CROSSIDENTITY
IAM CONVERGED

IAM in Pharma

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

Table of Contents

1. Executive Overview
2. The Pharma Identity Challenge: Data Integrity, Scale, and Complexity
3. Business and Risk Impact of Identity Failures in Pharma
4. Regulatory & Security Expectations for Pharma Identity Controls
5. Mapping Regulatory and Security Expectations to Converged Identity Controls
6. Why Fragmented IAM Tools Fail in Regulated Pharma Environments
7. From Fragmentation to Convergence: Identity Security for GxP Operations
8. Cross Identity's Converged Identity Security Platform for Pharma
9. Continuous Compliance, Access Reviews & Inspection Readiness
10. Implementation Approach
11. Conclusion: Cybersecurity-as-an-Infrastructure for Pharma

1. Executive Overview

1.1 Pharma in a Highly Regulated, Data-Driven Environment

Global pharmaceutical organizations operate in one of the most regulated and data-intensive industries. Across research, clinical development, manufacturing, quality, and commercialization, pharma companies rely on complex digital systems to manage intellectual property, patient data, regulated records, and global supply chains.

As operations become more digital, distributed, and collaborative, the number of identities interacting with critical systems continues to grow—spanning employees, researchers, clinical investigators, manufacturing staff, external partners, CROs, CMOs, APIs, and automated systems.

1.2 Identity as a Foundation for Data Integrity and Trust

In pharma, identity failures do not remain confined to IT security incidents. Weak identity controls can compromise data integrity, disrupt validated processes, and undermine confidence in regulated records. These failures can directly impact regulatory compliance, product quality, and patient safety.

As a result, identity must be treated as foundational infrastructure that governs access, accountability, and traceability across all regulated processes.

1.3 The Limits of Traditional Security Approaches

Traditional security models—focused on network perimeters, isolated access controls, or standalone tools—are insufficient for modern pharma environments. These approaches struggle to manage complex identity relationships across global teams, long system lifecycles, and extensive third-party collaboration.

Fragmented identity controls often result in inconsistent enforcement, reliance on manual processes, and gaps in inspection readiness.

1.4 Cybersecurity-as-an-Infrastructure in Pharma

Cybersecurity-as-an-Infrastructure reflects a shift from reactive security measures to embedded, always-on controls that operate as part of the organization's core operating model. In pharma, this means placing identity at the center of cybersecurity, ensuring access governance is consistent, auditable, and aligned with regulatory and quality expectations.

Identity becomes the control plane through which access to regulated systems, data, and processes is continuously governed.

1.5 Purpose and Scope of This Report

This report presents a global, convergence-led perspective on identity security for pharmaceutical organizations. It examines the business and regulatory impact of identity failures, outlines regulatory and security expectations, and explains how a converged identity security model supports data integrity, inspection readiness, and secure collaboration across the pharma ecosystem.

2. The Pharma Identity Challenge: Data Integrity, Scale, and Complexity IAM in the Global Pharma Ecosystem

2.1 Expanding Digital Footprint Across the Pharma Value Chain

Pharmaceutical organizations increasingly operate through complex digital ecosystems that span research, clinical development, manufacturing, quality, regulatory affairs, and commercialization. Core activities such as laboratory research, clinical trials, batch manufacturing, quality investigations, and regulatory submissions are executed through interconnected systems across global locations.

As these digital environments expand, ensuring consistent and secure access across the entire value chain becomes significantly more challenging.

2.2 Data Integrity as a Central Operational Concern

Data integrity is a foundational requirement in pharma operations. Regulated data must be accurate, attributable, contemporaneous, and reliable throughout its lifecycle. Identity plays a critical role in enforcing these principles by ensuring that only authorized individuals can create, modify, review, or approve regulated records.

Weak identity controls—such as shared accounts, excessive permissions, or poor lifecycle governance—undermine data integrity and introduce compliance and quality risk.

2.3 Diverse and Distributed Identity Populations

Pharma organizations manage a highly diverse identity population that includes scientists, clinical staff, manufacturing operators, quality teams, IT administrators, external investigators, CROs, CMOs, and vendors. In addition, automated systems and integrations generate a growing number of non-human identities.

Governing access consistently across this mix of internal and external users, each with different responsibilities and regulatory implications, is a major operational challenge.

2.4 Long System Lifecycles and Historical Accountability

Many pharma systems operate over long lifecycles and support records that must be retained for years or even decades. During this time, personnel, roles, and organizational structures change frequently. Identity systems must therefore support long-term accountability, enabling organizations to demonstrate who had access to regulated systems at specific points in time.

Without strong identity governance, reconstructing historical access during inspections becomes difficult and resource-intensive.

2.5 Third-Party Collaboration and Oversight

Collaboration with CROs, CMOs, laboratories, and academic institutions is essential to pharma innovation and scale. However, third-party access introduces additional complexity and risk. External users often require access to regulated systems and sensitive data, making precise scoping, monitoring, and lifecycle management essential.

Inadequate oversight of third-party identities is a common source of regulatory observations and inspection findings.

2.6 Automation and Non-Human Identity Risk

Automation supports efficiency across pharma operations, from laboratory workflows to manufacturing execution and reporting. APIs and service accounts often operate with elevated privileges, yet may lack the governance applied to human users.

Without proper controls, non-human identities can become high-impact risk vectors that compromise data integrity and system reliability.

2.7 Compounding Risk Across the Ecosystem

The combination of data integrity requirements, diverse identity populations, long system lifecycles, and extensive third-party collaboration creates compounding identity risk. These challenges cannot be effectively addressed through isolated or manual controls.

Managing identity at this scale requires a unified, infrastructure-level approach that aligns security, quality, and regulatory objectives.

3. Business and Risk Impact of Identity Failures in Pharma

3.1 Data Integrity and Quality Risk

In pharmaceutical environments, identity failures directly impact data integrity. When access controls are weak, shared, or outdated, regulated records can be created, modified, or approved without proper authorization or traceability. This undermines confidence in research data, clinical results, manufacturing records, and quality documentation.

Data integrity issues are among the most serious findings during inspections and can invalidate studies, delay product approvals, or trigger remediation programs.

3.2 Regulatory Findings and Inspection Outcomes

Health authorities and inspectors closely examine access controls as part of computerized system validation and data integrity assessments. Identity-related gaps —such as shared accounts, excessive access, poor segregation of duties, or missing access history—are frequently cited in inspection observations.

Repeated findings can lead to warning letters, increased inspection frequency, or restrictions on manufacturing and clinical operations.

3.3 Impact on Patient Safety

Identity failures in regulated systems can affect patient safety indirectly but significantly. Unauthorized changes to clinical data, manufacturing parameters, or quality decisions can compromise the integrity of products and trials. Even when issues are unintentional, the inability to demonstrate control and accountability raises serious safety concerns.

In pharma, patient safety is inseparable from data and process integrity.

3.4 Operational Disruption and Remediation Effort

When identity issues are identified, organizations often must perform extensive remediation. This includes system-wide access reviews, manual validation of records, corrective actions, and re-training. These efforts consume significant resources across quality, IT, regulatory, and business teams.

Operational disruption caused by remediation can delay production, trials, and regulatory submissions.

3.5 Reputational and Partner Impact

Regulatory findings related to data integrity and access controls can damage an organization's reputation with regulators, partners, and collaborators. CROs, CMOs, and research partners may face increased scrutiny, and trust in shared data and processes can be eroded.

Rebuilding confidence after identity-related issues is time-consuming and costly.

3.6 Constraints on Innovation and Scale

Persistent identity risk limits a pharma organization's ability to scale digital initiatives, adopt new technologies, or expand collaborations. Regulatory caution, additional controls, and internal risk aversion slow innovation and reduce agility.

Proactively addressing identity governance enables organizations to pursue digital transformation while maintaining regulatory and quality confidence.

4.4. Regulatory & Security Expectations for Pharma Identity Controls

4.1 A Highly Regulated and Security-Sensitive Environment

Pharmaceutical organizations operate under extensive regulatory oversight from health authorities and supervisory bodies across regions. While specific regulations differ, there is strong alignment around expectations for data integrity, system control, accountability, and traceability. Identity and access controls are a core component of these expectations because they directly determine who can interact with regulated systems and data.

In pharma, regulatory compliance and cybersecurity objectives are deeply interconnected.

4.2 Identity Controls as a Foundation for Data Integrity

Regulators expect pharma organizations to demonstrate that access to regulated systems is controlled, justified, and attributable to individual identities. Identity controls must ensure that only authorized users can create, modify, review, or approve regulated data, and that these actions are clearly traceable.

Shared or generic accounts, informal access practices, or weak authentication undermine data integrity and are commonly cited during inspections.

4.3 Segregation of Duties in Regulated Processes

Strong segregation of duties is a recurring regulatory and security expectation across GxP environments. Activities such as data entry, review, approval, batch release, deviation closure, and change management must be performed by independent roles. Identity systems are expected to enforce these separations through role-based access and workflow controls rather than relying solely on procedural checks.

4.4 Control of Privileged and Administrative Access

Administrative and privileged access to regulated and validated systems represents a high-risk area. Regulators and security teams expect such access to be restricted, approved, time-bound, and fully traceable. Permanent elevated access should be minimized, and all privileged activity must be attributable to specific individuals or systems.

Uncontrolled privileged access poses both cybersecurity and compliance risks in pharma

4.6 Governance of Automation and Non-Human Identities

As automation and system integrations increase, regulators and security teams expect governance to extend beyond human users. APIs, service accounts, and automated workflows must be uniquely identifiable, appropriately scoped, and auditable.
Non-human identity misuse can have wide-reaching impact in pharma systems and is an emerging area of regulatory and security focus.

4.7 Auditability, Monitoring, and Evidence of Control

Pharma organizations are expected to produce reliable evidence demonstrating that identity controls are effective over time. This includes records of authentication events, access grants and revocations, approvals, and privileged activity.
Security monitoring and audit trails must support both real-time oversight and historical reconstruction during inspections, investigations, and quality reviews.

5. Why Fragmented IAM Fail in Regulated Pharma Environments

5.1 Fragmentation Across GxP Systems

Pharma organizations typically operate a wide range of regulated systems across research, clinical, manufacturing, and quality functions. Identity controls for these systems are often implemented independently, resulting in inconsistent access models and varying levels of enforcement.

This fragmentation makes it difficult to maintain uniform identity governance across GxP environments.

5.2 Lack of End-to-End Identity Context

Fragmented identity tools do not share a unified view of identity, role, and responsibility. An access management system may provision users, a separate tool may manage privileged access, and audit logs may exist in different locations.

Without a shared identity context, pharma organizations struggle to understand who has access, why access exists, and how it relates to regulated responsibilities.

5.3 Manual Controls and Validation Burden

To compensate for fragmented tools, organizations rely heavily on manual procedures, including periodic access reviews, spreadsheet-based reconciliations, and procedural checks. These manual controls increase validation effort, introduce human error, and weaken inspection readiness.

Manual processes are particularly problematic in environments that require consistent, repeatable, and auditable controls.

5.4 Inconsistent Enforcement of Data Integrity Controls

Fragmented systems enforce access policies differently across platforms. A user's role may be updated in one system but not reflected in another. Privileged access may be tightly controlled in certain environments and loosely governed in others.

This inconsistency undermines data integrity and complicates compliance with GxP expectations.

5.5 Delayed Detection of Identity-Related Risk

Fragmentation limits visibility into identity-related activity. Signals such as unusual access patterns, misuse of elevated privileges, or inappropriate third-party activity are often detected late or in isolation.

Delayed detection increases the potential impact of security incidents and regulatory findings.

5.6 Fragmentation Conflicts with Cybersecurity-as-an-Infrastructure

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

For pharma organizations, fragmentation becomes a systemic risk rather than a manageable limitation.

6. From Fragmentation to Convergence: IAM Security for GxP Operations

6.1 Convergence as a Quality and Security Imperative

For pharmaceutical organizations, identity security convergence is not only a cybersecurity initiative but a quality and compliance imperative. Convergence unifies identity governance, access enforcement, monitoring, and auditability into a single framework that supports GxP requirements across the organization.

This approach aligns identity controls with the rigor and consistency expected of regulated pharma operations.

6.2 Identity as the Control Plane for GxP Systems

In a converged model, identity serves as the central control plane governing access to regulated systems and data. Every interaction—whether initiated by a human user, external collaborator, or automated process—is evaluated against a shared identity context that includes role, authorization, and regulatory relevance.

This ensures consistent enforcement of access policies across all GxP environments.

6.3 Lifecycle-Driven Governance Across Regulated Roles

Converged identity security integrates joiner–mover–leaver processes directly into access governance. Role changes, site transfers, project assignments, and exits automatically trigger access updates across systems.

This lifecycle-driven approach is essential for maintaining long-term accountability and inspection readiness in environments with frequent organizational change.

6.4 Embedded Segregation of Duties and Approval Controls

High-risk regulated workflows require clear separation between creation, review, and approval activities. Converged identity platforms enforce segregation of duties through system-level role definitions and approval workflows rather than relying solely on procedural controls.

This reduces the risk of data manipulation and strengthens compliance with GxP expectations.

6.5 Unified Oversight of External and Non-Human Identities

Convergence extends identity governance to CROs, CMOs, vendors, APIs, and automated systems. External and non-human identities are governed using the same policies, lifecycle controls, and monitoring applied to internal users.

This unified oversight reduces risk while supporting secure collaboration and automation.

6.6 Continuous Visibility and Inspection Readiness

A converged identity model provides continuous visibility into access and activity across regulated systems. Centralized audit trails and reporting enable pharma organizations to demonstrate control effectiveness during inspections without extensive manual preparation.

Convergence supports a shift from reactive remediation to proactive quality and security assurance.

7. Mapping Regulatory and Security Expectations to Converged Identity Controls

The table below maps key pharma regulatory, quality, and security expectations to a converged identity security model. This mapping connects compliance intent to system-enforced controls that protect data integrity, support inspections, and reduce operational risk.

Regulatory / Security Expectation	Security & Data Integrity Risk	Fragmented Tool Limitation	Converged Identity Control	Business, Quality & Compliance Outcome
Individual accountability for regulated actions	Shared accounts or unclear attribution of changes	Access and logs inconsistent across systems	Unique identities, strong authentication, centralized	Improved data integrity and defensible inspections
Controlled access to GxP systems and data	Unauthorized creation or modification of regulated records	Role definitions not consistently enforced	Role-based access with policy enforcement across systems	Reduced compliance risk and fewer audit observations
Segregation of duties for regulated workflows	Same user initiates and approves regulated actions	Manual checks or workflow-only controls	System-enforced role separation and approval workflows	Stronger control integrity and reduced quality risk
Restricted privileged access to validated environments	Admins can alter systems or data without oversight	Privileged tools isolated from identity lifecycle	Time-bound privileged access governed within identity framework	Protection of validated state and reduced insider risk
Oversight of CRO/CMO and external collaborator access	Third parties access beyond study/site scope	External access poorly lifecycle-managed	Scoped third-party identities with lifecycle and monitoring	Secure collaboration with accountability
Governance of non-human identities (APIs, automation)	Service accounts operate with excessive or unmanaged access	Non-human identities unmanaged and under-logged	Unified governance for human and non-human identities	Reduced systemic risk from automation
Timely access review and revocation	Orphan access persists after role changes or exits	De-provisioning inconsistent; reviews manual	Lifecycle-driven access updates and access certification	Lower residual risk and improved compliance posture
Inspection-ready audit trails and historical evidence	Inability to reconstruct who had access and when	Evidence scattered and difficult to compile	Centralized audit trails, reporting, and historical access view	Faster inspections and reduced remediation burden

8. Cross Identity's Converged Identity Security Platform for Pharma

8.1 Designed for Regulated, GxP-Critical Environments

Cross Identity is built to support the stringent regulatory, quality, and security requirements of global pharmaceutical organizations. The platform is designed around **Cybersecurity-as-an-Infrastructure**, embedding identity controls directly into regulated operations rather than layering them as disconnected tools.
This approach aligns identity security with the rigor expected in GxP environments.

8.2 A Unified Identity Fabric Across the Pharma Ecosystem

Cross Identity brings all identity types—employees, scientists, quality teams, IT administrators, CROs, CMOs, partners, APIs, and automated workflows—under a single identity fabric. Access decisions are driven by consistent policies based on role, lifecycle status, and regulatory context.
By operating on a shared identity layer, the platform eliminates gaps between provisioning, access enforcement, and auditability.

8.3 Lifecycle-Centric Access Governance

Identity lifecycle events such as onboarding, role changes, project assignments, and exits automatically trigger access updates across regulated systems. This ensures that permissions remain aligned with current responsibilities and regulatory requirements throughout long system and data lifecycles.
Lifecycle-centric governance reduces insider risk and simplifies inspection readiness.

8.4 Embedded Controls for High-Risk and Privileged Access

High-risk access—including administrative actions, configuration changes, and sensitive data access—is governed through embedded, policy-driven controls.
Elevated access is restricted, approved, time-bound, and fully traceable, without being isolated from broader identity governance.
Privileged access is treated as a regulated activity within the identity framework, not a standalone function.

8.5 Governance for External and Non-Human Identities

Cross Identity extends governance beyond internal users to include CROs, CMOs, vendors, APIs, and automation. External and non-human identities are uniquely identifiable, scoped to defined activities, and governed throughout their lifecycle.
This ensures secure collaboration while maintaining accountability and data integrity.

8.6 Continuous Visibility, Monitoring, and Evidence

The platform provides continuous visibility into identity access and activity across regulated systems. Centralized audit trails capture authentication events, access changes, approvals, and high-risk actions in a single, inspection-ready view.
This supports both real-time oversight and historical reconstruction during audits, investigations, and quality reviews.

8.7 Supporting Secure Innovation and Regulatory Confidence

By converging identity controls into a single platform, Cross Identity enables pharma organizations to adopt new technologies, expand collaborations, and scale digital initiatives without compromising compliance or data integrity.
Cross Identity positions identity security as a foundational capability that supports innovation while meeting regulatory and quality expectations.

9. Continuous Compliance, Access Reviews & Inspection Readiness

9.1 From Periodic Inspections to Continuous Compliance

Pharmaceutical organizations are expected to demonstrate ongoing control over regulated systems, not just during scheduled inspections. Regulators increasingly assess whether controls operate consistently over time, making continuous compliance a critical requirement.

Identity governance must therefore function as an always-on capability that supports daily operations and long-term accountability.

9.2 Access Reviews as a Quality and Compliance Control

Access reviews play a central role in maintaining compliance and data integrity. Rather than relying on ad-hoc or manual reviews, pharma organizations are expected to periodically verify that access remains appropriate for all users, including employees, external collaborators, and automated systems.

System-driven access certification helps prevent privilege creep and supports defensible inspection outcomes.

9.3 Lifecycle-Driven Review and Revocation

Effective access reviews are closely tied to identity lifecycle events. Role changes, project completions, site transfers, and contract terminations should automatically trigger access reassessment or revocation.

This lifecycle-driven approach reduces reliance on manual intervention and ensures that access remains aligned with current regulatory responsibilities.

9.4 Inspection-Ready Audit Trails and Evidence

Regulatory inspections require clear, reliable evidence demonstrating who had access to regulated systems and when. Identity systems must maintain tamper-resistant records of authentication events, access changes, approvals, and high-risk actions.

Centralized audit trails enable rapid retrieval of evidence during inspections, reducing preparation effort and stress on quality and IT teams.

9.5 Supporting Investigations and Data Integrity Reviews

In the event of data integrity concerns or suspected deviations, identity-based audit trails support timely investigations. These records help reconstruct user actions, validate accountability, and demonstrate control effectiveness to regulators.

Strong identity evidence reduces the scope and duration of investigations and supports transparent regulatory communication.

9.6 Continuous Compliance as Cybersecurity-as-an-Infrastructure

By integrating access reviews, lifecycle governance, and audit evidence into a unified identity framework, pharma organizations can shift from reactive inspection preparation to continuous compliance. This approach aligns directly with Cybersecurity-as-an-Infrastructure, embedding security and quality controls into the core operating model.

Continuous compliance strengthens regulatory confidence while supporting efficient, scalable operations.

10. Implementation Approach: Embedding Identity into GxP and Quality Infrastructure

10.1 Position Identity as a Quality and Compliance Control

In pharmaceutical organizations, identity security must be implemented as part of the quality system. Identity controls directly support data integrity, accountability, and traceability and should align with GxP principles, validation requirements, and quality management processes rather than operate as standalone IT controls.

10.2 Prioritize Regulated and High-Impact Systems

Implementation should begin with systems supporting regulated activities such as laboratory systems, clinical trial platforms, manufacturing execution systems, quality management applications, and validated infrastructure. Securing these environments first reduces inspection risk and protects critical data.

10.3 Move from Procedural to System-Enforced Controls

Manual and procedural controls should be replaced with system-enforced identity governance. Role-based access, segregation of duties, and approval workflows must be embedded directly into systems to reduce human error and strengthen inspection defensibility.

10.4 Implement Lifecycle-Driven Access Governance

Identity lifecycle events—onboarding, role changes, project transitions, and exits—should automatically trigger access updates across regulated systems. This ensures long-term accountability in environments where systems and records persist for many years.

10.5 Govern Privileged, External, and Non-Human Identities Together

Administrative access, external collaborators such as CROs and CMOs, and non-human identities like APIs and automation must be governed within the same identity framework. Access should be scoped, time-bound, approved, and auditable to preserve system integrity and data trust.

10.6 Build Continuous Inspection Readiness

Identity systems should continuously capture access history, approvals, and activity in centralized, tamper-resistant audit trails. This enables rapid response to inspections, investigations, and data integrity reviews without extensive manual preparation.

10.7 Align Implementation with Validation and Change Management

Implementation should follow a phased approach aligned with validation and change-management cycles. This minimizes disruption to regulated operations while establishing identity as long-term GxP infrastructure.

11. Conclusion: Cybersecurity-as-an-Infrastructure for Pharma

11.1 Identity as the Foundation of Data Integrity and Compliance

In pharmaceutical organizations, identity is inseparable from data integrity, quality, and regulatory compliance. Every regulated action—whether in research, clinical development, manufacturing, or quality—depends on controlled, attributable access to systems and data.

Treating identity as Cybersecurity-as-an-Infrastructure reflects the reality that access governance must be embedded, consistent, and continuously enforced across the pharma ecosystem.

11.2 Fragmentation Is a Structural Risk

Fragmented identity tools create gaps in visibility, inconsistent enforcement, and reliance on manual controls. In regulated pharma environments, these gaps translate directly into data integrity risks, inspection findings, and operational disruption.

As identity surfaces expand to include external collaborators, automation, and long system lifecycles, fragmentation becomes a structural weakness rather than a manageable limitation.

11.3 Convergence Enables Sustainable Compliance

A converged identity security model unifies lifecycle governance, access controls, privileged access, third-party oversight, and audit readiness into a single framework. This convergence enables pharma organizations to enforce consistent policies, maintain accountability, and demonstrate compliance across all regulated systems.

Convergence shifts identity security from a reactive response to findings into a proactive, infrastructure-level capability.

11.4 Supporting Innovation Without Compromising Quality

Pharma organizations must balance innovation with strict regulatory and quality expectations. A converged identity approach supports secure collaboration, digital transformation, and automation while preserving data integrity and inspection readiness.

By embedding identity into the core operating model, organizations can scale confidently without introducing new compliance risks.

11.5 A Path Forward for Regulated Pharma Organizations

The transition to Cybersecurity-as-an-Infrastructure is not a technology upgrade alone—it is a strategic shift in how pharma organizations manage trust, accountability, and risk.

Organizations that adopt converged identity security are better positioned to meet regulatory expectations, protect patient safety, and sustain long-term operational excellence.

Identity, when treated as Cybersecurity-as-an-Infrastructure, becomes a foundational enabler of compliance, quality, and secure innovation in the pharmaceutical industry.

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