Comprehensive Identity and Access Management in the Cloud

Bring Simple, Scalable Security to Your Landscape with SAP Cloud Identity Access Governance

Sarma Adithe
(sarma.adithe@sap.com) is Chief Product Owner for SAP's access governance solutions and is responsible for overall product development for SAP Access Control and SAP Cloud Identity Access Governance. He has more than 25 years of experience, 12 of which are in the access control domain.

Swetta Singh
(swetta.singh@sap.com) is Director of Product Management at SAP, with more than 17 years of experience in the IT industry. Over the last 13 years, she has focused on SAP Access Control, SAP Cloud Identity Access Governance, and the security marketplace.

With digital technologies continuing to advance at an unprecedented rate, and the Internet of Things (IoT) projected to connect to more than 200 billion devices by 2020,[1] businesses are faced with a rapidly changing technology landscape that has eroded traditional organizational boundaries. Increased adoption of various mobile devices and a growing number of digital identities are transforming business models, social norms, regulations, and the policy landscape across enterprises in all industries.

As organizations adapt to these new digital technologies, many are looking to the cloud to take advantage of benefits such as zero+ maintenance (having no infrastructure or application maintenance costs, except configuration), ease of access to applications, and the ability to choose and use the functions that fit your processes. Heterogeneous landscapes that span on-premise systems, the cloud, and assorted devices bring with them a range of security considerations, however, particularly when it comes to identity and access management. In addition, new and changing privacy regulations often require revisiting existing processes to ensure compliance.

To address these challenges, businesses require a comprehensive, unified, centralized approach to identity management and access governance. This article introduces security and compliance teams to SAP Cloud Identity Access Governance — a scalable, cloud-based solution designed to help organizations simplify, streamline, and optimize identity and access management across their on-premise and cloud-based software landscapes. It walks through each of the services provided by the solution and explains how they are used so that you can move forward with a governance plan for your own organization that can easily scale to meet the changing needs of your business.

A Cloud-Based Solution for a Digital Business Landscape

Built on SAP Cloud Platform and introduced in 2016, SAP Cloud Identity Access Governance is a software-as-a-service (SaaS) solution that integrates with your existing business applications to enable simplified identity and access management across heterogeneous system landscapes. SAP Cloud Identity Access Governance uses application programming interfaces (APIs) to retrieve data from a target system — either an on-premise system or a cloud-based system — and then analyzes that data using functionality provided by five different services. The functionality provided by the services is accessible

[1] See www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

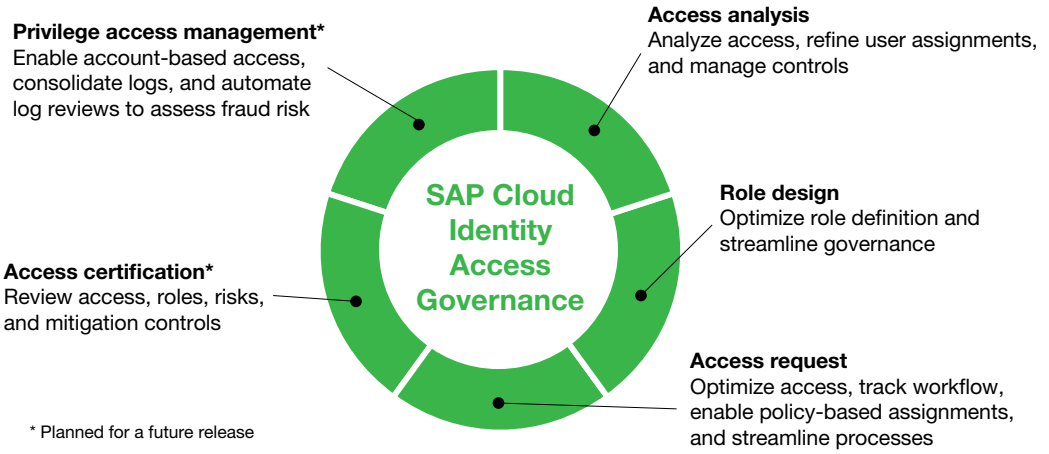

Figure 1 SAP Cloud Identity Access Governance provides five services that can be used alone or together to simplify identity and access management across heterogeneous system landscapes

through apps available in the SAP Fiori launchpad for SAP Cloud Identity Access Governance. **Figure 1** provides an overview of the five services.

These services, which can be used alone or together as needed, include:

- Access analysis, which is used to analyze access, refine user assignments, and manage controls
- Role design, which is used to optimize role definition and streamline governance
- Access request, which is used to optimize access, track workflow, enable policy-based assignments, and streamline processes
- Access certification, which is used to review access, roles, risks, and mitigation controls
- Privilege access management, which is used to enable account-based access, consolidate logs, and automate log reviews to assess fraud risk

The first three services are currently available with version 1711; the last two are under development and planned for future release.[2] Let's take a closer look at each service.

Access Analysis

The access analysis service delivers insights into segregation of duties (SoD) conflicts and critical access risks, and enables you to review and mitigate identified risks across your landscape. **Figure 2** shows the access analysis overview dashboard, which includes an overview of compliance and access risk across your landscape. The view that shows the top users by risk score identifies users with the highest risk score based on access risk, access usage, and the number of mitigated risks. You can also view the most frequently occurring risks along with information on the business processes with the most risk violations. The views that show risk trend by quarter and risk occurrence by risk level provide an overall health check of how your organization is performing with access compliance.

Access analysis enables compliance and security owners to follow a monitor-refine-mitigate cycle by using real-time visualizations to monitor and optimize access. Using the overview dashboard, you can select users to analyze and then customize predefined access policies and rules to remediate risks — for example, by refining user role assignments or optimizing user access based on changing business requirements, and by assigning a mitigation control to monitor for risk. The integrated control monitoring feature ensures that the controls are working as designed and flags any deficient controls that might be in active use and causing risk exposure. Every action is recorded in an audit log that can be viewed for a more detailed analysis.

[2] See the SAP Cloud Identity Access Governance roadmap at www.sap.com/products/roadmaps.html for the latest information on planned functionality.

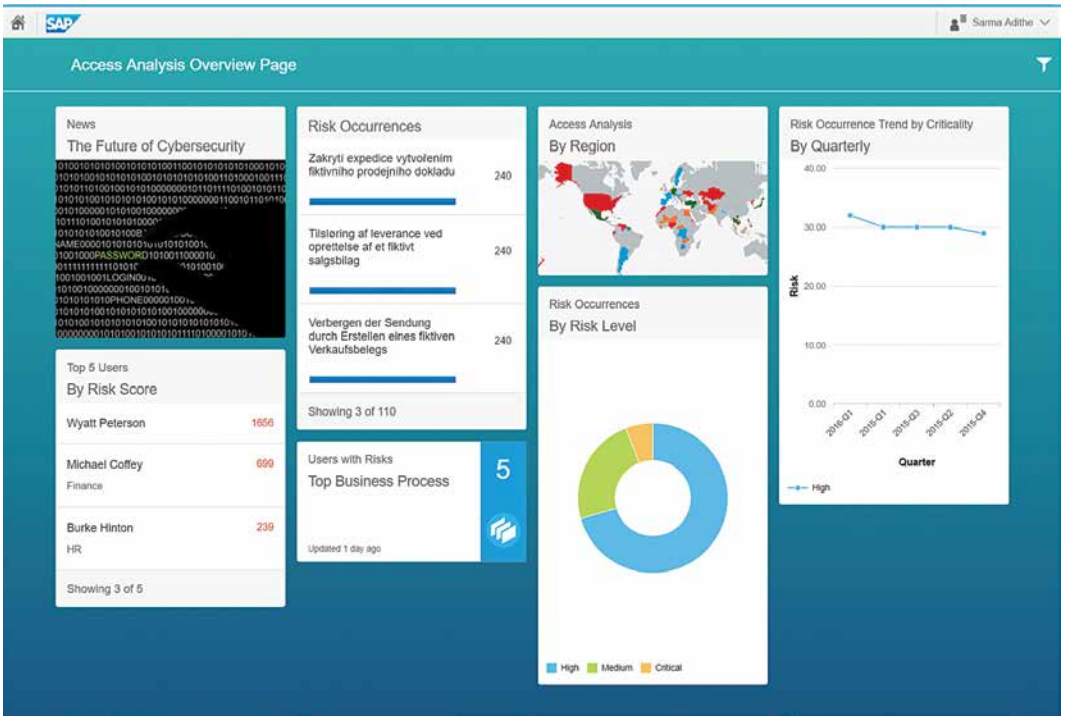

Figure 2 The access analysis overview dashboard

Role Design

The role design service provides a comprehensive approach to designing, maintaining, and optimizing business roles that reduces the complexity of role administration and simplifies the process of access assignment. It enables a bottom-up role design and refactoring process that ensures business role compliance with organizational policies.

To help role administrators, security administrators, and process owners optimize the design and maintenance of business roles, the role design service analyzes role and authorization information in the target system. Based on this analysis, as well as rule-driven algorithms, the service then makes recommendations to optimize user roles and processes and to remediate risk. The role design service provides risk metrics and usage trends within a business context to enable an integrated reconciliation process so that you can evaluate the impact a user's new role will have on existing assignments. Once you make the necessary role adjustments, affected users are notified of the changes.

Figure 3 on the next page shows the functionality provided by the role design service. This functionality includes the Business Roles app, which is used to create and maintain the business roles defined for your company, and the Role Designer app, which provides an overview of how roles are being used in your organization. It also includes the Create Candidate Business Roles and Select Candidate Business Roles apps, which are used to create more efficient business roles. The Role Design Administration app enables you to monitor and track the overall role design process.

Access Request

The access request service provides self-service functionality that allows users to gain access to different application types (on premise and in the cloud), databases, and devices, and integrated security controls that approvers — managers, role and process owners, and security administrators — can use to mitigate any risks associated with these access requests. The service enables a unified process through which employees are granted access to only what they require to fulfill their job responsibilities, and provides complete visibility into the critical or sensitive areas to which a user might have access to help prevent security breaches. The access request process also allows organizations to stay secure by preventing occurrences of stale or orphan accounts that stay alive even after the employee leaves the organization.

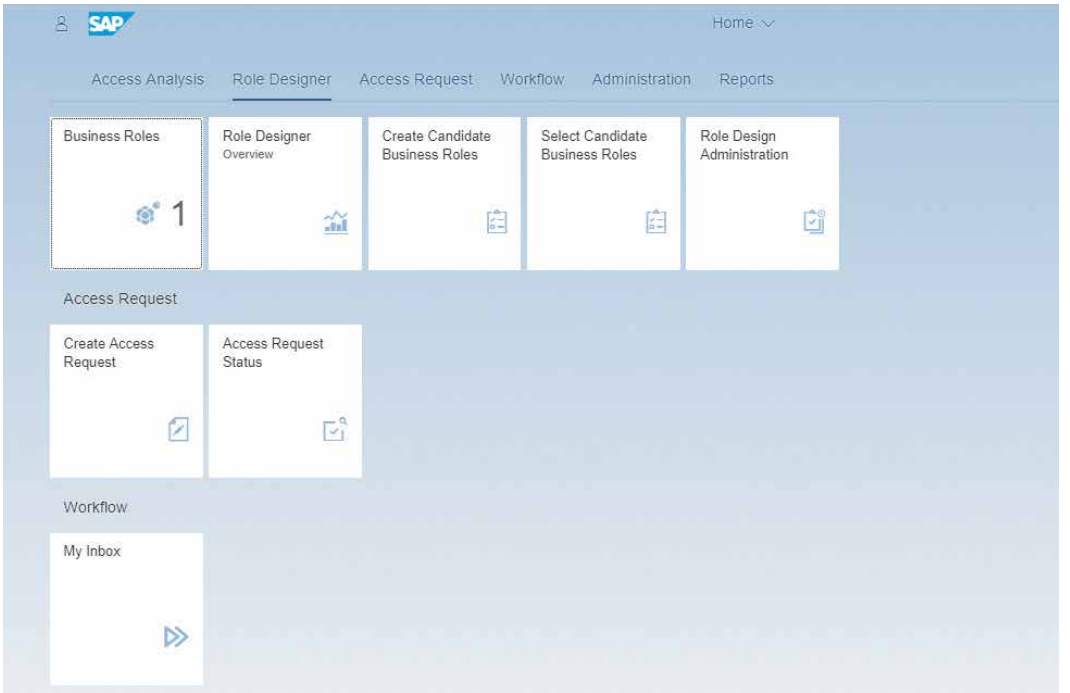

Figure 3 The role design service provides functionality for creating, maintaining, and optimizing business roles

When a user selects and requests a type of access, the service submits that request to the approver for review. The approver can then view identified risks via a simulation feature (see **Figure 4**), remediate those risks with mitigation controls, and then approve or reject the request. Once a request is approved, the service automatically provisions access to the user. The service also provides a complete audit history of all actions related to the request. Using the self-service feature, the user can check on the status of the request at any time, adjust it as needed, and then cancel or resubmit the request.

Access Certification

The access certification service is designed to prevent privilege creep, which happens when an employee's job responsibilities change, but access privileges that are no longer needed are retained along with the addition of new access rights. Periodic recertification of access privileges helps establish a governance process to identify changes in individual usage behaviors and prevent the accumulation of unneeded access privileges, which can lead to security risks. This process can also be extended to enable periodic review of critical application access, roles, and policies to ensure efficiency and adherence to audit requirements.

The access certification service optimizes access and access governance, addressing complex elements such as critical access points, SoD risks, and mitigation. Security and IT administrators can initiate a review of the access certification, and then distribute these reviews to various approvers, such as managers, role owners, and risk and mitigation owners, depending on the type of content and the review cycle. The reviews can then be monitored for timely completion. At the end of the process, user access is automatically adjusted to best fit the needs of the business based on review proposals. All activities are logged to enable audit reporting.

This service is currently under development at SAP and is planned for future release.

Privilege Access Management

The privilege access management service is designed to flag not only who accesses sensitive or administrative transactions, but also what is being executed with these elevated authorizations. This enables an effective review of all administrative or maintenance activities with elevated privileges to ensure that nothing fraudulent occurs during these activities.

Privilege access management establishes a governance process to monitor and reconcile all elevated privilege activities. It secures business applications,

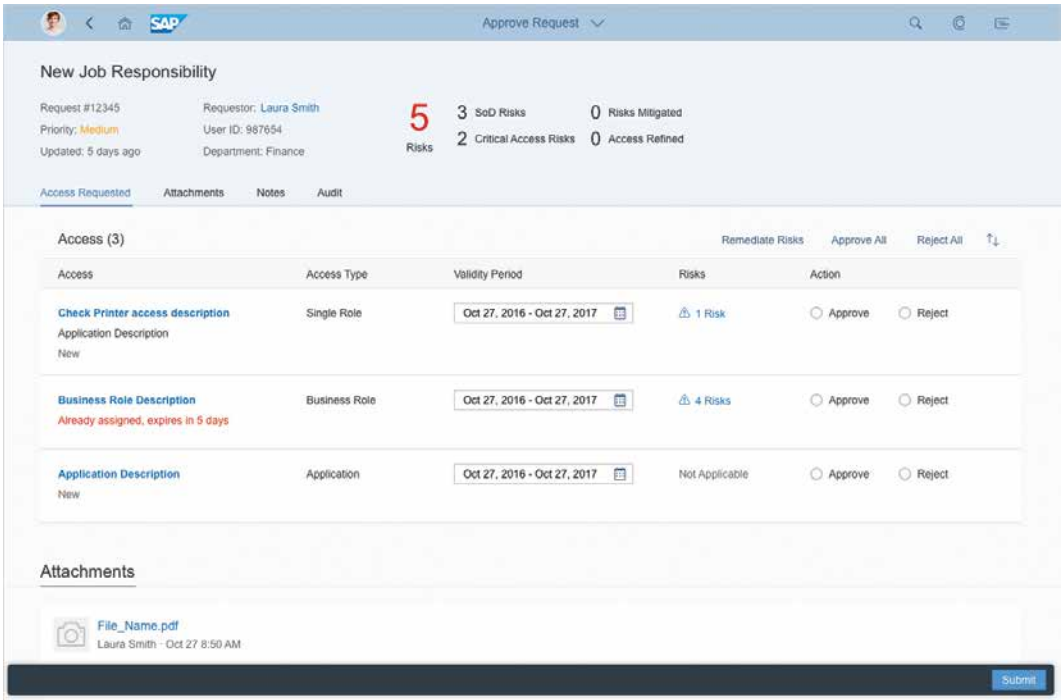

Figure 4 The access request service identifies potential risks associated with a user's access request

enforces accountability, and provides intelligence. Suspicious activities are immediately flagged by leveraging machine-learning capabilities to analyze the logs and identify anomalies, behavior changes based on historical data, and enforcement policies. Security administrators and those responsible for emergency maintenance can then use this information to review and audit users with privileged access to remediate risk.

This service is currently under development at SAP and is planned for future release.

Effective, Efficient Governance

Access governance, compliance, auditability, and provisioning are key features of SAP Cloud Identity Access Governance. Through its services, it provides mechanisms for optimally designing access in a way that provides protection for your business without compromising productivity. For example, you can provide users with birthright access — default access privileges assigned upon hire — by using business roles as a container for all necessary access, and in this way, minimize the need for users to request additional access. You can also take advantage of its process-driven approach as well as its analysis and logging features to ensure compliance and auditability.

SAP Cloud Identity Access Governance Resources

- **SAP Cloud Identity Access Governance product page**
  www.sap.com/products/cloud-iam.html
- **SAP Help Portal**
  https://help.sap.com/viewer/p/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE
- **SAP Roadmaps**
  www.sap.com/products/roadmaps.html

IT and security administrators are concerned about securely accessing business functions and having only the right individuals performing the right tasks, while business users want to have all the access that is required to successfully execute their business functions. SAP Cloud Identity Access Governance meets these expectations in a secure, effective, and efficient way, and makes it possible for identity and access management to be a business enabler rather than a business disabler. ■