CROSSIDENTITY
IAM CONVERGED

Cross Identity IAM in Insurance

+91 901 926 6824 inquiry@crossidentity.com www.crossidentity.com

Table of Contents

1. Executive Overview

1.1 Insurance in a Digitally Expanding Risk Environment

Global insurance organizations operate in an environment defined by digital distribution, ecosystem partnerships, and increasing customer expectations for seamless service. Policy issuance, claims processing, underwriting, renewals, and customer engagement are increasingly delivered through digital platforms that connect policyholders, agents, brokers, third-party administrators, and partners.

As insurance operations scale across products and geographies, the number of identities interacting with sensitive systems and data grows rapidly.

1.2 Identity as the Foundation of Trust and Security

In insurance, identity is central to trust. Every policy transaction, claim submission, settlement decision, and system change is tied to an identity. Weak identity controls expose insurers to fraud, data breaches, regulatory findings, and reputational damage.

Identity must therefore function as a foundational security control rather than a supporting IT capability.

1.3 The Limits of Traditional Security Approaches

Traditional security models based on network perimeters, isolated access controls, or standalone tools struggle to address the complexity of modern insurance environments. Diverse identity populations, outsourced operations, and automation introduce risks that fragmented tools cannot consistently manage.

These limitations often lead to inconsistent enforcement, delayed detection of misuse, and reliance on manual controls.

1.4 Cybersecurity-as-an-Infrastructure for Insurance

Cybersecurity-as-an-Infrastructure represents a shift toward embedded, always-on security controls that scale with the organization. For insurance, this means treating identity as core infrastructure that governs access consistently across policyholders, employees, agents, partners, and automation.

This approach enables insurers to balance digital growth with security, compliance, and operational resilience.

1.5 Purpose and Scope of This Report

This report presents a global, convergence-led perspective on identity security for insurance organizations. It explores the business and regulatory impact of identity failures, examines why fragmented tools fall short, and explains how a converged identity security model supports fraud prevention, regulatory confidence, and secure digital transformation.

2. The Insurance IAM Challenge: Policyholder Trust, Scale, and Complexity

2.1 Expanding Digital Insurance Operations

Insurance organizations are increasingly digital-first, with policy onboarding, renewals, endorsements, and claims processing executed through online portals, mobile apps, and partner platforms. These digital channels improve customer experience but significantly expand the identity surface that must be secured and governed.

As insurers scale across products and regions, managing access consistently across systems becomes more complex.

2.2 Diverse Identity Populations Across the Insurance Value Chain

Insurance environments involve a wide range of identity types, including policyholders, employees, agents, brokers, third-party administrators, surveyors, and service partners. Each group requires different access levels, responsibilities, and controls, often across multiple systems.

Governing access across this diverse population is a central identity challenge for insurers.

2.3 Claims Processing and Fraud Risk

Claims workflows are particularly sensitive to identity failures. Weak authentication, excessive access, or poor segregation of duties can enable fraudulent claims, unauthorized settlements, or manipulation of claim data. Because claims operations often involve multiple internal and external actors, identity governance must be precise and consistently enforced.

Identity weaknesses in claims environments can directly translate into financial loss and customer dissatisfaction.

2.4 Outsourced and Third-Party Access Complexity

Insurance organizations rely heavily on outsourced operations and partners, including TPAs, loss assessors, repair vendors, and call centers. These external identities frequently require access to sensitive systems and customer data, increasing exposure if access is poorly scoped or retained beyond necessity.

Managing third-party identity lifecycles remains a persistent challenge.

2.5 Automation, APIs, and Non-Human Identities

Automation supports underwriting, claims triage, fraud detection, and reporting in modern insurance platforms. APIs and service accounts often operate with broad permissions to enable system-to-system communication. Without strong governance, non-human identities can become high-impact attack vectors.

Ensuring visibility and control over automation is essential to managing systemic risk.

2.6 Compounding Risk and Operational Complexity

The combination of diverse identities, outsourced operations, claims sensitivity, and automation creates compounding identity risk. Fragmented controls and manual processes struggle to keep pace, increasing exposure to fraud, compliance issues, and operational disruption.

Addressing these challenges requires identity security that functions as infrastructure—scalable, policy-driven, and embedded across the insurance ecosystem.

3.The Extended Insurance Ecosystem: Agents, Brokers, TPAs, and Vendors

3.1 Identity Beyond the Enterprise Boundary

Insurance operations extend far beyond internal employees and policyholders. Agents, brokers, third-party administrators (TPAs), surveyors, repair networks, reinsurers, and service vendors regularly require access to core systems that support underwriting, claims processing, policy servicing, and customer data.

These external identities operate outside the organizational boundary but often interact directly with high-impact financial workflows.

3.2 Distributed Authority and Financial Impact

Agents and brokers initiate policy issuance and customer interactions. TPAs and surveyors influence claims validation and settlement decisions. Vendors and service providers may access systems to update claim statuses, process documents, or manage customer communication.

Because these identities influence financial outcomes, weak access governance can directly enable fraud, unauthorized changes, or data misuse.

3.3 Lifecycle Complexity in External Relationships

Unlike employees, external actors are governed by contracts, agreements, and evolving business relationships. Agent appointments change, TPA contracts end, vendors rotate, and broker relationships expand or contract across geographies.

Without lifecycle-driven identity governance, excessive or orphaned access can persist long after business relationships change.

3.4 The Need for Ecosystem-Level Identity Governance

Modern insurance identity security must extend beyond internal workforce governance to ecosystem governance. External identities must be uniquely identifiable, scoped to defined responsibilities, time-bound where appropriate, and continuously monitored.

Governing the extended ecosystem is essential to fraud prevention, regulatory compliance, and operational resilience.

4. Business and Risk Impact of Identity Failures in Insurance

4.1 Claims Fraud and Financial Loss

Identity failures are a major driver of insurance fraud. Weak authentication, compromised customer accounts, or poorly governed agent and partner access can lead to fraudulent claims, unauthorized settlements, and manipulation of policy data. Because claims operations often involve high volumes and multiple stakeholders, fraud can scale quickly before detection.

Even small access weaknesses can result in repeated financial loss across the claims lifecycle.

4.2 Customer Trust and Reputation Damage

Insurance is a trust-driven industry. Identity incidents that expose customer data, enable unauthorized claims activity, or disrupt customer access can severely impact confidence. Customers expect insurers to protect sensitive personal and financial information, and breaches can lead to long-term reputational damage.

Loss of trust directly affects retention, brand perception, and market competitiveness.

4.3 Regulatory Exposure and Compliance Consequences

Insurance organizations are subject to oversight from financial regulators and supervisory authorities globally. Identity-related weaknesses such as excessive access, lack of auditability, weak third-party governance, or inadequate access controls can trigger regulatory findings, remediation requirements, and penalties.

Repeated compliance gaps can lead to increased supervisory scrutiny and restrictions on operations.

4.4 Operational Disruption and Remediation Cost

When identity issues occur, insurers often face operational disruption through emergency access reviews, account resets, system restrictions, and incident investigations. These efforts consume resources across IT, security, claims operations, compliance, and customer support teams.

Remediation costs can be significant, often exceeding the direct impact of the initial incident.

4.5 Insider Risk and Privilege Misuse

Insurance environments involve sensitive access to claims, payouts, customer records, and underwriting rules. Excessive access or weak segregation of duties can allow insiders to manipulate approvals, alter claim outcomes, or misuse privileged system access.

Insider-driven incidents are particularly difficult to detect without strong identity governance and audit trails.

4.6 Constraints on Digital Transformation and Ecosystem Growth

Identity failures slow down innovation. Insurers may hesitate to expand digital channels, integrate new partners, or adopt automation if identity controls are fragmented or inconsistent. Identity risk becomes a barrier to growth, limiting the ability to modernize operations and improve customer experience.

Strengthening identity governance enables insurers to scale confidently while maintaining security and regulatory confidence.

5. Why Fragmented IAM Tools Fail in Insurance Environments

5.1 Tool Sprawl Across Core Insurance Functions

Insurance organizations often deploy identity-related tools incrementally across underwriting, claims, customer portals, agent systems, and IT operations. Authentication, access management, privileged access, fraud controls, and logging are frequently implemented as separate solutions to meet immediate needs. Over time, this creates a fragmented identity landscape that is difficult to manage consistently.

Tool sprawl increases complexity at the exact point where insurers need clarity and control.

5.2 No Single View of Identity and Access

Fragmented tools maintain independent views of users, roles, and access rights. One system may track customer authentication, another agent access, and a third privileged system changes. These tools rarely share real-time context or lifecycle information.

As a result, insurers struggle to answer basic questions such as who has access to what, why that access exists, and whether it is still appropriate.

5.3 Manual Workarounds and Process Dependency

To compensate for disconnected tools, insurance teams rely heavily on manual processes such as spreadsheets, email approvals, and periodic reconciliations. These workarounds introduce delays, increase error rates, and reduce confidence in access governance.

Manual identity processes are especially risky in claims environments where speed and accuracy are critical.

5.4 Inconsistent Policy Enforcement Across Systems

Fragmentation leads to uneven enforcement of identity policies. Role changes may be updated in one system but not reflected in others. Third-party access may be tightly controlled in some workflows and loosely governed in others. Privileged access controls often vary by environment.

This inconsistency creates exploitable gaps and weakens the overall security posture.

5.5 Delayed Detection of Fraud and Misuse

Without unified identity context, detecting identity-related abuse becomes reactive. Signals such as unusual claims activity, excessive access, or misuse of service accounts may go unnoticed until financial or operational damage has occurred.

Delayed detection increases the scale and impact of fraud and insider misuse.

5.6 Fragmentation Conflicts with Cybersecurity-as-an-Infrastructure

Cybersecurity-as-an-Infrastructure requires identity controls to be embedded, automated, and continuously enforced. Fragmented identity tools that rely on manual coordination and point-in-time checks cannot meet this requirement.

For insurers operating at scale, fragmentation becomes a structural barrier to secure, resilient operations.

6. From Fragmentation to Convergence: Identity Security for Modern Insurance Operations

6.1 Convergence as a Business and Risk Requirement

For insurance organizations, identity convergence is not simply a technology upgrade. It is a business and risk requirement driven by fraud exposure, regulatory expectations, and ecosystem complexity. Convergence unifies identity governance, access enforcement, monitoring, and auditability into a single framework that supports secure operations at scale. This shift enables insurers to strengthen control without slowing down customer and claims processes.

6.2 Identity as the Central Control Plane

In a converged model, identity becomes the central control plane governing access across underwriting, claims, customer portals, agent systems, and internal operations. Every access request—whether from a policyholder, employee, broker, partner, or automated system—is evaluated using shared identity context, including role, entitlement, lifecycle state, and risk. This enables consistent enforcement across systems and reduces exposure created by disconnected tools.

6.3 Lifecycle-Driven Access Governance

Convergence connects identity lifecycle events directly to access governance. Onboarding, role changes, partner onboarding, contract completion, and exits trigger automatic access updates across systems. This reduces privilege creep and prevents orphan accounts from persisting.

For insurance organizations managing large employee, agent, and partner populations, lifecycle-driven governance is essential for maintaining long-term control.

6.4 Embedded Segregation of Duties for Claims and Approvals

Claims and settlement processes require strong control integrity. A converged identity model enforces segregation of duties through system-level roles and workflows, ensuring that high-risk actions such as claim approvals, settlement overrides, and payout authorization cannot be completed end-to-end by a single identity.

This reduces fraud risk and strengthens accountability across claims operations.

6.5 Unified Governance for Partners, Agents, and Non-Human Identities

Insurance ecosystems rely on agents, brokers, TPAs, surveyors, repair networks, and automated integrations. Converged identity security extends governance beyond employees to include external users and non-human identities such as APIs and service accounts. Access is scoped, approved, lifecycle-managed, and monitored consistently across the ecosystem.

6.6 Continuous Visibility and Fraud-Resilient Operations

A converged model provides continuous visibility into who has access to what, why access exists, and how access is being used. This supports earlier detection of anomalous behavior and reduces reliance on reactive fraud investigations.

Unified audit trails also simplify compliance reporting and regulatory readiness.

6.7 Convergence Enables Cybersecurity-as-an-Infrastructure

By unifying identity controls into an always-on, policy-driven framework, convergence enables insurance organizations to treat identity security as infrastructure. This foundation supports fraud prevention, regulatory confidence, and resilient digital transformation while enabling insurers to scale customer experience and ecosystem partnerships securely.

7.Regulatory & Security Expectations for Insurance Identity Controls

7.1 A Global and Converging Regulatory Landscape

Insurance organizations operate under oversight from financial regulators, supervisory authorities, and data protection bodies across regions. While regulations vary by market, there is strong convergence in expectations around governance, customer data protection, fraud prevention, accountability, and operational resilience. Examples include regulators and supervisory bodies such as IRDAI, FCA, EIOPA, NAIC-aligned frameworks, MAS, and similar institutions globally.

Across these regimes, identity and access controls are consistently viewed as foundational to protecting sensitive insurance operations.

7.2 Strong Authentication and Customer Identity Protection

Regulators and security teams expect insurers to enforce strong authentication for customer access, particularly for high-risk activities such as policy updates, claims submission, beneficiary changes, and payout-related actions. Authentication controls must be consistent across digital channels and should support risk-based security for sensitive actions.

Weak customer identity controls increase fraud exposure and erode trust.

7.3 Least-Privilege Access and Role Governance

Insurance organizations are expected to implement least-privilege access aligned to defined roles and responsibilities. Over-permissioned users—especially in claims, underwriting, and finance—create exposure to fraud, data misuse, and operational errors.

Role-based access must be consistently enforced across systems and continuously updated as responsibilities change.

7.4 Segregation of Duties for Claims and Settlement Workflows

Claims processing and settlement decisions represent high-impact financial outcomes. Regulators and internal risk teams expect strong segregation of duties so that initiation, validation, approval, and payout activities are separated across roles. Systems should enforce maker-checker workflows and prevent end-to-end control by a single identity.

This reduces both insider fraud risk and unintentional operational errors.

7.5 Governance of Agent, Broker, and Third-Party Access

Insurance ecosystems depend heavily on agents, brokers, TPAs, surveyors, and service partners. Regulators expect insurers to maintain strong oversight of third-party access by ensuring permissions are scoped, monitored, and revoked promptly when no longer required.

Poor governance of external access is a major driver of compliance gaps and fraud risk.

7.6 Governance of APIs and Non-Human Identities

Automation and system integrations are essential to modern insurance platforms. APIs and service accounts often handle sensitive workflows such as policy issuance, claim processing, fraud scoring, and reporting. Regulators and security teams increasingly expect non-human identities to be uniquely identifiable, tightly scoped, and auditable.

Uncontrolled automation access can lead to systemic security failures.

7.7 Auditability, Monitoring, and Evidence of Control

Insurance organizations must be able to demonstrate that identity controls operate effectively over time. This requires reliable records of authentication events, access grants and revocations, approvals, privileged actions, and third-party access activity.

Audit-ready evidence is essential for regulatory reviews, fraud investigations, and operational risk management.

8.Mapping Regulatory and Security Expectations to Converged Identity Controls

The table below maps common regulatory and security expectations in global insurance environments to a converged identity security model. This mapping shows how Cybersecurity-as-an-Infrastructure translates expectations into system-enforced, auditable controls across policy, claims, and ecosystem operations.

Regulatory / Security Expectation	Underlying Insurance Risk	Fragmented Tool Limitation	Converged Identity Control	Business & Compliance Outcome
Strong customer authentication for sensitive actions	Account takeover and claims fraud	Authentication inconsistent across channels	Unified authentication with risk-based step-up	Lower fraud and improved customer trust
Least-privilege access aligned to roles	Excess internal access in claims/underwriting	Role changes not reflected across systems	Lifecycle-driven RBAC with automated access	Reduced insider risk and cleaner audits
Segregation of duties for claims and payouts	Self-approval of settlements and payout misuse	Manual checks; workflow controls isolated	System-enforced maker–checker workflows	Stronger claims control integrity
Controlled privileged access to critical systems	Admin misuse or compromised elevated	Privileged tools isolated from governance	Time-bound privileged access governed within	Reduced operational and breach impact
Governance of agent, broker, and TPA access	Over-permissioned external access	External identities unmanaged lifecycle	Centralized third-party identity governance with	Stronger partner oversight and compliance
Governance of APIs and non-human identities	Service account misuse and systemic abuse	Non-human identities under-governed	Unified governance for human and non-human identities	Reduced automation-driven risk
Timely access revocation	Orphan access after exits or contract ends	De-provisioning inconsistent	Policy-driven lifecycle revocation and access	Fewer security gaps and audit findings
Auditability and traceability	Unable to prove who did what and when	Evidence scattered across tools	Centralized audit trails and reporting	Faster audits and investigations

Why This Mapping Matters

In insurance, identity failures directly impact fraud exposure, claims integrity, customer trust, and regulatory posture. Fragmented identity tools introduce inconsistency and manual dependency that cannot scale with digital insurance ecosystems. A converged identity security model unifies governance, enforcement, and evidence so identity controls operate as infrastructure—embedded, always-on, and scalable.

9. Cross Identity's Converged Cybersecurity-as-an-infrastructure Platform for Insurance

9.1 Built for Fraud-Sensitive, Ecosystem-Driven Insurance Operations

Cross Identity is designed to address the fraud exposure, regulatory oversight, and ecosystem complexity that define modern insurance organizations. Built on the principle of Cybersecurity-as-an-Infrastructure, the platform embeds identity security directly into insurance operations rather than relying on disconnected tools and manual controls.

This approach enables insurers to strengthen control while maintaining speed across policy, claims, and partner workflows.

9.2 A Unified Identity Fabric Across the Insurance Ecosystem

Cross Identity unifies all identity types—policyholders, employees, agents, brokers, TPAs, service partners, APIs, and automated workflows—into a single identity fabric. Access decisions are governed through consistent, policy-driven controls that account for role, lifecycle status, and risk.

This eliminates gaps between customer identity, workforce access, privileged access, and auditability.

9.3 Lifecycle-Centric Governance for Agents and Partners

Insurance ecosystems experience frequent onboarding, role changes, and contract transitions. Cross Identity ties identity lifecycle events—such as agent onboarding, role updates, partner offboarding, and contract completion—directly to access governance.

This ensures access remains aligned with active business relationships and reduces orphan or excessive access across claims and underwriting systems.

9.4 Embedded Controls for Claims, Settlements, and Privileged Access

High-risk insurance activities such as claims approval, settlement overrides, payout authorization, and system administration are governed through embedded, system-enforced controls. Elevated access is restricted, approved, time-bound, and fully traceable within the broader identity framework.

Privileged access is treated as a regulated risk area rather than an isolated technical function.

9.5 Governance of APIs and Automated Insurance Workflows

Automation plays a critical role in underwriting decisions, fraud scoring, claims triage, and reporting. Cross Identity extends governance to APIs and non-human identities by enforcing ownership, scoped permissions, and auditable activity.

This reduces systemic risk from automation while supporting scalable digital insurance operations.

9.6 Continuous Visibility, Fraud Detection, and Audit Readiness

Cross Identity provides continuous visibility into identity access and activity across insurance systems. Centralized audit trails capture authentication events, access changes, approvals, and high-risk actions in a single, inspection-ready view.

This supports faster fraud investigations, simplified regulatory reporting, and improved operational resilience.

9.7 Enabling Secure Growth and Regulatory Confidence

By converging identity controls into a single platform, Cross Identity enables insurance organizations to expand digital channels, onboard partners, and automate workflows securely. Security, fraud prevention, and compliance are addressed together rather than in silos.

Cross Identity positions identity security as foundational infrastructure that supports trust, resilience, and sustainable growth in global insurance operations.

Cross Identity is recognized by leading analysts such as KuppingerCole as a Leader in IGA, IAG, and CIEM, validating its depth across governance, entitlement security, and continuous enforcement.

10. Implementation Approach: Adopting Cybersecurity-as-an-Infrastructure

10.1 Treat Identity as a Core Fraud and Risk Control

Insurance organizations should position identity governance as a foundational fraud, risk, and compliance capability rather than a supporting IT function. Identity directly governs access to policy, claims, underwriting, and payout workflows, making it central to financial and operational control.

10.2 Prioritize High-Risk Workflows and Sensitive Systems

Implementation should begin with high-impact areas such as claims processing, settlement approvals, payout authorization, underwriting rule management, customer data platforms, and core policy administration systems. Securing these environments early delivers immediate reduction in fraud exposure and operational risk.

10.3 Replace Manual Access Controls with Policy-Driven Automation

Disconnected identity tools often force insurers to rely on manual approvals and spreadsheet-based access reviews. A converged identity approach replaces these with automated, policy-driven governance that continuously enforces least privilege, segregation of duties, and approval workflows.

This reduces errors and strengthens control consistency across operations.

10.4 Extend Governance to Agents, Brokers, and Third-Party Administrators

Insurance ecosystems depend heavily on external access. Agents, brokers, TPAs, surveyors, and vendors must be governed with clear access scopes, lifecycle controls, and auditability. External access should be provisioned and revoked based on business relationships, role definitions, and contractual timelines.

10.5 Govern APIs and Automation as First-Class Identities

Automation is critical in digital insurance, but APIs and service accounts often operate with broad permissions. Implementation should ensure non-human identities are uniquely identifiable, owned, scoped to defined purposes, and continuously monitored.

This reduces systemic risk and prevents automation misuse.

10.6 Build Continuous Compliance and Audit Readiness

Identity controls must support continuous evidence generation rather than periodic audit preparation. Centralized audit trails, access reviews, and historical access visibility enable insurers to respond quickly to regulatory inquiries and fraud investigations.

10.7 Adopt a Phased Rollout Aligned to Business Priorities

A phased implementation approach allows insurers to secure critical functions first while minimizing disruption. Aligning identity initiatives with fraud programs, digital transformation, and ecosystem expansion ensures sustainable adoption and measurable business impact.

11. Conclusion: Identity as Cybersecurity-as-an-Infrastructure for Insurance

11.1 Identity as the Foundation of Trust and Fraud Resilience

In insurance organizations, identity underpins trust, fraud prevention, and operational integrity. Every policy action, claim decision, settlement, and system change depends on controlled and accountable access. Treating identity as Cybersecurity-as-an-Infrastructure reflects its role as a foundational capability rather than a supporting IT control.

11.2 Fragmentation Creates Persistent Risk

Fragmented identity tools introduce inconsistency, manual dependency, and limited visibility across insurance operations. At scale, these gaps translate directly into fraud exposure, regulatory findings, operational disruption, and loss of customer confidence. Fragmentation is no longer sustainable for insurers operating in digital-first, ecosystem-driven environments.

11.3 Convergence Enables Secure Digital Growth

A converged identity security model unifies governance, access enforcement, monitoring, and auditability across policyholders, employees, agents, brokers, partners, and automation. This convergence enables insurers to scale digital services, streamline claims operations, and expand ecosystems without compromising security or compliance.

11.4 Supporting Regulatory Confidence and Operational Resilience

By embedding identity controls into daily operations, insurers can maintain continuous compliance and respond confidently to regulatory reviews and fraud investigations. Centralized visibility and auditability reduce remediation burden, strengthen accountability, and support resilient operations across the insurance value chain.

11.5 A Foundation for the Future of Insurance

As insurance organizations continue to digitize and collaborate across ecosystems, identity security must function as long-term infrastructure. Cybersecurity-as-an-Infrastructure enables insurers to protect policyholders, reduce fraud, and support sustainable innovation.

When identity is treated as infrastructure, insurance organizations gain a durable foundation for trust, compliance, and scalable digital transformation.

About Cross Identity

Elevate your identity security with Cross Identity, World's #1 converged IAM platform trusted by over 1,200 organizations to secure more than 70 million identities. More than just an IAM solution, Cross Identity unifies authentication, authorization, governance, and administration into a single, seamless experience. Our platform not only enhances security and compliance but also delivers an user experience and recommended by leading analysts that set the standard for the industry.

+91 901 926 6824
inquiry@crossidentity.com
www.crossidentity.com