Accenture application security leverages SAP Identity Management to enhance digital compliance, agility and efficiency
Client profile

Accenture's internal IT organization is charged with driving the company's digital agenda. Building on the legacy of a notable IT transformation, the CIO group is focused on three key roles: aligning IT with business priorities, enabling a digital Accenture and driving down the cost of IT. Accenture must put in place the technologies that provide its more than 300,000 employees with access to the information and capabilities to be a high-performing business. The company’s single-instance SAP enterprise resource planning (ERP) is critical to the organization's drive for high performance.

Opportunity

Accenture is running a core set of global applications, including a single global instance of SAP that provides the backbone of Accenture's business for its more than 300,000 employees in more than 120 countries. This requires a robust application security model and security operations processes that protect the confidentiality, integrity and availability of Accenture's data. These operations must also contend with a fast pace of business change and growth and Accenture's digital agenda. Given this environment, Accenture faces the ongoing need to deliver a comprehensive user security solution that is compliant with controls and operates with increasing compliance, agility and efficiency across multiple business units, business processes and applications via a single source of truth.

Solution

Over the past decade, Accenture has combined a rigorous approach of governance and process-focused delivery of security operations with an Identity Management (IDM) and Governance, Risk, and Compliance (GRC) solution, both from SAP, to achieve the goals of delivering a solution simultaneously compliant, agile and efficient. Three key factors have contributed to the solution’s long-running success: 1) governing with a process-centered, cross-organizational perspective 2) integrating GRC capabilities and 3) automating role authorization using centralized IDM.

Govern with process-centered, cross-organizational perspective

Residing in Accenture’s Operations Support for the Enterprise (OSE) organization, strong governance for the OSE Security team is enabled through business leaders from Accenture’s internal IT organization, Finance, Human Resources, Business Operations and Geographic Services, serving as an essential integrator.

Responsibilities of the OSE Security Team include governance and operations of Security Provisioning, Compliance and Reporting for Accenture’s core global business applications. Working seamlessly across the IDM, GRC, and other IT areas, the team manages consistent but flexible designs and service agreements across the respective internal business functions, including Finance, Human Resources, Business Reporting, Forecasting and Sales.

OSE Security and Accenture’s internal IT organization collaborate with various assurance teams such as Internal Controls, Internal Audit, external audit and Accenture’s Information Security organization to ensure Accenture is compliant with areas such as Sarbanes-Oxley, ISO27001, data privacy and the corporate insider trading policies.

“Our process-centered security governance allows us to run global applications, including a single global instance of SAP but still secure users across several dimensions," says Todd Harding, Managing Director of Global Operations and Reporting. “We have a solution that is dynamic in the way it provisions user access to applications so as to support Accenture's ability to act fast while tightly managing user access.”

Moreover, governance decisions made by the security teams are supported by data analytics. The focus of Accenture’s early analytics was to understand the level of automation and performance against provisioning service level agreements (SLAs). By 2008, Accenture was using detailed analysis to ensure upgrades were handled with minimal security impact to the business. Most recently, Accenture's reports and analytics have enabled the security teams to closely manage user profiles and licenses, finding significant long-term savings.

Integrate GRC capabilities

GRC tools are crucial for consistent and repeatable control of complex application environments. Accenture transformed itself from having a manual solution, to one centered on SAP GRC but with limited integration, to a system based on SAP GRC 10 having both a business reporting module and segregation of duties (SoD) simulation capability tied to the user business role request and approval process.

“Since the early days of our GRC integration, we have seen a significant improvement in efficiency,” says Todd Black, Operations Support for the Enterprise Application Security Lead. “We began with a very manual, multi-step process and evolved to where the automated process chain runs in under a day and produces a report for the business owners to review in a few hours.”

With the release of SAP GRC 10, the OSE Security team was able to further expand the monitoring capability, which it did with the deployment of two modules, SAP Access Risk Analysis and SAP Emergency Access Management (EAM). These modules enable the team to anticipate and control potential SoDs and monitor use of special production support IDs with elevated privileges needed for rapid support of production issues and software releases.

Opportunity

Accenture is running a core set of global applications, including a single global instance of SAP that provides the backbone of Accenture’s business for its more than 300,000 employees in more than 120 countries. This requires a robust application security model and security operations processes that protect the confidentiality, integrity and availability of Accenture’s data. These operations must also contend with a fast pace of business change and growth and Accenture’s digital agenda. Given this environment, Accenture faces the ongoing need to deliver a comprehensive user security solution that is compliant with controls and operates with increasing compliance, agility and efficiency across multiple business units, business processes and applications via a single source of truth.

Govern with process-centered, cross-organizational perspective

Residing in Accenture’s Operations Support for the Enterprise (OSE) organization, strong governance for the OSE Security team is enabled through business leaders from Accenture’s internal IT organization, Finance, Human Resources, Business Operations and Geographic Services, serving as an essential integrator.

Responsibilities of the OSE Security Team include governance and operations of Security Provisioning, Compliance and Reporting for Accenture’s core global business applications. Working seamlessly across the IDM, GRC, and other IT areas, the team manages consistent but flexible designs and service agreements across the respective internal business functions, including Finance, Human Resources, Business Reporting, Forecasting and Sales.

OSE Security and Accenture’s internal IT organization collaborate with various assurance teams such as Internal Controls, Internal Audit, external audit and Accenture’s Information Security organization to ensure Accenture is compliant with areas such as Sarbanes-Oxley, ISO27001, data privacy and the corporate insider trading policies.

“Since the early days of our GRC integration, we have seen a significant improvement in efficiency,” says Todd Black, Operations Support for the Enterprise Application Security Lead. “We began with a very manual, multi-step process and evolved to where the automated process chain runs in under a day and produces a report for the business owners to review in a few hours.”

With the release of SAP GRC 10, the OSE Security team was able to further expand the monitoring capability, which it did with the deployment of two modules, SAP Access Risk Analysis and SAP Emergency Access Management (EAM). These modules enable the team to anticipate and control potential SoDs and monitor use of special production support IDs with elevated privileges needed for rapid support of production issues and software releases.
Eventually, with the introduction of the SAP IDM system as the request and provisioning engine, the team was able to further integrate the GRC system and deliver online scan results embedded in the approver workflow. This solution presented simulation results to the business approver during request review of single-privilege requests, which increased visibility of potential SoDs.

**Automate role authorization**

A complex security model was needed to protect Accenture’s global applications, including the single-instance global SAP solution against fraud or material misstatement of financials as well for the protection of data privacy. The solution was to use organizational- and geography-specific authorizations based on data scope selected by the user to limit a person’s access to only the areas of data they where they needed to transact or view data. By governing from a single source of authorization truth using SAP IDM, Accenture is able to grant access consistently across its Finance, HR, Business Reporting, Forecasting and Sales systems.

Leadership decided to use the SAP IDM application as the engine for Accenture’s next IDM solution. “Given that SAP was the hub of our financial and HR data,” notes Dan Kirner, executive director of Accenture’s SAP Strategy, Program and Operations, “SAP NetWeaver Identity Management proved to be the best solution for Accenture.” On top of the SAP IDM platform, Accenture’s internal IT organization then built a custom .NET user interface to enhance and simplify the user experience.

Once the 12-month project was completed, the much improved visibility of SAP IDM allowed the teams to clean up and recalculate user data and locate security master data issues previously unseen in the legacy system. This effort involved processing at a peak of 1.7 million calculations per month for a four-month period. The resulting business benefit was accurate, doubt-free reconciliation between the IDM data and the target SAP systems. Today, this solution is used to provision to more than 15 global applications, including custom applications and third-party, cloud-based systems. It is also used to track workflow for several lower-volume applications still using manual provisioning.

The IDM solution automates more than 99 percent of the SAP-related privileges in a standard month and more than 90 percent of entitlements across all applications in scope, allowing a provisioning team smaller than it was 10 years ago to support five times the number of applications and greater user request volumes.

**Results**

Accenture today operates with a global security solution that is compliant with controls, yet delivers business solutions with increasing compliance, agility and efficiency, via one single source of truth. “Accenture now has transparency in its Finance and HR systems environment that is well beyond what is expected for an environment as complex as ours,” notes Karen Quick, Internal Controls lead. “And we can address audit questions better, faster and more cost-effectively than in prior years.” Moreover, rather than audit teams finding issues, Accenture’s security teams now prevent issues or proactively identify and resolve them.

From a business perspective, while audit findings were low previously, the implementation and integration of the solution with SAP GRC 10 has driven them lower with earlier visibility. Today, the percentage of segregation of duties (SoDs) per user has since been reduced by nearly 98 percent compared to the pre-SAP GRC days. Fewer than five in 10,000 users are permitted to retain long-term, locally mitigated SoDs in Accenture’s SAP Finance and HR system. Through gains from the integration with GRC BW reporting, the weekly process now runs in just a few hours, enabling Accenture to be more proactive and timely in its regular operational compliance efforts.

SAP IDM integrated with a custom SAP Solution Manager report allows the OSE Security team to reduce unused authorized business roles and profiles, resulting in a 50 percent reduction in the number of active users. Additionally, a long-standing issue with complex users having more privileges approved than what SAP ECC permits was corrected by performing a detailed analysis of the role and design data.

By following Accenture’s security delivery methodology, over a three-year period through fiscal year 2014, more than 700 changes in the business impacting application security were made from over 50 different Accenture teams and initiatives. The solution is agile enough to keep pace with the changes, while at the same time managing the workflow of more than 100,000 authorizations per month.

In efficiency, SAP IDM has helped Accenture significantly reduce the steps needed to make a user provisioning request. The request process, which took 15 minutes and 34 clicks, was reduced to 13 steps and only requires two to five minutes from a user, an improvement of more than 250 percent and with a 67 percent reduction in labor. Provisioning, now highly automated, has been reduced from one to two days on average down to just a few minutes.

Support costs for SAP IDM are lower compared to the prior team needed to support the legacy application architecture. Accenture estimates that over a three-year period the total cost of ownership is projected to decline by 40 percent.

Accenture’s security solution has been built in such a way that Accenture’s internal IT organization can accept changes from SAP as it releases new functionality, and upgrade the solution without service interruptions. Accenture was also able to take advantage of SAP’s rapid updates over an 18-month period, and continues to incorporate them on an ongoing basis. The current capability enables Accenture to deliver security at the speed of business change and at the same time consider new areas of analytics and mobility for its security solution.

Accenture treats SAP GRC and IDM as an asset, and continually looks to the power that these tools can bring to better comply, be agile and be efficient. Implementing SAP GRC and SAP IDM has served to further enhance the value of SAP at Accenture, and will help to continue improve operations, support digitization initiatives and deliver business value.
About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.