SAVIYNT

SOLUTION GUIDE

SAVIYNT FOR SERVICENOW

THE POWER OF ITSM COMBINED WITH THE GOVERNANCE AND COMPLIANCE OF AN IGA SOLUTION

THE POWER OF SERVICENOW ITSM

The use of ServiceNow as an ITSM solution gives customers the ease of going to a single place for all requests. Whether physical or logical access, ServiceNow provides a consistent experience for end users; a place to monitor the status of requests, and a rich workflow engine to monitor approvals and fulfillment.

However, the broad focus of ServiceNow makes it difficult to manage their complex security models, policies and controls around end user logical access.

GOVERNANCE AND RISK CHALLENGES

Monitoring granular access details and defining when an end user shouldn't have certain and potentially toxic combinations of access is a complicated business process. The same person that issues refunds shouldn't be the approver of those refunds.

When these combinations aren't kept current, or the detailed access in an application isn't easily transferred to ServiceNow, it can lead to people approving and receiving access without ever understanding the risk.

Saviynt's Identity Governance and Administration creates valuable collaboration through integration with ServiceNow to inject risk-aware governance and compliance into access decisions.

WHAT PRECISELY IS GOVERNANCE?

Identity governance typically refers to placing policies around what access should be granted to an identity in what situation, and subsequently monitoring that the granted access is both current and being used correctly. Governance focuses upon ensuring the right person has the right access at the right time and uses it in the right fashion.

End users often experience complexity gaining access to applications, roles, and particular rights within those applications. It can be confusing determining what to request. Many organizations default to a process where new employees ask to have the same access as an existing employee. Risk can be incurred because the existing employee may have accumulated excessive access rights. We need to provide the right access, not excess access.

Managers and application owners need to periodically review user access and confirm it is correct. Not all access needs to be reviewed, but access tied to risk should be validated and reviewed more frequently. In an ideal world, access attestation should happen in real-time, each time a person's position or access changes, not just every quarter or year.

Governance and ITSM have natural synergies. The ITSM ticketing system centralizes all the requests for access and their status. The Governance solution handles the risk, provisioning access, attestation and auditability of the access requests from the ticketing system.

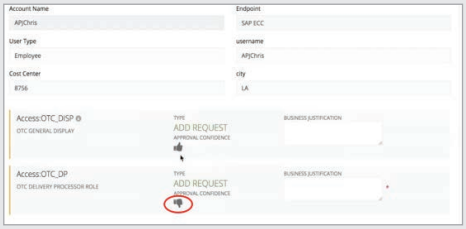
BENEFITS OF INTEGRATION BETWEEN SAVIYNT AND SERVICENOW

Cross-application real-time provisioning and governance	As users join the organization or change roles within it, Saviynt's rules and policy driven provisioning process automates onboarding of user's access and rights for business applications, including ServiceNow. User accounts are created with appropriate access at the right time, such as adding a user to ServiceNow resolver and security groups. This improves organizational security posture and productivity through consistent provisioning automation processes.

BENEFITS OF INTEGRATION BETWEEN SAVIYNT AND SERVICENOW

Customizable access to digital assets	All requests begin in ServiceNow with requests for digital assets automatically initiated in Saviynt from ServiceNow. Saviynt opens the ticket in ServiceNow while syncing with Saviynt for real-time ticket status. Interim, Saviynt runs analytics, assesses risk and proposes recommendations. Depending on the level of risk, the request is either referred to the manager for approval and Saviynt fulfills the request or the request is automatically approved. If access must be manually fulfilled, Saviynt can assign the ticket to Resolver groups in ServiceNow. Access to digital assets can be customized depending on your business needs.
Integrated risk analysis and Segregation of Duty (SoD) in workflow	When end users request logical access and rights, Saviynt proactively informs the user if the access causes significant business risk and if there is risk of any potential SoD violations. If the access is approved, the approver has the option to add mitigating controls to the SoD. This results in end-to-end visibility into risky access.

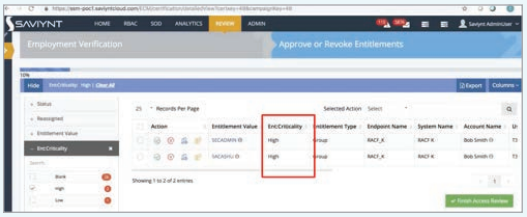
SHARING RESPONSIBILITY



INTELLIGENT IDENTITY. SMARTER SECURITY.

As organizations undergo digital transformation, the notion of shared responsibility is usually applied to cloud services. But even within an organization, responsibility can be shared. When every person in the process has clear visibility into the risk they are incurring, employees, managers, and application owners all make more careful decisions. As shown above, visibility is surfaced at each level of the request and approval process. You can view risk at the employee request, displayed to the approver, and then called out during certification campaigns. In this way, risky access doesn't slip through the cracks. This is how Saviynt's intelligent identity and analytics enhance ServiceNow's rich ITSM system and enrich the information needed for business decision-making.

CERTIFICATION AND RISK



RISK-BASED ANALYTICS.

Managers or application owners often review who has access numerous times. As a result, they may not be able to focus on the most meaningful information. This repetitive process often leads to approval fatigue where the reviewer will rubber-stamp all access. Many organizations have experienced incidents and breaches from access where someone simply continued approving without examination. With Saviynt's risk-based analytics it is easy to drill down into the access, which might be high risk, and focus on whether the end user still needs that access. Intelligent analytics for user access is the core function of identity governance. Using Saviynt's intelligent analytics, combined with our seamless integration with ServiceNow, helps improve an organization's security posture significantly.

LEARN MORE

FIND OUT
why Saviynt received the highest product score for Midsize or Large Enterprise & Governance-Focused use cases in Gartner's 2018 Critical Capabilities for IGA.

TRY A DEMO
of the Saviynt IGA Platform

START A FREE TRIAL
of Saviynt's Enterprise Solution

ABOUT SAVIYNT

Our vision is to redefine IGA by converging traditional Identity Management with Cloud Security, PAM and Application GRC capabilities. In doing this, Saviynt enables enterprises to secure applications, data and infrastructure in a single platform for cloud and enterprise.

VISIT OUR WEBSITE

CLOUD PLATFORM BENEFITS

- Ease over-burdened IT resources
- Deploy rapidly
- Keep current with continuous upgrades
- Stay ahead of compliance needs with online access to Saviynt's Controls Exchange
- Flexible and tailored integration to meet your needs

SAVIYNT, INC. (Headquarters) 1301 E. El Segundo Bl, Suite D, El Segundo, CA 90245, United States **Tel. 310. 641. 1664** **www.saviynt.com** | info@saviynt.com