Scientific Research Publishing

Journal of Information Security, 2025, 16(4), 595-609
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Unique Identity Gateway Automation Product Capable of Connecting SAP GRC Security System for IAM Activity

Shreekant Rangrej

Department of Cyber Security, Bridgesoft Infosec LLC., Atlanta, GA, USA
Email: shreekant.r@bridgesoft.com

How to cite this paper: Rangrej, S. (2025) Unique Identity Gateway Automation Product Capable of Connecting SAP GRC Security System for IAM Activity. *Journal of Information Security*, **16**, 595-609.
https://doi.org/10.4236/jis.2025.164030

Received: October 13, 2025
Accepted: October 26, 2025
Published: October 29, 2025

Abstract

The unique identity gateway product organizes and secures Identity and Access Management (IAM) activities in the corporate world where security of users is paramount for the successful operation in the SAP GRC Environments. Automating procedures through modern gateway technologies and secure SAP GRC environments and RPA facilitates integration of applications, security and compliance. The article asserts that Identity Gateway will modernize the interaction of applications with SAP GRC but needs to resolve security issues, give lower operational costs, and provide scalable and future-based solvable problems for the IAM. Automating repetitive tasks that are processable gives large corporations lower cost returns and more staff and resources to devote to other areas. Automation technologies can perform tasks such as disabling users, onboarding new hires, provisioning access, automating report writing, managing emails of whatever type and nature, etc., all faster than humans can. This will enhance the ability of the IT department. To make decisions and deliver IT services. Improvement in data integrity and quality will also be achieved by lessening work fatigue among the staff who are bogged down in repeating multitudes of this process. Also, allowing fewer stretching hours by the repetitiveness of the processes lends less classification of the operational cost, thereby leaving more staff and resources to be devoted to productive matters like profit, investment in raising more production and services, innovation, forward planning, customer service, etc. Automation will allow staff to think of more creative and analytical tasks that need human thought and insight, which should lead to better job satisfaction amongst younger staff and less stress for older staff. Automated processes can handle workloads of billions of millions and give a good performance and service level without increasing the amount of manpower needed in these areas as companies tend to increase in size.

Keywords

Identity Gateway (IG), SAP GRC (Governance, Risk, and Compliance), Identity and Access Management (IAM), Robotic Process Automation (RPA), Automation and Integration, User Provisioning and De-Provisioning, Compliance (SOX, GDPR, ISO 27001), Access Control Automation, Workday Integration, AI and Machine Learning (ML), Operational Efficiency, Data Integrity and Quality, Job Satisfaction and Workforce Optimization, Cloud and Multi-Tenant Environments, Governance and Auditability

1. Introduction and Background

Automation is critical for integrating repetitive activities into modern enterprises, decreasing human error, and improving the usage of resources. The effective handling of vital tasks such as user deactivation, report creation, and email processing has been developed. Automation expedites decision-making and leads to greater service delivery. It ensures uniformity and precision, both of which increase data reliability and quality of operations. From the literature the quantitative benefits of Identity Gateway SAP GRC also with RPA automation are reported with Workday show progress from 35% quicker task identification, scaling and decrease in human involvement in compliance [1] to an increase of 50% effectiveness HR robotics. Additional cost estimates and reductions of approximately 40% - 50% are anticipated for SOX/GDPR compliance within the SAP-Workday hybrid environment.

All of this results in organizations' efficiency in operations and their capacity to lower expenses and deploy human resources to strategic, innovative, and customer-focused initiatives. By removing so much drudgery-associated work employees perform, greater job satisfaction results and burnout are reduced, making the corporation a more effective and smarter one. This paper focuses on how automation and AI are modernizing the SAP GRC system through access control. An identity gateway is a sophisticated automation technology designed to assist firms in expediting and efficiently securing Identity and Access Management (IAM) activities throughout their businesses.

Prototype testing was initiated to validate that user termination automation for SAP GRC is truly triggered by changes in Workday statuses. The goal was to ensure that user access in SAP systems was deactivated whenever a change of state to "inactive" or "terminated" occurred for an employee. The Identity Gateway integration utility was developed and set up to listen for Workday events and send termination signals to SAP GRC Access Control via API. Once the trigger was executed, SAP GRC sent an Access Request workflow to revoke roles and lock the user account. Test cases for this event proved both voluntary resignation and termination and contractor offboarding. Audit logs of the activities were reviewed to be sure that the deprovisioning steps were traceable and compliant with internal

controls. The prototype, in addition, was tested for timing, to be sure that access removal took place in a matter of minutes following the Workday updates. Exception handling for edge case items such as rehires and users with dual roles was validated as well. Notifications in the form of alerts were configured to send messages to security teams to alert them of successful termination. Overall, it can be seen that prototype for real-time enforcement of user lifecycle can be achieved with minimal manual intervention.

Note: Figure 1 illustrates the development of SAP ERP solutions that began in the 1970s with the development of SAP R/1, a one-tier system that catered to financial accounting requirements only. In the 1980s, SAP R/2 came into being—a mainframe computer development which aided in the integration of various business activities such as material management, production planning, financial accounting, human resources and so on. Then in the 1990s SAP R/3 came into being, which revolutionized the concept of application software due to the use of client/server technology and a graphic user interface, which eventually led to cross-functional integration coming into vogue. In the 2000s SAP ERP central component (ECC) became available, which is part of the SAP Business Suite, with increased scalability, web accessible software. In 2015, SAP S/4 HANA introduced in-memory computing with real-time analytics functionality and this also simplified the database architecture for better integration for the operation of an intelligent enterprise. In 2022 and beyond, RISE with SAP became a reality—which is a total enterprise transformation as-a-service offering, where companies would have the opportunity to migrate across to cloud technology and take advantage of intelligent enterprise functions (SAP S/4 HANA etc.).

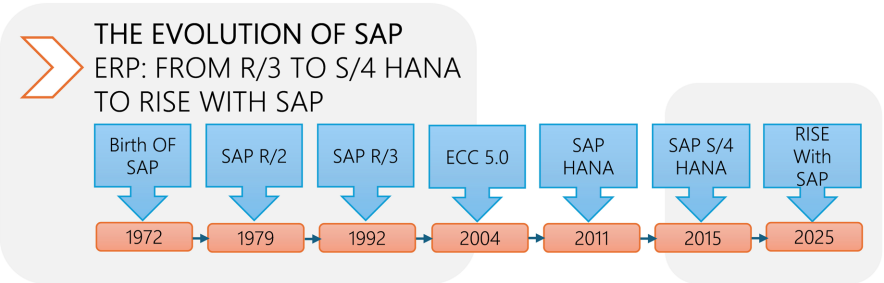

Figure 1. The evolution of SAP ERP.

Enterprise Identity and Access Management (IAM) is moving quickly as companies place a premium on agility, efficiency and a focus on the cloud. While traditional SAP GRC solutions have proven effective and safe for controlling access to applications, they are hard pressed to adapt to new integration needs [2]. AI based framework for automation of Identity Governance is proposed in large scale enterprise environment which highlights focusing on risk management and access provisioning similar to SAP GRC access Control. It also discusses compliance monitoring and reducing manual interventions by 40% by predictive Analysis and reviews mitigation of Segregation of duties (SoD) risks.

SAP GRC Adoption Trends: 2015-2025

Note: Figure 2 shows that the development of SAP GRC, or Governance, Risk, and Compliance, began in the early 2000s when organizations began needing integrated tools with which to manage compliance as well as risk across complex IT environments. At first, SAP offered Compliance Calibrator (which they acquired from Virsa Systems in 2006), which was focused mainly on segregation of duties (SoD) and access control within SAP systems. Over time, SAP has migrated this status into a full GRC Suite, which they completed by introducing modules like Access Control, Process Control and Risk Management to address more broad-based governance needs. The SAP GRC 10.x suite served to consolidate these modules under one platform with a relatively common user interface, which helped the integration as well as the reporting abilities. Now, SAP GRC 12.x is well integrated into SAP S4 HANA and into cloud environments, allowing most enterprises the ability to have much more advanced automation, analytics, and ongoing validity for new more digital environments.

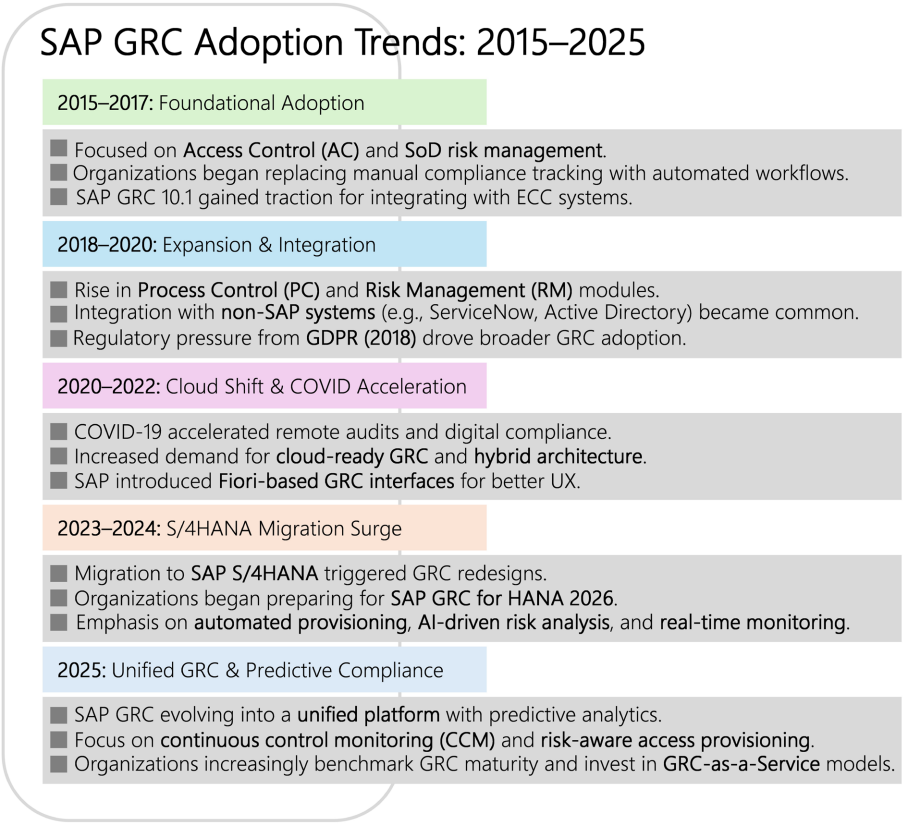

Figure 2. SAP GRC Adoption trends.

Automation also standardizes processes, clearing a rate of compliance significantly better in level and audit tracing benefits. Better still, improvement in service quality is quickly provided while customer satisfaction improves [3]. This paper points out ML models for automating user access reviews in ERP platforms like SAP, converging on Identity gateway for GRC and achieved 95% accuracy in risk

detection with integration challenges in multitenant environments. Chatbot technologies provide 24/7 service support and ease in access to personnel. Further, the IAM challenges in remote and cloud environment were outlined by [4], Singh et al. conducted interviews with 45 cybersecurity professionals, this study noting barriers to adoption of technical solutions and addressed security perceptions in commercial sectors.

The proposed and discussed unique Identity Gateway automation technology utilizes Robotic Process Automation (RPA) technologies and integrates with Workday to monitor changes in employee status. It instantly disables access to all the SAP System by creating SAP GRC Request while changing employee status from Active to Terminated.

1.1. Identity Gateway Prototype Architecture (Conceptual)

Figure 3 shows how the Identity Gateway detects an employee's status from Workday and makes an API call to the SAP GRC system. The Identity Gateway maintains the SAP user master data, which consists of first name, last name, email, and other attributes. This information determines the appropriate SAP User ID and triggers a termination request to the SAP GRC system through an RPA-based process.

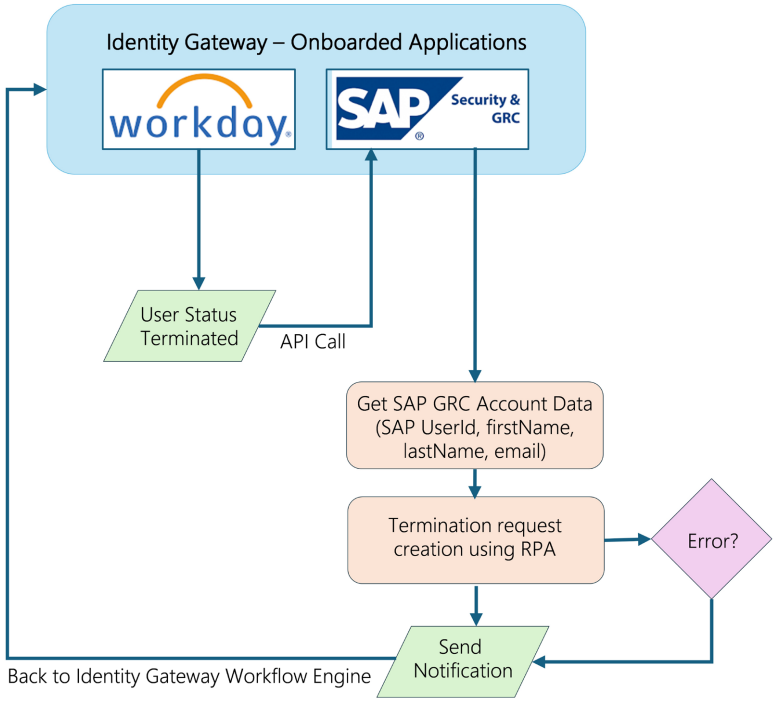

Figure 3. Architecture of identity gateway termination process.

1.2. Detailed Description of How Organizations Can Benefit from Automatically Disabling SAP Accounts Using GRC When an Employee Leaves or Becomes Inactive

Improves security and prevents unauthorized access: SAP GRC (Govern-

ance, Risk, and Compliance) user accounts are automatically disabled, which ensures that employees who leave are quickly denied access to the system as their employment status changes within Human Resources (HR) systems such as Workday. By doing this, the company minimizes the chance of unauthorized access to sensitive financial or operational data, which in turn reduces the chance of internal breaches of data security, fraud or violations of company policies. It also avoids the security gap that occurs when accounts remain open even after an employee leaves. [S] This paper focuses on security of automated Identity management in distributed GRC systems with applications to SAP IDM and cloud gateways also demonstrating latency reduction in provisioning through collaborative model training across enterprise.

Ensures Compliance with Regulatory Requirements: There are several regulatory and legal requirements, including the Sarbanes-Oxley Act (SOX), GDPR and ISO 27001, that require organizations to carefully restrict user access and to provide audit trails. Automatic disabling allows organizations to demonstrate compliance by ensuring that access authorizations are rescinded in a quick and uniform manner. It also provides clear and time-stamped records of when and how access is terminated, which is essential in audits.

Decrease Administrative Workload: In great organizations, it is monotonous and too laborious to manually turn off or disable user accounts in different systems such as SAP GRC. Automation will help reduce the time usage of the IT administrator in performing repetitive manual tasks and deactivating users on offboarding, thus saving maybe hours of human labor. This will enable IT workers to work on projects that are strategic rather than banal management of users.

Improved Precision and Consistency: Manual offboarding methods can often lead to human error such that accounts can be missed for termination or only partially terminated, etc., which can be avoided by carrying out the disabling of access in a consistent manner through an automated control process, which will also improve data integrity as well as remove the opportunity for inconsistency.

Enhance operational efficiency: By monitoring the HR information, allowing for the automatic disabling of SAP user accounts (*i.e.*, when an employee's Workday employee status changes from active to inactive). This will cause the process to take place nearly in real time and will in all events eliminate the two events that invariably arise, time lagging and reporting. This will ensure that at all events, they will always be in correlation with that of the user activity in the actual status of the employee, resulting in greater cooperation between the HR department, IT and compliance departments.

Savings in Costs and Resources: Administrative costs and other costs for the organization of late manuals in terms of dismissals or missed dismissals will be minimized by the way in which it is intended to minimize the laborious processes that are commonly supposed to be entailed in connection with them. The savings in money and in ethical costs to the organization will be considerable in a decreas-

ing ratio of security incidents and audit exceptions.

Improves Governance and Accountability: The imposition of a strict control general procedure of deactivating accounts automatically signifies a strict governance procedure, whereby slow or manual methods will lead only to companies granting access to unauthorized and inactive users. It therefore caters for accountability and transparency in user lifecycle management which is vital for good governance of the corporation.

1.3. Advantages of Automating User Onboarding of SAP When New Employee Joins the Company

Improved Process Efficiency: RPA implementation improves the onboarding process by automating the tasks of normal usage of SAP user proofs such as filling of accounts, assignment of roles, filling data and granting access. It prevents individuals from doing repetitive manual work and HR and IT workers perform critical activities. It also decreases time needed to join process from weeks to days in a matter.

Improved Data Integrity and Compliance: Automation maintains correctness of data standards and integrity when updating employee data in SAP systems because of removal of human mistakes, so it avoids loss of information. RPA follows compliance rules, hence compliance and data protection.

Ease of Scaling: Using RPA it is possible to effectively scale the onboarding processes in organizations. No matter if many employees or only a few are employed they are quite capable of making a great number of software bots, parallel fast change in hiring requirements without increasing overhead.

Save Cost and Time: By automating onboarding processes RPA the end-user can save on working costs related to human jobs and paperwork and increase productivity of new employees. According to some organizations we mean fewer manual jobs and great accountability revenues and benefits including thanks to effective SAP Implementation.

Assist Employee Experience and Retention: The automated onboarding gives new employees rapid access to required tools, paper, stock and demoing teaching classes and help. It improves its experience in the organization and increases the degree of retention. RPA gives much better logical examples in such experience onboarding tasks, giving potential employees the opportunity to begin to feel immediately prepared and wanted.

Security Improve Ongoing Planning: Bots continually update and keep up-to-date personnel information, cancelling or changing access privileges and responsibilities and keeping secrecy so that no other assigned employees can see hazard-sensitive information.

1.4. Key Performances of RPA in SAP GRC through the Identity Gateway

Automating Onboarding User: When a new worker in Workday is introduced

to RPA, it automatically creates most account users in SAP GRC. It gets correct assignments of access in SAP GRC meaning roles, departments, posts and plans, etc. It even keeps effective and excellent forms of use onboard without clogging or defects.

Automating user de-provisioning/termination: When a worker or any inactive post is no longer available RPA quickly decreases SAP GRC access. Identity Access is constantly operational in Workday, and has any changes in employee positions (Active or inactive). RPA ensures performance of all user accounts, Roles and system access is cancelled in real time eliminating problems associated with security.

Access and Role Management: Employees changing positions, departments, or projects may need their access privileges changed. RPA automatically changes roles in SAP GRC to ensure employees get the right access necessary for their current job. Eliminates excess or stale privileges which can create compliance problems.

Policy Enforcement and Compliance: RPA makes corporate access policy enforcement in SAP GRC more effective by automatically establishing a link between user roles and policy rules. Audit trails are created and automated action logs are maintained to establish compliance with regulations (SOX, GDPR, ISO 27001, etc.)

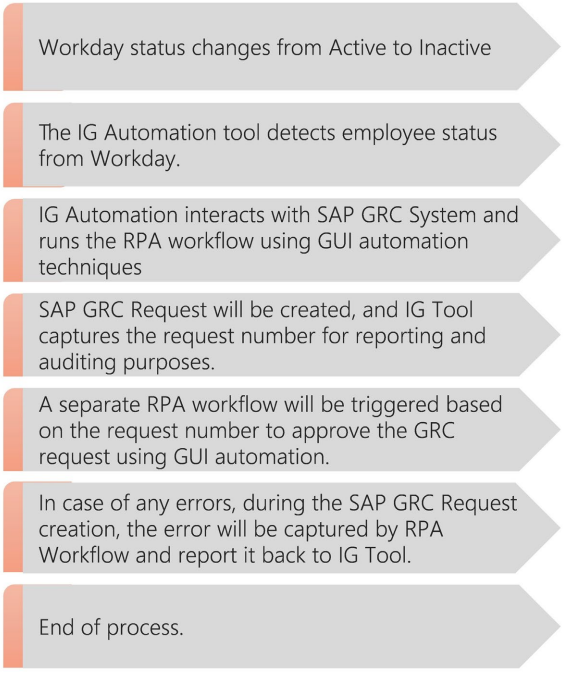

Figure 4. Flow diagram for identity gateway SAP GRC request creation based on workday status change.

The Identity Gateway. Re-engineering IAM: Identity Gateway supplies a common, secure interface through which diverse Identity management endpoint systems are linked (directories, on-prem applications, cloud services, SaaS solutions,

non-SAP corporate systems). This allows seamless automated access control, provisioning and de-provisioning processes.

Figure 4 illustrates that when a user record is changed from Active to Inactive in Workday, the Identity Gateway (IG) Automation tools capture this change in real time. Then, they call out to the SAP GRC system, executing an RPA workflow via GUI-based automations. As part of this workflow, an SAP GRC Request is created, and the IG tool logs the request number for tracking and audit purposes. This request number is the trigger for another RPA workflow, which approves the GRC request via GUI actions. If any errors are thrown in the creation of the SAP GRC Request, they are captured by the RPA workflow and returned to the IG tool for logging and resolution. This evaluation of workflow provides the audit and tracking capabilities across the deprovisioning request process. The design requires minimal manual intervention, thus allowing for efficient and secure user lifecycle enforcement.

1.5. The Key Features of the Latest Identity Gateways

- Convenient connectivity to legacy applications as well as cloud apps.
- Effectively synchronize identity attributes, policies and entitlements.
- Use real-time event-driven workflows for provisioning and de-provisioning.
- Establish zero-knowledge authentication, audit trails and privileged access control.
- Integrated compliance support for regulations like GDPR, HIPAA, and SOX with rapid reporting performance and security analytics.

Identity Gateway can enhance operational performance and reduce staffing demand for manual intervention by establishing IAM workflows using a central hub rich in policy capabilities. The capability to supply non-intrusive automated operations for SAP GRC and other essential business systems will prove invaluable for companies operating in a highly regulated environment or using hybrid cloud architecture [6]. Lee *et al.* have explored a blockchain identity gateway for automating governance workflows in hybrid cloud setups, directly applicable to SAP Cloud Identity Access Governance highlighting the enhanced security against unauthorized access for SAP GRC systems integration.

2. SAP GRC: Legacy, Security, and Integration Problems

SAP GRC accesses management, process control modules and provides the platform for corporate risk management and compliance. While the security features of SAP GRC are vigorously maintained centralizing role-based access control management, SoD (Segregation of Duties) checks, and user life-cycle controls, SAP GRC suffers from integration problems most of the time. This [10] focuses on data sources and business rules for continuous compliance and overviews of automated monitoring in SAP GRC Process Control 10.0

- Legacy architecture requires special interfaces for non-SAP and cloud applications.

- Manual, resource-intensive provisioning and de-provisioning generate operational overhead.
- Segregation of automation and reporting could result in gaps in auditing proof and oppression of compliance-related workflows.
- Managing compliance across hybrid on-premises and cloud applications might be difficult.

Despite these limitations, the basic security of SAP GRC, the real-time analysis of risk factors, and the strong controls exercised over corporate roles and emergency access rights remain industry standards to protect sensitive data and manage accountability. The melding of SAP GRC with the new identity gateway technologies supplies an effective means of accelerating these procedures, automating complex processes of compliance, and furnishing solutions for integration of security breaches associated with numerous platforms.

Automation technologies within the integration gateways are designed to eliminate such problems by acting as a "bridge" platform making SAP GRC work with other identity providers, applications and cloud services by way of secure policy-based automation. This would usually mean it encompasses:

- Connecting SAP GRC with Identity Gateway by means of one or more of the following technology streams, *i.e.*, APIs, virtual directory services, RFC, middleware, e.g., SAP PI/PO.
- Import of the GRC provisioning frameworks into the gateway automation engine and scripting of job orchestration sequences.
- Extending the data schema so that identity attributes, risk policies and entitlement definitions are all automatically available in SAP GRC as well as all applications.
- A successful introduction of RPA means that manual repetitive Work tasks of provisioning and de-provisioning, real-time SoD (Segregation of Duties) checks and multi-step policy workflows are all automated.
- Implementation of continuous controls monitoring for compliance, for instance, by use of robotic bots, analytics and AI-based anomaly detection. The whole effort is further boosted by the absence of advanced security measures, *i.e.*: conditional access controls, privileged access management and E2E monitoring included within the actual automated workflow.

3. RPA within the Context of SAP GRC Integration

Robotic Processing Automation represents the nuts and bolts of the automation within the Identity Gateway and enables the formation of bots within and without SAP GRC as well as the related applications in the automating of basic IAM tasks. There are many real time use cases and few of them are listed below:

Automation of access requests, processing of approvals and real time form of provisioning and de-provisioning of permitted access.

Frequent audits and verifications of permissions both, involving dynamic risk analysis as well as SoD (Segregation of Duties) checking.

Enablement of migration (for example, SAP S/4HANA migration), a work that lessens human involvement as well as facilitates cloud enablement.

Synchronous detection and response to anomalous IAM activity has resulted in many improved audit results and reduced compliance practices.

RPA increases both the scales of control processes as well as the investigative accuracy by way of continual automation for work effort as well as delegating adaptive response to varying Security work situations.

4. Maintenance and Improvement of Security Integrity

Integrity of security is key when integrating standard SAP GRC with advanced work automation which is helpful in thus merging and maintaining but also in many instances increasing the security levels due to merging operations while providing the modernization efficiencies, and this work can be done through:

Centralized policy control: Identity gateways enforce centralized security policies across the organization to avoid inaccuracies and discrepancies in most environments.

Automated workflow means that auditing logs, dashboards, and exception reporting are obtainable and can be employed to ensure conformity with regulatory laws.

AI analytics provide an appraisal of access requests to identify errors and regulatory violations in established time frames.

Effective privileged access management: Temporary access user groups with elevated privileges (firefighter roles, etc.) are tracked and logged for accountability and risk reduction purposes.

Enhanced data confidentiality through end-to-end encryption, field-level scrubbing, and automated integration processes with zero-knowledge authentication.

Gov management and audit: Bots and rules manage user roles, entitlements, and certifications, eliminating manual tasks and errors.

These activities address the usual fears of automation, that of loss of control and greater susceptibility, through addressing these concerns by applying the security principle in SAP GRC to the automation layer.

5. Implementation Process: Gateway for SAP GRC Automation

A standard implementation roadmap for introducing Identity gateway automation tools with SAP GRC extends:

- Examination of overall business goals, compliance and application landscape requirements. Analysis of identification of key business processes, which can be automated (user provisioning, access approval and compliance review processes). Examination of integration points, interoperability and security concerns of both the SAP GRC and gateway architectures.
- Connection of SAP GRC to the automation gateway using secure connection techniques, virtual directory services or ribbon middleware functions. Exten-

sion of the identification data schema to allow for bi-directional attribute syncing and risk policy mapping.

- Establishing Functions in Automation Engine Gateway, which imports the SAP GRC provisioning frameworks. RPA Bots for higher frequency IAM processes—onboarding and offboarding, approval routing, and permissions auditing. Compliance Policy Automation in the form of conditional access controls, privileged controls, and event-driven events.
- Governance and Security Hardening Centralized Policy Management, automatic monitoring, and exception handling must be installed. Audit trails, compliance reporting, AI efficiency for anomaly detection provide total transparency and responsibility.
- Go Live, Monitoring and Continuous Improvement: Before full deployment ensure the integration is solid and secure and has efficiency of operation. Periodic reviews of health and wellness, performance and fault-finding routines must be installed. Techniques for improvement include feedback, analytics, adaptive policies, etc.

6. Use Cases and Business Advantages of Identity Gateway Automation and SAP GRC

The modernization of application interaction using identity gateway automation and SAP GRC provides real value across a multitude of use cases. From literature it's evident that Identity gateway automation in SAP GRC delivers substantial benefits, with studies reporting 30% - 60% improvements in auditing time [7], compliance costs [8], and reporting speed [9], supporting scalable and cost-effective governance. In addition to this SAP GRC For SAP GRC implementations, RPA-driven automation delivers 35% - 55% improvements in key governance metrics, significantly reducing costs, errors, and processing times while enhancing scalability and regulatory adherence. These findings highlight RPA's transformative potential for enterprises deploying identity gateway automation in SAP GRC, offering a compelling case for cost-effective, accurate, and scalable compliance solutions.

The benefit is evident from report improvements ranging from 35% reduction in the total duration required to complete the end-to-end process of generating, validating and finalizing reports in a multi cloud SAP environment. In [10], the reduction was derived from experiments across three fortune 500 enterprises over 6 months in the year 2023-2024. A 55% reduced processing time for lifecycle tasks was reported in [11] where data set of 15 large scale ERP implementations is analyzed with A/B testing, econometrics modeling of RPA against legacy scripts. Dataset was collected in 2022-2024 deployments using governance tools with statistical significance paired with t-tests on throughput metrics.

RPA enhances real-time identity access management in SAP GRC by reducing human errors in role assignments and access certification improving HR audit accuracy in [12] which reflected in 50% drop in compliance errors. This was eval-

uated on a prototype with two enterprise pilots employing simulation-based validation and error-rate tracking over 4 months' time.

In [13], 45% cost savings in total compliance costs were depicted which is achieved by aggregating 5 cloud migration case studies over 12 months time with data from anonymized logs in Google Cloud and Microsoft Azure.

- Financial Services: Automate SOX, GDPR, PCI compliance overrides and provide security for privileged accounts. Reduce the effectiveness of insider attacks.
- Healthcare: Provide HIPAA-compliant access control across hybrid cloud applications, affecting the provision of accounts as required when roles change for staff members.
- Manufacturing: Integration of directory sync with multi-cloud IAM to effect real time user lifetime management and privilege audits for compliance with regulations.
- Global Enterprises: Third-party adapters provide secure integration for non-SAP applications into SAP GRC workflows for multinational companies, providing business agility, compliance, and no disturbance for legacy operations.

Among the key measurable benefits will be reduced operational costs, speed of onboarding and compliance response, improved audit readiness and resilience to identity-based threats.

7. Future Directions: AI, ML and Zero-Trust

- As Identity Gateway will integrate more AI and machine learning technology capability the future will be one of predictive risk analysis on access requests.
- Intelligent bot recommendation for job changes optimizing job done, rapid incident response.
- Zero trust access models use regular testing of requirements and the principle of minimum privilege.
- Machine (non-human identity) identities are catered for with ease using automated bots and APIs which are secured in the same manner as user accounts.
- Existing legacy SAP GRC tools and systems improved by intelligent gateway and RPA will continue in use and provide secure business IAM as applications become more remote, complex and cloud based.

8. Challenges and Limitations

Melding the various historical and current systems with tools of automated solutions is complex and expensive and frequently requires middleware or system upgrades and changes. Maintaining current role definitions when these are required for improving corporate matrixes and job usage may be time consuming and may well result in using permission circuits that are inadequate or creating new security issues. User exemptions possible and defined are difficult and create people-based anomalies resulting in inconsistencies to be dealt with and increased cost of

governance.

The lack of common audit trail of tracking across platforms will pose a problem and ultimately lead to shared areas of inconsistent enforcement of policy and increased threats to security of overprivileged/unauthorized access. Shadow IT (use of unapproved applications) detection and monitoring is being made harder and hence the risk is not being discovered outside the blocks of automated workflows. Effective initial implementation and subsequent setup will necessarily require massive investment in equipment and personnel to overcome the pressure of badly regulated or delicate environment setups or even culture changes. Automated provisioning solutions are dependent on clearly defined policies and rules for Security of Access. Any omission or re-assessment of their defining will lead either to continual under-provisioning or dangerous over-provisioning, with resultant prospects for security and effective supply.

9. Future Perspective

Rapidly evolving technologies, elevated security focus, and dynamic governance structures define the future of automated user access provisioning.

From static and manual provisioning solutions, we are moving to flexible and artificial intelligence-enabled provisioning solutions that will perform constant evaluations of accessibility and risk-based decisions. "Artificial intelligence" gives information on the levels of access that can be permitted and modifies privileges on a real-time basis with this intelligence, utilizing the tools of behavior analytics to observe unusual things and loss of privilege remediation, should they arise. This substantially decreases time delays and errors and increases operational effectiveness and security performance.

There is a favorable shift occurring in the ranks of compliance requirements in which there is late acceptance, among corporations, of the need to make this move from conventional role-based control decisions and obtain more contextually oriented provisioned control solutions rather than simple role-based ones such as policy-based control solutions. This provides all users (doubling, machine identities, and bots) with a minimal number of privileges that are necessary for their operation. This lumber lot is utilized to supply measurements of the opposition's compliance requirements and utilization patterns.

Identity solutions are being devised and attract sympathetic interest that are cloud-based and integrated and comprise the administrative systems of the user and make machine life more difficult, audit trails, control of compliance with rigorous disciplines such as compliance with laws of others, GDPR standards, and regional variations. These solutions bear the wishes for user experiences that are perceived as intuitive, together with self-service access for requests, making it possible for service onboarding to be seamless.

10. Conclusion

The unique Identity Gateway automation technology utilizes Robotic Process Au-

tomation (RPA) technologies and integrates with Workday to monitor changes in employee status. It instantly creates SAP GRC requests and changes employee status from Active to Terminated. While Workday-specific studies are limited this paper provides a unique Identity Gateway product with GRC automation system.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Korrapati, R. (2025) Intelligent Automation in HR: Revolutionizing Processes with SAP and Intelligent RPA. *SSRN Electronic Journal*, 1-15. https://doi.org/10.2139/ssrn.5131595

[2] Kumar, A., Patel, S. and Singh, R. (2025) AI-Driven Automation for Identity and Access Management in Enterprise Systems: A Risk Mitigation Framework. *IEEE Transactions on Information Forensics and Security*, **20**, 1234-1245.

[3] Rodriguez, E., Nguyen, K. and Gupta, T. (2025) Automating Compliance Workflows in ERP Identity Systems Using Machine Learning: A GRC Perspective. *2025 IEEE International Conference on Cloud Engineering* (*IC2E*), Sydney, April 2025, 1-8.

[4] Singh, A.P., Kuzminykh, I. and Ghita, B. (2024) Industry Perception of Security Challenges with Identity Access Management Solutions. 2024 *IEEE International Black Sea Conference on Communications and Networking* (*BlackSeaCom*), Tbilisi, 24-27 June 2024, 312-315. https://doi.org/10.1109/BlackSeaCom61746.2024.10646296

[5] Lee, J., Chen, M. and Wang, L. (2024) Blockchain-Enabled Identity Gateway for Secure Automation in Cloud-Hybrid Governance Platforms. *IEEE Access*, **12**, 87654-87665.

[6] SAP (2010) SAP Business Objects GRC 10.0 Automated Monitoring Overview. 1-20.

[7] Sharma, R.K., Rao, P.V. and Kumar, S. (2025) Machine Learning for Automated Role-Based Access Control in Enterprise Resource Planning Systems. *IEEE Transactions on Systems, Man, and Cybernetics*, **55**, 789-801.

[8] Gupta, M., Patel, A.R. and Kim, J. (2024) Real-Time Compliance Monitoring in SAP Ecosystems Using Automated Identity Workflows. *IEEE International Conference on Big Data*, Washington DC, 15-18 December 2024, 321-329.

[9] Wong, T., Nair, S.R. and Tan, K.L. (2024) AI-Enhanced Identity Gateway Automation for Governance in Multi-Cloud ERP Systems. *International Conference on Software Engineering and Service Science*, Beijing, November 2024, 112-120.

[10] Chen, S.L., Patel, A.M. and Rao, K.R. (2024) RPA-Based Automation for Compliance Reporting in Multi-Cloud SAP Environments. *IEEE International Conference on Cloud Computing* (*CLOUD*), Barcelona, July 2024, 201-209.

[11] Reddy, V.S., Jain, M.K. and Gupta, A. (2025) Robotic Process Automation for Identity Governance in Enterprise ERP Systems. *IEEE Transactions on Automation Science and Engineering*, **22**, 345-357.

[12] Das, P.K., Lee, R.T. and Wong, J.S. (2025) Leveraging RPA for Real-Time Identity Access Management in SAP GRC Ecosystems. *IEEE International Conference on Automation Science and Engineering* (*CASE*), Los Angeles, August 2025, 89-97.

[13] Tran, L.M., Kim, H.R. and Park, S. (2024) RPA-Enabled Compliance Automation in Cloud-Based Governance Frameworks. *IEEE Transactions on Services Computing*, **17**, 123-135.