International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 1382-1388
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

RPA Integration with Identity Management Platforms: A Scalable IAM Orchestration Pattern

Neha Asthana*

Independent Researcher, USA
* **Corresponding Author Email:** reachnasthana@gmail.com - **ORCID:** 0000-0002-0047-7077

Article Info:

DOI: 10.22399/ijcesen.5033
Received : 05 January 2026
Revised : 28 February 2026
Accepted : 08 March 2026

Keywords

Identity Governance Automation,
Robotic Process Automation Orchestration,
Continuous Behavioral Authentication,
Machine Identity Lifecycle Management,
Access Control Policy Enforcement

Abstract:

The rapid proliferation of non-human identities across cloud and hybrid environments has exposed significant gaps in conventional identity governance architectures, which were designed primarily around human access patterns and periodic compliance assessment cycles. Integrating robotic process automation with identity governance platforms introduces a scalable orchestration model in which the governance platform serves exclusively as the policy and decision authority while automation agents execute provisioning tasks through a database-mediated communication layer. This separation of policy enforcement from execution responsibility eliminates uncontrolled privilege escalation and enables provisioning across applications that lack native connector support. Continuous behavioral authentication mechanisms, multi-interface communication redundancy, cryptographic audit trail enforcement, and event-driven remediation together form a unified control architecture that extends identity assurance beyond point-in-time verification into the full operational lifecycle. Quantifiable improvements in provisioning speed, compliance accuracy, breach risk reduction, and administrative cost confirm that governance-centric automation delivers measurable security and operational value across regulated enterprise environments.

1. Introduction

Identity and Access Management (IAM) has become more complex as non-human identities have proliferated and RPA (Robotic Process Automation) platforms have become widely accepted within enterprise business processes. Identity governance tools such as IdentityIQ that safeguard and manage human identities are not enough to protect and oversee automated enterprise business processes. Machine identities, including those for service accounts, application programming interfaces (APIs), IoT devices, and RPA bot credentials, contribute to over 60% of all credentials in the cloud [1]. The increasing prevalence of non-human-based machine identities in cloud environments is expected to continue as organizations expect more than 25 billion IoT devices to require machine identities by 2030. Machine-identity lifecycle management reduces the potential for unauthorized access through compromised credentials or keys [1].

Over 50% of organizations report that machine-identity lifecycle management (certificate provisioning, key rotation, and credential decommissioning) is a key operational challenge [1]. Adding RPA automation capability to provision identities into siloed accounts, applications, and systems that do not have native connectors can significantly enhance governance efficiency while maintaining policy control. Organizations without automation and monitoring may be more susceptible to attack methods such as credential sprawl, orphaned identities, and other vectors that allow unauthorized access [1].

The connection between robotic process automation and identity governance platforms offers a way to manage IAM functions that can grow and be checked easily. Enterprises that use automated identity governance processes have a 50% lower risk of a breach related to expired or orphaned certificates than organizations that provision manually [1]. AI-powered monitoring and RPA automation can reduce the mean time to resolution by 30-40% when compared to a non-automated reactive model [1]. Applying automation to identity lifecycle processes also yields operational benefits. For example, once operationalized, the cloud or

hybrid environment can be up to 30% less expensive than other models due to reduced administrative overhead [1].

A potential downside of combining identity governance and RPA is security. Governance policies and rights management must ensure that identity controls are the exclusive source of policy and approval decisions, while RPA provisions are directed to target systems and applications, especially those without APIs. The paper discusses the reference architecture, integration patterns, and measurable uplift delivered by a best-practice RPA-IAM project; the lifecycle management constructs; the ownership and accountability model; and the continuous monitoring framework to give readers the tools to construct governance models that reduce identity security risk while increasing provisioning speed and compliance posture [2].

2. Architecture Overview

Identity governance and administration (IGA) platforms continue to evolve to manage identities across heterogeneous infrastructure landscapes. Attestations and access reviews at regular intervals are not sufficient to manage identities at scale, particularly in environments having automated workloads and distributed services that communicate across organizational boundaries and trust domains. In conjunction with identity lifecycle management, AI-enabled governance frameworks provide a method of extending compliance enforcement mechanisms outside of provisioning events to the operational runtime of applications and services.

The deployment of AI-based data governance frameworks within enterprise identity architectures has shown success in improving privacy, compliance, and operational efficiency. Anomaly detection models in data governance frameworks have demonstrated an accuracy of 95% in detecting unauthorized access attempts during live data processing. Organizations that have employed AI data governance frameworks have reduced data breach incidents by 70% compared to legacy data governance frameworks [3]. Automation of classification and policy enforcement workflows resulted in a 60% reduction in manual review effort, allowing governance teams to focus their efforts on higher-risk entitlements and access exceptions rather than on customary access certification reviews. These quantitative benefits reflect an architectural shift from audit-driven to continuously enforced, intelligence-driven access control for identity governance platforms [3] .

Identity and supply chain attacks have compelled organizations to build more advanced identity governance architecture that considers compliance assurance beyond the development pipeline. Supply chain attacks globally increased 742% from 2019 to 2021. Targeted attacks are using dependency injection and credential compromise to bypass perimeter-based security controls [4]. Given that there were 245,000 malicious OSDs identified and blocked in 2022 alone, more than double the number observed in the prior years combined, it's clear that point-in-time compliance validation isn't a sufficient stand-alone governance solution. These attack vectors leverage the gulf between pipeline-based compliance checks and runtime identity-based trust, both of which AI-enabled governance tools are ideally placed to address.

Modern identity governance architectures for adaptive compliance must incorporate behavioral analytics, machine learning, and anomaly detection, as well as continuous monitoring to understand changes in access behavior and the dynamic attack surface. Identity data across a range of heterogeneous stores—directory services, human resource management systems, cloud identity providers, and in-application entitlement repositories—must be integrated and normalized to enable access risk decisions. This extends identity governance beyond provisioning processes to consider application vulnerability posture continuously during runtime, enforcing zero-trust principles through the entire identity lifecycle, rather than only focusing on the pre-deployment state [4].

Combining AI-enabled governance with continuous identity assurance transforms customary control from a periodic to a continuous process that detects and reacts to compliance violations in real time by embedding policy checks into workflows of provisioning and attestation: governance platforms can automatically quarantine non-compliant workloads, reducing mean time to remediate compliance violations and the time during which newly discovered security vulnerabilities or entitlement anomalies could pose risk to the cloud environment [3].

3. High-Level Integration Pattern

3.1 IIQ-Driven Workflow Orchestration

In the proposed governance-centric integration model, IdentityIQ is used as the control plane and policy engine for all access governance transactions. After the access request is approved in IIQ workflows, the IdentityIQ access request creates a structured work item message, which includes the identity identifiers, target applications, entitlements, requested operations, correlation

identifiers, and audit data (request identifiers and approval timestamps). The workflow updates the associated application record, setting it to a processing state of "ReadyForProcessing," and writes a normalized entry to a table in the database that serves as an orchestration queue. This decouples the logic that makes governance decisions from the logic that executes provisioning logic; it enables deterministic state transitions, controlled exception routing, and full audit traceability for the entire provisioning lifecycle .

3.2 Multi-Interface Communication Infrastructure

Identity governance workflows leverage multiple communication pathways to interact with distributed applications and ensure reliable provisioning across geographically dispersed infrastructure. Research on communication management for hyperconnected environments demonstrates that multi-interface deployments reduce communication loss windows significantly—systems employing combined interface strategies experience only 12 s of communication disruption compared to 118 s observed in single-interface configurations, representing a fundamental reliability improvement for environments where identity provisioning operations cannot tolerate extended connectivity gaps [5]. By using dynamic path selection strategies, governance systems can be made to shift traffic across available interfaces in real time. Two-hop wireless communication paths achieve round-trip times of 21 ms, enabling governance platforms to maintain responsive identity verification even when primary communication links become temporarily unavailable [5]. In distributed cloud environments where provisioning operations must sustain throughput across concurrent workloads, multi-interface architectures support the continuity and availability requirements that identity governance at an enterprise scale demands.

3.3 Continuous Behavioral Authentication

Beyond communication infrastructure, identity governance requires a set of authentication systems that can provide continuous authentication in the entire identity lifecycle. Machine learning of physiological/behavioural signals from sensor-based systems can be used to build such continuous authentication methods, which can cope with a drift in user behavior over time at a considerably higher fidelity than single-factor or static authentication methods [6]. Convolutional neural network architectures followed by long short-term memory networks, combined with behavioral and biosignal data, achieve 97% classification accuracy, showing a novel application of behavioral pattern recognition to provide higher assurance and continuous identity verification throughout the provisioning lifecycle, integrated with identity governance workflows, allowing access decisions to be responsive and adaptable to behavioral anomalies rather than depending solely on possession of credentials to maintain trust.

3.4 Event-Driven Remediation and Continuous Monitoring

Communication infrastructure supporting identity governance must also sustain sufficient throughput capacity to handle concurrent provisioning workloads without degradation. Research demonstrates that when aggregate traffic across simultaneous provisioning channels approaches bandwidth thresholds of 7 Mb/s on individual interfaces, load-balancing mechanisms must dynamically redistribute flows across available pathways to prevent packet loss and maintain provisioning accuracy [5]. Policy violations or deviations from behavioral baselines detected by continuous monitoring trigger provisioning and remediation workflows in the governance platform. This shifts access governance to behavior-based decision systems (beyond periodic access reviews) that track identities throughout their operational lifecycle and rapidly respond to unauthorized access patterns across a dynamic estate of applications.

4. Execution Flow and Implementation

The execution model of the IIQ-RPA integration is a sequencer-governed process providing scalable automation across a heterogeneous application portfolio. With distinct boundaries between policy evaluation, task execution, and audit logging, the governance control plane ensures that tasks cannot provision a change in the system until appropriate approvals are obtained.

4．1 Workflow Initiation and Staging of Tasks

Once a request is approved, IdentityIQ will run all approval processes, including the requestor's identity validation, manager approval, compliance policy validation, segregation of duties validation, etc. IIQ then creates application records in the integration database tables with metadata and updates the "ReadyForProcessing" status to indicate that the records are ready for processing. These are delivered using a database that includes user

IDs, entitlements, target systems, execution deadlines, and compliance context flags. This enables provisioning to disconnected systems and centralized auditing of the application portfolio.

4.2 RPA Task Retrieval and Execution

Provisioning scenarios including account creation, credential provisioning, group assignment, and application-specific entitlement configuration are completed in target systems through polling logic that retrieves work items in batches from integration tables. The RPA engine performs the required provisioning action in the target system, captures execution logs and response metadata, and posts a success, failure, partial, or retry-required status record back into the database. IIQ retrieves the status message and either completes the workflow or enters an exception-handling state for human intervention routing.

4.3 Policy Evaluation and Authorization

Access control policy enforcement at workflow entry points, rather than at individual function boundaries, provides a more efficient and proactive authorization model for IAM architectures. Proactive rejection of unauthorized requests at the gateway level prevents permissioned workflows from being exploited, with governance-integrated access control architectures outperforming unprotected implementations by 22% when unauthorized request proportions reach 30% of incoming traffic [7]. When sustained denial-of-service conditions are considered, proactive ingress-level authorization generates significant cost savings compared to standard platforms that permit unauthorized requests to partially traverse workflows before rejection [7]. These findings confirm that embedding policy evaluation at workflow entry points simultaneously reduces computational overhead and limits the attack surface available to credential-based exploitation attempts in distributed provisioning environments.

4.4 Audit Trail and Encryption in Multi-Tenant Environments

Multi-tenant cloud environments require cryptographic audit mechanisms that enforce fine-grained access policies while maintaining tamper-evident records of all provisioning events. Attribute-based encryption schemes applied to audit log infrastructure demonstrate baseline cryptographic operation times of 85 ± 4 ms for encryption and 60 ± 3 ms for decryption under five-attribute policies, establishing that cryptographic enforcement of access control within provisioning audit pipelines operates well within the latency tolerances of enterprise IAM workflows [8]. By employing hash-chaining mechanisms that detect any tampering or unauthorized modification of historical provisioning records instantly, concurrent audit logging architectures can sustain 200 records/s throughput under workloads with high concurrency without compromising integrity [8]. These cryptographic guarantees provide assurance that the RPA-controlled provisioning activity's audit trail is compliant with the requirements of regulated industries' governing frameworks.

4.5 Architectural Characteristics

This governance-centric integration model demonstrates how policy enforcement decoupled from execution automation via database intermediation delivers deterministic state transitions, controlled exception routing, full auditability, and extensibility across diverse automation use cases while preventing unattended privilege escalation.

5. Performance Gains and Quantifiable Benefits

Research demonstrates that integrating RPA with AI/ML enhances process efficiency, boosts accuracy, and reduces costs in healthcare and administrative processes. A systematic review of AI/ML and RPA applications in healthcare shows that the performance of these implementations can vary considerably. The best implementations achieve a 94% accuracy and an 85% precision within RPA implementations, which is the highest reported in the literature [9]. This indicates that smart automation can successfully perform complex healthcare end-to-end processes with low error rates when designed and integrated effectively.

Comparative studies of RPA usage have also been performed. Silva Maria and Ahmed Al-Mansouri compared the use of RPA in radiological diagnostic systems and found that RPA achieved an 85% accuracy and 80% precision [9]. Barla, Nilesh, Harshit, et al. investigated RPA in healthcare systems and found at least an 80% accuracy rate and 75% precision [9]. Silva further investigated RPA in specialized healthcare and diagnostic imaging with deep learning. Barla studies the application of RPA to operational issues within health care during COVID-19 and in key areas of care delivery [9].

Additionally, RPA has increased the accuracy and reduced the time consumption and cost. Patel and Singh used RPA in their human resources case

study and mentioned that the time of processing documents such as ID card generation and validation reduced by 75%, according to Ashwini Rahude et al. [10]. All of these improvements may reduce the amount of human labor necessary, allowing more time for human judgment and decision-making.

Overall RPA automation of administrative processes can result in processing time reductions of up to 70%. Automating low-value, repetitive, rule-based work results in substantial productivity savings, particularly in ID card production, data entry, and information processing workstreams [10]. Industry benchmarks for RPA implementation in similar working practices report processing time reductions of greater than 50% in healthcare, HR, and school administration [10]. These performance improvements reduce operational costs, improve data accuracy, and enhance organizational agility in the face of growing administrative burden on institutions.

Combining governance elements of RPA orchestration with an identity platform can make policy decisions much more efficient, accurate, and compliant by allowing the policy to be enforced rather than merely delegating it to the RPA agents. The database-mediated communication pattern improves the accuracy of provisioning handoffs and provides full audit capability.

AI/ML and RPA adoption can improve accuracy by 80% to 94% and precision by 75% to 85%. Cycle times can be reduced by 50% to 75%. This is part of the AI, ML, and RPA-led digital transformation business case for healthcare revenue management, identity management, and back-office administrative processes, where accuracy and efficiency have traditionally been seen as difficult to achieve.

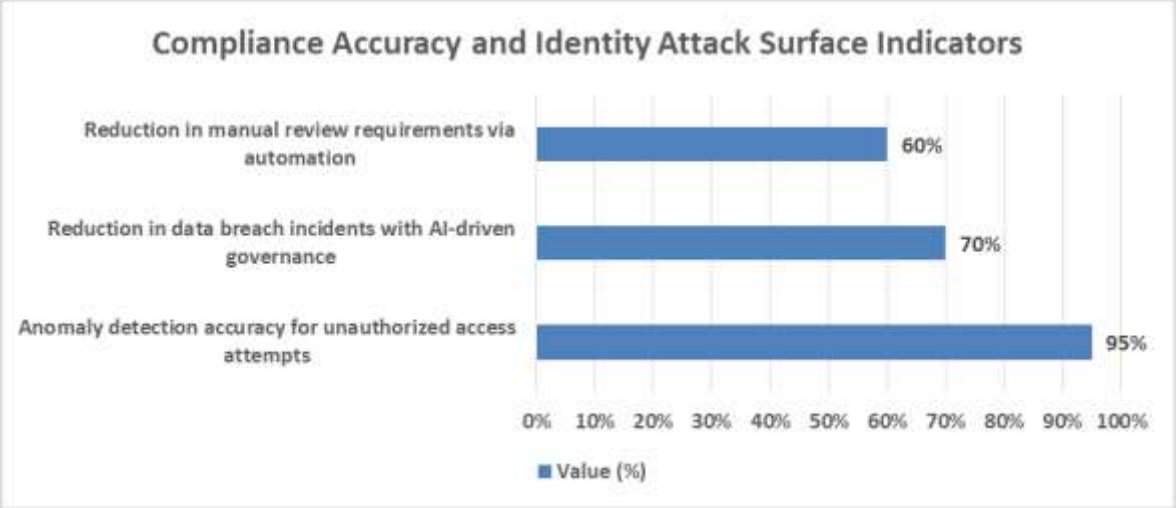

Figure 1: *Compliance Accuracy and Identity Attack Surface Indicators [3, 4]*

Table 1: *Machine Identity Proliferation and Operational Cost Impact Metrics [1, 2]*

Identity and Risk Metric	Value
Machine Identity Credential Share in Cloud Environments	60%
Projected Global IoT Devices Requiring Machine Identities (2030)	25 billion
Breach Risk Reduction with Automated Governance	50%
Mean Time to Resolution Improvement (AI-Powered Monitoring)	30-40%
Operational Cost Reduction Range (Cloud/Hybrid)	Up to 30%

Table 2: *Cryptographic Operation Times and Authorization Performance Indicators [7, 8]*

Metric	Value
Performance improvement at 30% bad traffic	22%
Encryption time under five-attribute policy	85 ± 4 ms
Decryption time under five-attribute policy	60 ± 3 ms
Concurrent audit logging throughput without integrity loss	200 records/s
Unauthorized request proportion triggering performance advantage	30%

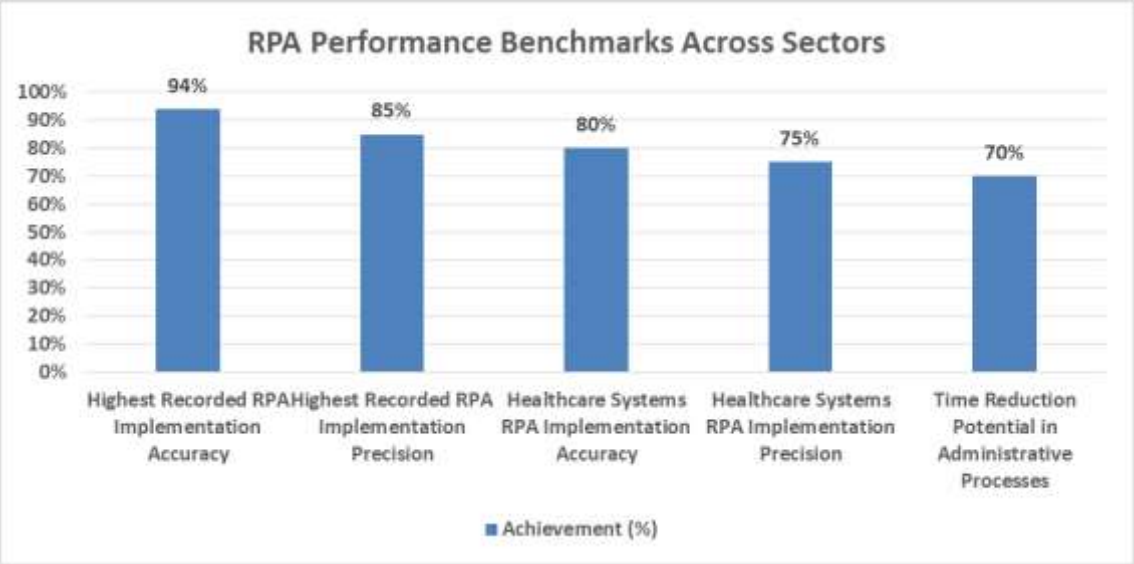

Figure 2: *RPA Performance Benchmarks Across Sectors [9, 10]*

4. Conclusions

Governance-centric automation represents a foundational advancement in how identity lifecycle operations are managed across distributed and cloud-native enterprise environments. By utilizing an identity governance platform as the sole decision-making authority and executing robotic process automation by leveraging a structured database intermediation layer, the provisioning architecture becomes scalable, auditable, and immune to privilege escalation. Multi-interface communication redundancy, continuous behavioral authentication, cryptographic audit enforcement, and proactive policy evaluation at workflow ingress points collectively address both infrastructure reliability and credential security dimensions of identity management. Data from healthcare, administrative services, and finance shows that intelligent automation dramatically improves provisioning speed, compliance posture, and operational cost efficiency. The exponential growth of non-human identity volumes and industry regulations suggests that governance-driven automation should be viewed as a long-term architectural requirement, helping organizations achieve a high degree of identity governance and control while permitting the continued acceleration of digital transformation in diverse application estates.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Anant Wairagade, "Machine Identity Security in Cloud & AI: Ensuring Lifecycle Management, Ownership, and Accountability for Non-Human Identities," IJCTT, Feb. 2025. Available: https://www.ijcttjournal.org/2025/Volume-73%20Issue-2/IJCTT-V73I2P110.pdf

[2] Saranya Balaguru, "Securing Automated Intelligence: Challenges and Solutions in RPA and Generative AI Integration," IJFMR, 2024. Available: https://www.ijfmr.com/papers/2024/5/27900.pdf

[3] Narendra Devarasetty, "AI-Driven Data Governance Frameworks for Enhanced Privacy and Compliance," IJSRM, 2023. Available: https://ijsrm.net/index.php/ijsrm/article/view/4380/3768

[4] Diego Gama et al., "Supporting continuous vulnerability compliance through automated identity provisioning," ACM, 2024. Available: https://dl.acm.org/doi/epdf/10.1145/3697090.3697098

[5] Victor Sanchez-Aguero et al., "Communication Manager for Hyper-Connected RPAS Environments," MDPI, 2023. Available: https://www.mdpi.com/2504-446X/7/2/137

[6] Hend S. Saad et al., "Employing machine learning and wearable devices in healthcare systems: tasks and challenges," Springer Nature, 2024. Available: https://link.springer.com/article/10.1007/s00521-024-10197-z

[7] Arnav Sankaran et al., "Workflow Integration Alleviates Identity and Access Management in Serverless Computing," ACM, 2020. Available: https://dl.acm.org/doi/epdf/10.1145/3427228.3427665

[8] Rakesh Pal, "Secure Cloud Storage with Attribute-Based Encryption and Audit Logs," IJARCSE, Sep. 2025. Available: https://ijarcse.org/index.php/ijarcse/article/view/76/95

[9] Kiran Babu Macha, "Integrating AI, ML, and RPA for end-to-end digital transformation in healthcare," WJARR, Jan. 2025. Available: https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-0264.pdf

[10] Ashwini Rahude et al., "Robotic Process Automation: ID Card Generation System," IJSET, 2025. Available: https://www.ijset.in/wp-content/uploads/IJSET_V13_issue2_327.pdf