ANOMALIX

The Future of Vendor Management Systems

Published by

Anomalix

Learn more

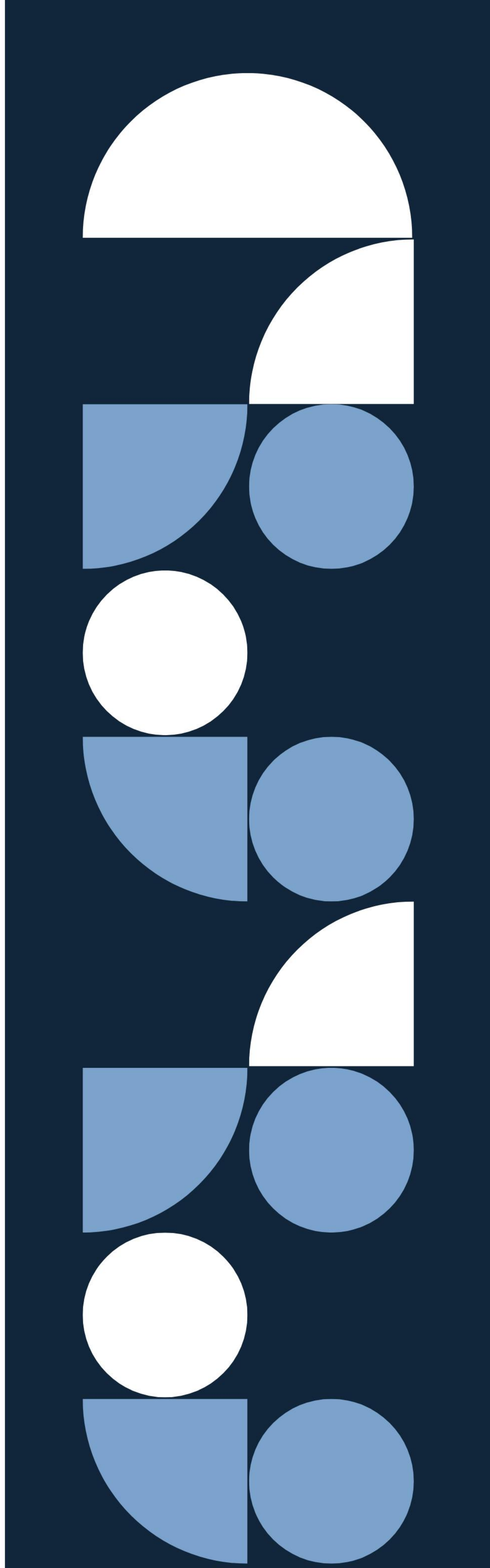
https://www.anomalix.com/

Contact us

info@anomalix.com

Table of Contents

Executive Summary	03
Why is vendor management changing in the era of hybrid work?	05
What are the biggest security risks in non-employee lifecycle management?	07
How does identity governance improve vendor security?	10
What is the best approach to secure vendor identity lifecycle management?	12
How do legacy and modern vendor management systems compare?	15
What does the future hold for vendor management and identity governance?	17
References	19



Executive Summary

Companies depend on vendors, contractors, and temporary workers more than ever, but managing their access to internal systems remains a challenge. Traditional vendor management systems (VMS) were designed to handle contracts and payments, not security. As a result, many organizations don’t have the adequate tools to track and control non-employee identities, creating security risks, compliance gaps, and operational inefficiencies.

Non-employee access is a growing risk

Every additional vendor, contractor, or partner with system access increases an organization’s exposure to security threats. Nearly a third of data breaches involve non-employee access [1]. Despite this risk, companies often fail to remove system access when contracts end. The longer an account remains active, the greater the chance it will be exploited.

Security teams also struggle to enforce compliance. Regulations like GDPR, SOC 2, and HIPAA require strict access controls, but when vendor identities are scattered across multiple systems, it becomes difficult to monitor and enforce policies. Without centralized identity governance, organizations risk audit failures, security breaches, and regulatory penalties.

Traditional vendor management systems don’t address identity security

Most VMS platforms were built for procurement and finance teams, not IT or security.

They help companies track vendor contracts and payments but provide little visibility into who has access to what systems. This creates several problems and gaps that leave organizations vulnerable. Without automated access controls, IT teams must manually onboard, monitor, and offboard non-employees—an inefficient and error-prone process.

Why vendor management needs an identity-first approach

A vendor management system that integrates identity governance solves these problems. Organizations need tools that can provision, monitor, and revoke access automatically, ensuring that non-employees only have access when needed and lose it as soon as their engagement ends.

Looking ahead

Managing non-employee identities is becoming just as important as managing employee identities. More companies are recognizing the risks of outdated vendor management practices and shifting toward solutions that treat vendors like internal users when it comes to security and access controls.

Moving forward, organizations that adopt identity governance for non-employees will be better positioned to minimize risk, streamline operations, and meet compliance requirements.

Why is vendor management changing in the era of hybrid work?

The evolving role of vendor management systems

Vendor management systems were originally built to help businesses track contracts, payments, and procurement workflows. They were not designed to manage non-employee identities or control access to sensitive systems. As a result, most traditional VMS platforms lack the security and automation needed to support today's workforce.

Companies now rely on a growing number of non-employees, including contractors, freelancers, and third-party service providers. Many of these workers need access to internal systems, applications, and data to perform their jobs. However, without proper identity governance, organizations struggle to monitor and control vendor access, leading to security risks and compliance issues.

The impact of hybrid work on vendor management

Hybrid work has accelerated the shift toward remote vendor management. Organizations are engaging more offsite contractors and global vendors, which means more external identities need system access. However, traditional VMS platforms are not equipped to handle remote, dynamic, and short-term identities securely.

Some of the biggest challenges include:

- Lack of visibility – Companies don't always know who has access to their systems, how long they need it, or when it should be revoked.

- Manual access management – Onboarding and offboarding vendors often require manual approvals, increasing the risk of delays and human error.
- Compliance risks – Organizations need to meet strict regulatory requirements, but many do not have the tools to track vendor access in real time.

Why traditional VMS are no longer enough

While legacy VMS platforms can help businesses track vendor relationships, they don't provide real-time access monitoring or automated identity lifecycle management. This creates security blind spots, leaving organizations vulnerable to unauthorized access and compliance failures. There is a range of problems that organizations may run into:

- Vendors often retain access long after their contracts end, increasing the risk of unauthorized activity.
- Many organizations manage vendor identities across multiple disconnected systems, making it difficult to enforce consistent security policies.
- Security teams have limited visibility into vendor access, complicating audits and compliance reporting.

Without proper controls, vendors can become an easy target for attackers looking to exploit weak access policies. According to Secureframe, 98% of companies work with at least one vendor that has experienced a security breach [2].

The shift to identity-first vendor management

A modern vendor management system must prioritize identity governance.

Companies are moving toward automated, AI-driven, and security-first approaches to vendor management, ensuring that non-employees only have access to the systems they need—and nothing more. An identity-first approach to vendor management helps organizations:

- Reduce security risks by continuously monitoring vendor access and enforcing least-privilege policies.
- Improve compliance by ensuring access aligns with regulatory requirements and is easily auditable.
- Increase efficiency by automating onboarding, offboarding, and access approvals.

What are the biggest security risks in non-employee lifecycle management?

Managing non-employee identities is more complex than managing full-time employees. Vendors, contractors, and service providers often work for multiple companies, have temporary access needs, and may not go through the same onboarding and security processes as employees. Without a structured identity management approach, organizations face serious security risks, operational inefficiencies, and compliance challenges.

Inconsistent onboarding and offboarding

Many organizations don’t have a standardized process for provisioning and deprovisioning vendor access. Unlike employees, who typically follow a defined onboarding process, non-employees often have access provisioned manually. This results in delays, misconfigurations, and access being granted beyond what is necessary.

Offboarding is even more problematic. Vendors frequently retain system access long after their contract ends, increasing the risk of insider threats and security breaches. Without automated offboarding, organizations lose control over who has access to critical systems and for how long.

Regulatory compliance risks

Strict regulations like GDPR, SOC 2, HIPAA, and industry-specific security frameworks require businesses to control and monitor vendor access. However, many organizations lack a centralized system to track vendor identities, making compliance difficult.

Common compliance challenges include:

- No audit trail – Organizations struggle to provide regulators with a clear record of who accessed what systems, when, and why.
- Excessive privileges – Vendors often receive broad access instead of role-based access, violating least-privilege policies.
- Data exposure risks – Non-employees may handle sensitive customer, financial, or intellectual property data without proper security oversight.

Failing to manage vendor access properly can result in regulatory fines, reputational damage, and legal consequences.

Fragmented identity sources

Most companies manage vendor identities across multiple disconnected systems. Procurement teams use a VMS for contracts and payments, IT teams use an identity and access management (IAM) system for provisioning, and compliance teams maintain separate audit records. Without integration between these systems, security teams have no single source of truth for vendor access.

This fragmentation leads to:

- Security blind spots – Companies can't quickly determine which vendors have access to critical systems.
- Access creep – Vendors accumulate permissions over time, creating long-term security risks.
- Slow incident response – If a vendor's credentials are compromised, IT teams may not have immediate visibility into which accounts need to be revoked.

Security gaps in legacy vendor management systems

Traditional VMS platforms were not designed to manage non-employee identities securely. Their primary function is tracking vendor contracts and payments, not enforcing security policies, monitoring access, or automating offboarding.

The result? Security gaps that put organizations at risk:

- Many vendors retain access for months or years after contracts end.
- 50% of organizations do not monitor the security and privacy practices of vendors with whom they share sensitive or confidential information [2].

How does identity governance improve vendor security?

Managing non-employee identities is more than just a security concern—it is a business necessity. An identity governance framework helps organizations track, control, and automate the entire vendor identity lifecycle. Instead of treating vendor management and security as separate processes, identity governance integrates them into a single, automated system that ensures only the right people have access, at the right time, for the right reasons.

What is identity governance?

Identity governance and administration (IGA) is a structured approach to managing who has access to what systems and under what conditions. It applies the same principles of employee identity management to vendors, contractors, and other non-employees.

A strong identity governance strategy includes:

- Automated provisioning and deprovisioning – Ensuring vendors get access only when needed and lose it immediately when no longer required.
- Role-based access control (RBAC) – Assigning access based on specific job functions rather than giving broad, unnecessary permissions.
- Just-in-time (JIT) access – Granting temporary access only when required, then revoking it automatically to minimize exposure.
- Continuous monitoring and risk assessment – Tracking vendor access in real time and flagging unusual or high-risk behavior.

Applying Zero Trust principles to non-employee access

Traditional vendor management systems operate on implicit trust, assuming that once a vendor is onboarded, their access remains valid until manually revoked. This is an outdated approach. A Zero Trust vendor model ensures that no vendor is automatically trusted. Instead, access is continuously verified using:

- Risk-based authentication – Adjusting security measures based on the vendor's access level, location, and behavior.
- Least privilege access – Granting the minimum level of access necessary for the vendor to complete their work.
- Session-based access controls – Requiring re-authentication for sensitive transactions or prolonged system activity.

Why identity governance matters for vendor management

Organizations that implement identity governance for non-employees benefit from stronger security, improved compliance, and increased operational efficiency.

- Stronger security – Automated access control prevents vendors from retaining system privileges longer than necessary.
- Regulatory compliance – Identity governance ensures vendors meet data security standards like GDPR, SOC 2, and HIPAA.
- Faster, more efficient vendor management – Automating vendor access reduces the workload on IT and security teams while ensuring proper oversight.

What is the best approach to secure vendor identity lifecycle management?

The Anomalix-recommended approach

Traditional vendor management systems were designed for contract tracking, not for securing non-employee identities. As vendor relationships become more complex, organizations need a centralized, automated, and security-driven approach to managing vendor access. A modern vendor identity lifecycle strategy ensures that vendors receive the right access at the right time—and lose it the moment it’s no longer needed.

Key elements of a future-proof vendor identity strategy

A vendor identity governance model should integrate security, automation, and compliance to provide full visibility and control over non-employee access. The most effective approach includes:

1. Centralized identity governance

Vendor identities are often scattered across multiple systems, making it difficult to track access or enforce security policies. A single source of truth for vendor identities gets rid of gaps, redundancies, and security blind spots.

A centralized identity governance system:

- Connects VMS platforms with identity and access management tools.
- Provides real-time visibility into vendor access across all systems.
- Enforces consistent security policies for all non-employees.

2. Automated workflows for onboarding and offboarding

Manual vendor onboarding and offboarding increase security risks and operational inefficiencies. Automating these processes ensures vendors receive access only when they need it—and that access is removed as soon as their engagement ends.

- Automated onboarding – Ensures vendors receive access based on predefined roles and approvals.
- Just-in-time access – Grants temporary access only when needed, then automatically revokes it.
- Automated offboarding – Immediately removes system access when contracts end, preventing unauthorized access.

3. Zero Trust and AI-driven security

A Zero Trust approach assumes that no vendor should be trusted by default. Every access request is verified, and access is continuously monitored. AI-powered tools analyze vendor behavior, detect anomalies, and enforce risk-based authentication to minimize insider threats.

- Risk-based authentication – Applies different levels of security based on vendor risk profiles.
- Least privilege access – Vendors receive only the minimum access required for their role.
- Continuous monitoring – AI-driven tools track vendor behavior and flag suspicious activity.

4. Compliance-focused vendor management

Industries regulated by GDPR, SOC 2, HIPAA, and other frameworks must ensure vendor access aligns with security and privacy standards. An effective vendor identity lifecycle management strategy should include:

- Automated compliance reporting – Generates audit logs for regulators and security teams.
- Role-based access control – Ensures vendors access only the data they are authorized to see.
- Real-time policy enforcement – Blocks access that violates security rules.

How do legacy and modern vendor management systems compare?

Feature	Legacy VMS	Modern VMS
Primary function	Contract and payment tracking	Identity governance and security-first vendor management
Access control	Manual, inconsistent, and error-prone	Automated, policy-driven, and risk-based
Onboarding and offboarding	Requires manual provisioning and deprovisioning	Automated workflows ensure timely access revocation
Security monitoring	Limited or non-existent	Real-time access tracking and anomaly detection
Compliance readiness	Difficult to track access for audits	Integrated audit trails and regulatory compliance reporting
Integration with identity management	Separate from IAM and security tools	Seamlessly connects with IAM, Zero Trust, and security platforms

Traditional vendor management systems were designed to handle contracts, invoices, and payment processing. They were not built to manage non-employee identities or secure vendor access to company systems. As organizations rely on more contractors, service providers, and external partners, the limitations of legacy VMS platforms have become clear.

A modern VMS goes beyond administrative tracking. It integrates identity governance, automated access control, and security monitoring to ensure that vendors only have the access they need—and lose it the moment they no longer require it.

Why legacy VMS is no longer enough

Legacy vendor management systems focus on contracts and payments, not security. As a result, many organizations:

- Struggle to track vendor access across multiple systems
- Lack real-time monitoring of vendor behavior
- Manually grant and revoke access, leading to security gaps
- Have difficulty proving compliance with regulations like GDPR, SOC 2, and HIPAA

The benefits of a modern, security-first VMS

A modern VMS with integrated identity governance ensures that vendor access is controlled, monitored, and revoked automatically when no longer needed. Key benefits include:

- Stronger security – automated vendor access controls prevent unauthorized system entry
- Improved compliance – real-time tracking simplifies audits and regulatory reporting
- Reduced IT burden – automated workflows replace manual processes, reducing human error
- Faster response to security incidents – real-time monitoring detects and mitigates risks immediately

What does the future hold for vendor management and identity governance?

Managing non-employee identities is no longer just an administrative task—it is a core security function. As organizations rely more on vendors, contractors, and service providers, traditional vendor management systems are proving inadequate. A modern, identity-first approach is necessary to reduce security risks, improve compliance, and streamline vendor access management.

Key takeaways

- Identity governance must be integrated with vendor management. Organizations need automated access control, real-time monitoring, and policy enforcement to manage vendor identities securely.
- Manual processes increase security risks. Legacy VMS platforms require manual onboarding and offboarding, leading to access creep and unauthorized system entry. Automation eliminates these risks.
- Regulatory compliance depends on effective vendor access controls. Regulations like GDPR, SOC 2, and HIPAA require audit trails, access reviews, and strict privilege management for vendors.
- Zero Trust is the future of vendor security. Organizations must assume no vendor is automatically trusted and enforce continuous verification, least-privilege access, and risk-based authentication.
- AI and automation will drive the next generation of vendor identity management. Machine learning-based anomaly detection, AI-driven risk scoring, and intelligent access policies will become standard.

Looking ahead

Companies that fail to modernize vendor identity management will continue to face data breaches, compliance violations, and inefficiencies. The shift toward automated, identity-driven vendor management is already underway, and organizations that adopt these practices early will have a competitive advantage in security, compliance, and operational efficiency.

References

1. SecurityScorecard, "2024 Global Third-Party Cybersecurity Breach Report," https://securityscorecard.com/blog/2024-global-third-party-cybersecurity-breach-report/?.
2. Secureframe, "99+ Essential Third-Party Risk Statistics and Trends for 2024," https://secureframe.com/blog/third-party-risk-statistics?.

Next-generation security & identity management

https://www.anomalix.com/

info@anomalix.com

159 N Sangamon St, Suite 200, Chicago, Illinois
60607, US