



Finding the route to value with Identity Management

A Datamonitor whitepaper commissioned by BMC

Identity Management has become a must-do function of the overall business service management approach: allowing businesses to improve security, reduce their system administrators' workload, increase user productivity and meet strict regulatory compliance.

Creating a comprehensive Identity Management structure is a big task, however, and few organizations know where to begin and how value can be quickly achieved. This white paper looks at how clear 'routes to value' can help businesses achieve their individual goals within a more acceptable timeframe.

Publication Date: 12/04

www.datamonitor.com

Datamonitor USA

245 Fifth Avenue
4th Floor
New York, NY 10016
USA

t: +1 212 686 7400
f: +1 212 686 2626
e: usinfo@datamonitor.com

Datamonitor Europe

Charles House
108-110 Finchley Road
London NW3 5JJ
United Kingdom

t: +44 20 7675 7000
f: +44 20 7675 7500
e: eurinfo@datamonitor.com

Datamonitor Germany

Kastor & Pollux
Platz der Einheit 1
60327 Frankfurt
Deutschland

t: +49 69 9750 3119
f: +49 69 9750 3320
e: deinfo@datamonitor.com

Datamonitor Asia Pacific

Darling Park
Tower 2, Level 21
201 Sussex Street
Sydney NSW 2000
Australia

t: +61 2 9006 1526
f: +61 2 9006 1559
e: apinfo@datamonitor.com

Datamonitor Japan

Wakamatsu Bldg 7F
3-3-6 Nihonbashi-Honcho
Chuo-ku
Tokyo 103-0023
Japan

t: +813 6202 7681
f: +813 5778 7537
e: jpinfo@datamonitor.com

ABOUT DATAMONITOR

Datamonitor plc is a premium business information company specializing in industry analysis.

We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt, Sydney and Japan.

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Datamonitor plc.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Datamonitor delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Datamonitor can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.

INTRODUCTION

In today's tough, competitive environment, many organizations are looking to achieve important efficiencies by tying their IT systems to their business processes. As IT departments look to demonstrate their worth to the business, many look to deliver IT as a service that can be consumed by the organization. The business service management (BSM) strategy that many organizations have implemented to meet these objectives must be optimized to ensure that all business needs are met and that the administrators' workload is reduced. This white paper looks at one element of BSM – Identity Management – and details how following a set path allows organizations to achieve measurable benefits within shorter timeframes.

BUSINESS SERVICE MANAGEMENT

For IT to best meet business needs the services must be delivered in a timely fashion, with problems quickly resolved to ensure that disruptions are reduced. IT departments now deliver 'business services' and to ensure their effectiveness, many have implemented management tools and processes to spot potential problems before they arise and thereby resolve issues quickly. BSM is the term used to describe these tools and processes.

Because of the importance of IT in meeting business needs, developing an effective BSM structure is vital. Sadly, there is no single solution for this phased approach. Each organization has reached a certain maturity level for each element and may even have reached (or partially reached) an optimal operations level. By putting what they have already achieved within an overarching structure, enterprises can determine their levels of maturity and see what else they need to do to achieve further improvements.

FINDING ROUTES TO VALUE

With BSM not only is it difficult to know where to begin, but organizations also find it difficult to know how much work still remains. As a result, action tends to be taken in a piece meal fashion – with more time spent 'fire fighting' than taking their systems management structures forward. It is rare that there is only a single driver justifying a specific IT solution's adoption. For organizations to gain the full value of the solution, they must meet and determine how to better satisfy it. Through this, customers can understand what needs have been met and where more attention should be focused.

To overcome these and other issues, customers need specific 'routes to value'. By breaking BSM into 'bite-size' pieces, organizations take what may be a daunting task and divide it into a number of objectives. When met, these allow organizations to benefit from a comprehensive management approach. Datamonitor believes that it is the responsibility of vendors to help customers understand how each element of this infrastructure fits into an overall BSM architecture and how to tackle bigger problems one step at a time.

IDENTITY MANAGEMENT

Because IT architectures grow over time, often through different purchasing regimes, they may consist of thousands of PCs, servers, other networked devices and applications. Mergers and acquisitions exacerbate the problem, making architectures highly heterogeneous. With a large architecture where users may access hundreds of applications, provisioning on an application-by-application basis is extremely time-consuming. Until provisioning is achieved, however, new users or those who have changed their role may be unable to access the systems they need to do their jobs.

In addition, if deprovisioning is not done properly, former employees may still have access to sensitive information. Regulations such as HIPAA in the US healthcare sector, Basel II in retail banking and Sarbanes-Oxley for all publicly listed US-based organizations increasingly force organizations to demonstrate to auditors the checks put in place to ensure confidentiality, integrity and availability - as well as the decision-making process for granting such privileges. Clearly there are a number of very strong drivers for improving the Identity Management structure. The issue is that there is no 'silver bullet' solution to the problem and, as with BSM, even the planning process for such an initiative can be extremely time consuming.

For BSM there must be clear routes to value that ensure organizations get the most from their investment. Supporting this need, BMC has implemented an easy-to-understand yet comprehensive system for determining the optimum routes to value for each element of the BSM model, including Capacity Management and Provisioning, Incident and Problem Management and Identity Management. Within this white paper, Datamonitor will examine the route to value for Identity Management and how each milestone achieved can bring considerable value to an organization.

Within the phased approach laid down by BMC, there are three key achievements, or milestones, that an organization can reach when looking for effective Identity Management. This modular approach allows organizations to determine how specific needs are being met so that investment can be prioritized according to how pressing that need is. By achieving each milestone, organizations will instantly gain tangible

benefits. Achieving all three, however, gives benefits that are greater than merely the sum of its parts because of the important synergies between achievements. Within each milestone, there are three core objectives that must be met. With each objective met, an organization will be able to more effectively establish, monitor and demonstrate compliance with identity and user access policies.

Standardizing Identity Management tools and processes

To achieve the first of the three milestones, the organization must establish a standardized set of tools and processes for identity administration and monitoring. First, businesses should be able to identify and inventory the tools used to provision and monitor access privileges. Secondly, the organization should review both the policies themselves and the procedures for implementing them, to highlight oversights and revise policies where necessary. Finally, the organization must develop a common methodology for managing the identity lifecycle (from when the user joins through to when they leave) and make it as automated as possible to reduce administrator workloads.

There are three principle steps that must be taken to meet the three objectives for the first maturity level. First, by implementing centralized monitoring of who can access which resources, applications and operating systems, the organization can spot security holes created by previous practices. Next, deploying user identity administration tools that manage access rights can simplify the provisioning process avoiding potential security flaws and save time. Finally, putting in place tools to help rapidly and accurately provision or de-provision access can further reduce administrator time spent on Identity Management issues and more effectively and quickly provision users.

Policy-based automation and self-service password management

To reach the second maturity level, an organization must look to implement policy-based automation and self-service password management. Again, to achieve this level of maturity, an organization should look to first identify and address the issue of password change and reset requests - a major pain point for many that can take up a great deal of administrator time. The next step is for organizations to establish clearly defined controls for assigning and removing access rights, which speeds up the process while ensuring that security is not compromised. This can be improved by empowering end-users to request access rights and manage passwords individually.

To achieve the three goals for this milestone, businesses must first implement identity profile definitions that enable provisioning of rights based upon roles of responsibility and rules of access. This will remove the possibility of users granting themselves rights to which they are not permitted. Secondly, by putting in place self-service tools for end-user password management and self-registration, users can request on-demand access rights to key services without involving administrators. Lastly, for this to work, the organization must have a proper administration process in place to expedite workflow automation approvals.

Meeting regulatory compliance

Earlier, Datamonitor highlighted the fact that meeting regulatory requirements was a key reason to improve Identity Management practices. Failure to do so could lead to hefty fines, a poor reputation and, in some cases, jail sentences for negligent executives. As a result, the third maturity level that an organization must reach is ensuring that it can measure its access policies for such regulatory compliance. To begin with, it should be able to demonstrate that it has clear knowledge of who has access to what resources, what the user is doing with this access and who authorized this access in the first place.

Having the information is one thing, but because this will be a regular process, organizations should also look to ensure that this data is quickly and easily available so that it can be presented to auditors upon request. Not only will the auditors be able to decide more quickly whether or not these rights are appropriate and sufficient, but it will ensure that the information gathering process is not excessively time-consuming. Next, the organization should be able to audit identity policies and provisioning approvals and ensure that tolerance thresholds for access and provisioning are enforced. This will make it easier to more effectively report on and react to exceptions. Once these steps have been achieved the firm should aim to put in place procedures for handling compliance exceptions, as well as for remedying them and for continuously improving policies.

In order to ensure that the organization has done enough to achieve regulatory compliance, it should undertake three tasks. To begin with, the organization should conduct and complete a comprehensive review of its Identity Management processes and tools to optimize the linkages that exist between Identity Management and relevant IT and business processes. This will help organizations and regulators alike understand what risks the business has been exposed to - should identity policies be violated. Secondly, the organization should ensure that access management processes are optimized to minimize administrative time and resources while maintaining a high, auditable degree of security.

Ideally, because Identity Management is an important part of the overall BSM strategy, information from this audit should be integrated with change management and business continuity reviews. Finally, to ensure that meeting regulatory requirements does not adversely impact business operations, organizations should look to automate the user life-cycle access process. This will help optimize Identity Management efforts and ensure that access to business services and applications is handled in an expeditious manner.

CONCLUSIONS

With all information technology system implementations, businesses need guidance to ensure that each project goes as smoothly as possible. Vendors can help businesses gauge for themselves how mature their organization is in meeting specific BSM goals by putting their achievements within a milestone structure. The benefits of such a move will better determine how far they have already come to perfecting each set of processes and can then see what remains to be accomplished. Identity Management improvements can bring a number of important benefits to every business that heavily uses IT resources – particularly those who have tied this infrastructure to the business processes.

Through a carefully crafted Identity Management program, organizations can cut help desk costs, increase productivity, improve administrator workloads, enhance security and meet regulatory requirements. Because the task of constructing an effective Identity Management program is a complex one, customers should look to break the task down into a series of clearly defined steps to make the overall process more manageable. The 'routes to value' approach taken by BMC is a prime example of such a program. It allows customers to gain tangible returns on their investment within shorter time frames and determine quickly what else must be done to achieve their overall objectives.