



IDENTITY MANAGEMENT >>

Control IT application access whilst reducing costs

Automating provision of access to IT systems is the route businesses need to take in order to reduce cost, improve security and prepare the way for support of a range of legislation and regulation.

Increasingly security best practice and regulation requires organisations to manage and control user access to their business critical applications. The purpose is to minimise the security risk of business service misuse leading to brand damage or potential financial loss.

TRANSFORMING RISK INTO VALUE

THE ISSUE

Security best practice requires that an appropriate segregation of duties exists between users in different roles. In a trading environment, for example, traders should not have access to the payments systems.

In order to implement security best practice and segregation of duties, organisations need to understand three components – business processes, the technical expertise across the critical IT systems that support the business, and the ability to deliver the appropriate controls at the application level.

Organisations that have initially achieved security and legislative compliance through manual activities and procedural controls should consider the benefits of automation in this area to realise year-on-year savings.

OUR SOLUTION

The Atos Origin solution recognises what is important to key stakeholders, because it is they who must certify that there are appropriate controls to manage risk associated with access to critical IT systems and business services. Our solution brings these stakeholders, including HR, IT, accounting and audit representatives together to ensure that appropriate segregation of duty policies are in place, supported by the technical measures and solutions.

Following our proven method, user access may be controlled by policies implemented in single large application environments (e.g. SAP) and the introduction of role-based access control tools across multiple applications.

THE BENEFITS

Organisations will be able to lower their costs by reducing the number of staff required to support computer user setup and password reset processes. Security is improved as a result of tighter controls around removing old users, application access permissions and system access audit controls.

OUR APPROACH

Our approach starts by engaging the business, control, IT and HR communities within an organisation to develop and establish the current processes, systems and controls regarding the management of their IT user populations. This includes the classification of business critical systems for security purposes.

Concentrating on the business critical systems, we make sure that the correct organisational controls are in place to prevent abuses of privilege, breaches of trust and malicious activities by individuals.

From a technology perspective we review the ability of the existing business critical systems to implement segregation of duty. We will then propose solutions that leverage existing software investments and introduce appropriate tools for the enforcement of segregation of duties. Our aim is to provide effective security policy controls using a combination of people, processes and technology.

This approach creates business value by ensuring technical and organisational controls that deliver the operational and cost benefits are in close alignment.

For us it's all about trust. Our solutions focus on developing trust by managing business risk across the enterprise. In so doing we deliver solutions that transform risk into value.

WHY CHOOSE ATOS ORIGIN?

We help advance your security through a three-stage cycle: Risk and Control Profiling followed by Control Transformation and Business Control Management. Our unique transformational approach is based on integrating the perspectives of people, processes and technology change. We emphasize changing individual behavior as much as we do technology, governance and process.

Atos Origin offers deep domain expertise in vertical markets, bringing to bear an understanding of industry-specific business processes and operating models. Our senior Security and Information Risk Consultants are constantly apprised of best practice through participation in national forums and recognised security organisations – such as the Institute of Information Security Professionals of which we are a corporate founder member.

For more information please visit www.atosorigin.com/security, email security@atosorigin.com or call Mark N Jones, Global Domain Director of Identity, Security & Risk Management on +44(0)7866 767 959.



The Atos Origin solution recognises what is important to key stakeholders, because it is they who must certify that there are appropriate controls to manage risk associated with access to critical IT systems and business services.