with the incident and problem management application, the identity management system can provide the same comprehensive user information to the support technician as it does to the service desk agent. In addition, the incident and problem management application can use the identity information to determine the configuration of the user's client computer and automatically populate the relevant fields on the technician's screen. This saves time for the support staff and speeds incident and problem resolution.

Furthermore, bidirectional integration of the identity management system with the incident and problem management application enables the incident and problem management application to move automatically and proactively to address events occurring in the IT environment.

Here's an example:

- > The event management system receives six events in which six different user IDs have failed password authentication — all in a span of just a few minutes.
- > The event management system correlates these events as indication of suspicious activity and automatically generates an incident ticket to the incident and problem management application.
- > The incident and problem management application interrogates the user data in the identity management system and determines that all six attempts have been made by the same person (or have come from the same IP address), indicating that some sort of attack may be underway.
- > As a result, the incident and problem management application immediately triggers the identity management system to revoke that person's access to all IT resources (if the preset rules dictate this). This automated, immediate response strengthens protection of the IT infrastructure against malicious attacks.

Change, Release, and Configuration Management

People-related information is especially important in change management, release management, and configuration management, and it plays a key role in change authorization, change notification, user provisioning, standard configuration enforcement, and service continuity management.

Change Authorization

The following controls are essential for change authorization to ensure compliance with corporate policy and government regulations:

- > Only authorized people should be permitted to approve and implement changes to the IT infrastructure.
- > Authorized people should be allowed to approve and implement only those changes that they are authorized to approve or implement.
- > One person should not be able to both approve and implement a change.

An identity management system maintains the link between people and their change approval and implementation privileges. The change management application can leverage this information to control changes. The application can also maintain an audit trail showing which person approved each change, who implemented it, and when it was approved and implemented.

Change Notification

In many cases, especially when changes affect critical business services, the change management staff must notify affected users of planned changes and keep these users updated on change status. An identity management system maintains the links between people and the resources they are authorized to access. The change management application can leverage this information to automatically notify affected users.

Automatic Provisioning

The user base is in a continual state of flux as new employees come on board and current employees change roles or terminate their relationships with the organization. This situation also applies to employees of business partners. These types of changes require provisioning or reprovisioning of IT resources, such as client computers and access to enterprise applications and data.

Equipment configurations and access privileges vary widely based on the user's role in the organization. An identity management system maintains the links between people and their roles. Change management and change release management applications can leverage that information to automatically provision or reprovision equipment and access privileges to users.

Here's an example:

- > A new employee joins the company and is entered into the HR system. This change triggers the identity management system to add the employee and his or her attributes, such as role and group membership, to the identity management data.
- > The identity management system generates a change request to the change management system to provision the new employee.
- > The change management application, in concert with the release management application, automatically provisions the appropriate resources based on the employee's role. This involves allocating and provisioning a client computer with the appropriate software, as well as with access to enterprise applications and data.

Likewise, when an employee changes assignments or leaves the organization, a change is entered into the HR system, triggering a change to the employee's role information in the identity management system. In response, the identity management system generates a change request to the change management application to reprovision the newly assigned employee or deprovision the terminated employee. In the case of a reassignment, the change management application reprovisions the employee according to the employee's new role as defined in the identity management system.

In the case of a termination, the identity management system immediately deprovisions the employee and terminates the employee's access to enterprise applications and data.

Enforcement of Standard Configurations

The configuration management application continually monitors the configurations of IT resources, including client computers, and identifies configurations that deviate from the standard configurations. When the configuration management application finds a resource that is out of compliance, it can restore it to the standard configuration. For example, assume an employee has installed an unauthorized game on a desktop computer. When the configuration management application detects the variance from the standard, it determines the appropriate configuration based on the employee's role as defined in the identity management system. The application can compare the current configuration to the appropriate standard configuration, identify the unauthorized game program, and uninstall the offending software, returning the client machine to standard configuration.

IT Service Continuity Management

When a failure occurs, the identity management system can provide information to the change management application to permit automatic reprovisioning of all users who need access to the resource. Automatic reprovisioning assures that users can access the failed resource as soon as it is restored to service. For example, when a server running a critical business application fails and is then restored to service, the event management application generates a change request to the change management application to reprovision access to all affected users. The change management application determines, through the identity management information, which users to reprovision and at what access privilege level. It then reestablishes all appropriate user accounts on the server.

Security Management

Identity management helps organizations address salient requirements warranted by ITIL Security Management. Identity management:

- > Helps in the attainment of various lifecycle-related objectives — from allocation of responsibilities and setting up service level agreements to ensuring effective control of access rights and compliance with policies.
- > Provides the means to address requirements associated with phases identified in ITIL Security Management, such as accountability of information assets, segregation of duties, effective authentication, control of access rights, and compliance with policies, regulations, and laws.
- > Provides comprehensive reporting and analysis capabilities that address auditing, evaluation, and documentation requirements. These capabilities, which can be used to

highlight, assess, and convey important data concerning security management activities, are essential for a comprehensive, effective security process.

Identity management systems provide a comprehensive solution to the management of digital identities within and across security domains, thus enabling the ability to facilitate, enforce, and assess adherence to standard processes involving access to resources. Such processes imply access permissions on data that should be appropriately assigned, and are also likely to warrant associated workflow processes, which need to be defined, implemented, enforced, and monitored. This approach is directly in line with the central theme of ITIL, which is greater efficiency through standardization of process and nomenclature.

The ability of a well-designed identity management system to facilitate interaction between independent parties, while still ensuring information security, can be illustrated with an example from the healthcare industry. Here, a patient's medical data must be shared by a variety of people in different organizations, while also protecting the patients' privacy in accordance with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

In this example, a private physician refers a patient to a hospital for medical services. The physician's staff accesses the patient's insurance data to clear him for hospital admission. As the patient is moved to different treatment locations in the hospital, the various attending physicians and laboratory technicians access and update the patient's health data. When the patient has completed treatment, the hospital business staff enters data to complete the insurance adjudication process and conclude the financial business transaction. Through all these access points, the identity management system enforces standard processes, permitting only authorized people to access the patient's data and limiting that access to authorized privilege levels.

A Foundation for Integration

One of the key aspects of ITIL is the integration of IT processes both within and across IT disciplines. Solutions are available today that provide this integration out-of-the-box through ITIL-compatible applications. This integration enables IT to streamline IT service management processes. For example, when the event management application is integrated with incident and problem management, it can automatically generate incident tickets to the incident and problem management application. The tickets can include rich contextual information to help speed resolution.

The foundation for integration is typically a configuration management database (CMDB). The CMDB is a fundamental component of the ITIL framework. It serves as a single source

of reference, facilitating integration and synchronization among ITIL management processes, all of which contribute and consume CMDB information.

The CMDB defines a set of configuration items (CIs) and can maintain all IT resources — technology assets, processes, and people — as CIs. For technology assets, it maintains such details as their configurations and their physical and logical relationships. Automatic discovery tools can perform the initial population of the CMDB with technology asset CIs and their physical and logical relationships. This facilitates CMDB implementation. Discovery tools also continuously scan the IT environment to keep the CMDB up to date, ensuring accurate representation of the IT environment.

A CMDB based on a federated architecture enables the creation of a single, logical data store that can reside on multiple data sources. These sources can be located internally within the organization, as well as externally with business partners or other stakeholders.

Just as it provides a point of integration for ITIL process management applications, the CMDB also provides a point of integration between the ITIL process management applications and the identity management system. Integration permits ITIL processes to leverage identity data.

Integration of ITIL process management applications with the identity management system implies the addition of certain identity-related data to the CMDB. It is advisable to include only core identity data in the CMDB. Core information provides a comprehensive view of all people who have access to IT resources, including their organizational alliances, their roles, and their relationships to the IT resources to which they have access. Maintaining only core information in the CMDB keeps it manageable, and still enables the ITIL process management applications to access any additional identity data they need from the federated identity management system. Although the CMDB does not contain all the information directly, it can point applications to that information.

Automatic discovery tools are available that populate the CMDB with core identity information by accessing it from the identity management database. These tools can also keep the CMDB updated as changes in identity-related data occur.

Conclusion

ITIL process management applications and identity management solutions each deliver compelling business benefits on their own. ITIL process management applications enable organizations to align IT more closely with the business for improved service, reduced costs, and increased business agility. An identity management solution automates and streamlines the process of provisioning people with proper and tightly controlled access to IT resources, increasing user productivity and reducing administrative costs. Both ITIL process management applications and identity management solutions help ensure regulatory compliance, and facilitate IT governance.

Integrating identity management solutions with ITIL process management applications leverages a strong synergy between them. ITIL process management applications can leverage identity data and interact with the identity management system to enhance IT processes in a variety of ITIL areas, including service desk, incident management, problem management, change management, release management, configuration management, IT service continuity management, and security management. The result is increased process automation and effectiveness, which significantly amplifies the business benefits delivered individually by the ITIL process management applications and the identity management solution.

BMC Software and BMC Partner ILANTUS Technologies offer solutions that address the identity management and ITIL issues discussed in this paper. For more information about ITIL and identity management, visit:

www.bmc.com/itil for ITIL information from BMC

www.bmc.com/idm for BMC® Identity Management information

www.ilantus.com for information on identity management solutions from ILANTUS



ACTIVATE BUSINESS WITH THE POWER OF IT.™

About BMC Software

BMC Software delivers the solutions IT needs to increase business value through better management of technology and IT processes. Our industry-leading Business Service Management solutions help you reduce cost, lower risk of business disruption, and benefit from an IT infrastructure built to support business growth and flexibility. Only BMC provides best practice IT processes, automated technology management, and award-winning BMC® Atrium™ technologies that offer a shared view into how IT services support business priorities. Known for enterprise solutions that span mainframe, distributed systems, and end-user devices, BMC also delivers solutions that address the unique challenges of the mid-sized business. Founded in 1980, BMC has offices worldwide and fiscal 2006 revenues of more than \$1.49 billion. Activate your business with the power of IT. www.bmc.com.

About ILANTUS

ILANTUS Technologies is a leading global provider of identity management solutions. Now in its seventh year of operations, the company has executed more than 150 projects and serves a number of Fortune 1000 companies, including Capital One, ANZ Bank, CMS, Conoco-Phillips, Fifth Third Bank, Citibank, Singapore Press Holding, and Cognizant Technology Services. The projects have involved deployment of identity management solutions in a variety of industry verticals, including banking, insurance, financial services, telecom, government, pharmaceutical, healthcare, manufacturing, retail, and software. ILANTUS is an Intel-funded organization with offices in the U.S., U.K., Singapore, Australia, and India.

About the Authors

Ken Turbitt, best practices director for BMC, has broad experience in best practices management, IT, and consulting. He has held an Information Systems Examination Board (ISEB) ITIL Manager/Masters qualification for more than 10 years, and was a Gartner-qualified TCO consultant.

Rami Elron, senior systems architect for BMC, has more than 15 years of leadership experience in computing infrastructure and development environments. He is responsible for the design of BMC security solutions and next-generation architecture. Elron has received several industry awards, lectured in numerous industry events, co-authored a book on Windows XP, and is a member of the Organization for the Advancement of Structured Information Standards Provisioning Services Technical Committee (OASIS PSTC), the organization that created the Service Provisioning Markup Language (SPML) standard.

Christopher Williams, director of consulting services for ILANTUS Technologies, has been associated with IT organizations for the past 25 years in a variety of industries. Currently he manages the ILANTUS North American Identity Management practice. Prior to joining ILANTUS, Williams was with BMC for nine years, serving the Identity Management Business Unit as software consulting manager, marketing manager, identity management specialist, and a member of the Thought Leadership Council for regulatory compliance.

