The Responsibility of Risk

Maintaining Cyber Risk Compliance Amid Expanding Global Regulations

New regulations around the world now demand faster incident discovery, more complete investigations, and clear evidence that organizations can protect personal data. These mandates assign risk ownership to specific leaders and hold them accountable for proving controls worked when an incident occurred.

This shift makes continuous monitoring, behavioral awareness, and reliable investigation documentation essential. Compliance programs must now account for activity from both people and the autonomous agents that act within enterprise systems. These agents move at machine speed and introduce new forms of insider risk that regulators expect organizations to control.

This paper explains the structural changes driving these expectations, outlines the responsibilities assigned to risk owners, and shows how organizations can maintain provable, audit-ready compliance.

Cyber Risk Has Become Regulated Risk

Governments continue to expand data protection laws, shorten reporting windows, and raise penalties for noncompliance. These rules vary by region, but consistently require organizations to demonstrate visibility, accountability, and rapid response.

Examples include:

- **GDPR**, with its strict 72-hour reporting window and high penalties for mishandling personal data
- **Indonesia's Personal Data Protection (PDP) Law**, which requires prompt investigation, formal notification, and a designated Data Privacy Officer (DPO) capable of coordinating incident response
- **Japan's APPI,** with expanded reporting mandates and operational expectations for breach management
- **Singapore's PDPA Amendments**, increasing penalties and emphasizing faster, documented response steps
- **United States Executive Order 14028,** which requires federal agencies and contractors to adopt practices such as zero-trust principles, rapid incident reporting, improved supply chain transparency, and expanded event logging requirements

For all of these frameworks, regulators expect organizations to maintain situational awareness, document their actions, and demonstrate control effectiveness during audits and investigations.

Accountability Is Explicit and Personal

Regulators now assign responsibility to named individuals. These leaders must understand the organization's obligations, oversee data protections, and ensure that incident response programs are not only defined but actively followed.

Common roles include:

- Chief Information Security Officer
- Data Protection Officer
- Cyber Risk or Compliance Officer
- Executive with regulatory reporting authority

These individuals must show that controls were consistently applied, that monitoring covered relevant systems, and that incident timelines accurately reflect what occurred. Their responsibility extends from strategy to execution and includes coordination with legal, operations, and executive leadership.

The Expanding Scope of Compliance Responsibility

Modern compliance requires teams to observe and understand behavior throughout a distributed environment where activity spans cloud platforms, SaaS applications, identity systems, APIs, and integrated services.

Regulators expect organizations to identify unusual or high-risk behavior across:

- Human users
- Devices and applications
- Privileged identities
- Third-party integrations
- AI agents performing operational tasks

The last group represents a growing expectation. AI agents act inside enterprise systems, execute tasks at high speed, and interact with sensitive data. They introduce new forms of operational and insider risk that compliance programs must monitor. These agents can behave outside intended boundaries, be manipulated, or amplify mistakes at scale. Regulators expect organizations to govern these activities the same way they govern human behavior.

Understanding Emerging Insider Risk From Agents

Digital workers and agents are becoming common, from IT automation to customer support tools to internal copilots. These agents perform real actions in enterprise environments and must be treated as security subjects.

Organizations must apply the same diligence to agent activity as they do to human users. This includes:

- Monitoring agent behavior
- Detecting behavior that indicates misuse, compromise, or configuration drift
- Documenting agent actions so they can be audited
- Ensuring human policy defines what agents can do
- Preserving human judgment and oversight

Humans and AI agents now work together inside enterprise environments. Agents move at machine speed, but their actions must still follow human-defined policies and limits. This approach aligns with modern compliance expectations, which emphasize documented oversight, verifiable evidence, and clear accountability for every actor, human or non-human.

What Compliance Execution Requires Today

Understanding Regulatory Obligations

Teams need a clear map of applicable laws, including reporting windows, required documentation, and privacy protections. Requirements vary by geography but share an expectation for rapid, accurate reporting.

Continuous Behavioral Modeling

Compliance requires ongoing visibility into activity across users, systems, and agents. Understanding normal behavior allows teams to identify anomalies early, reducing the risk of undetected breaches that violate reporting timelines.

Documented Investigation Workflows

Every investigation must produce a clear, complete record. Regulators expect detailed timelines showing what happened, when it happened, and how the organization responded.

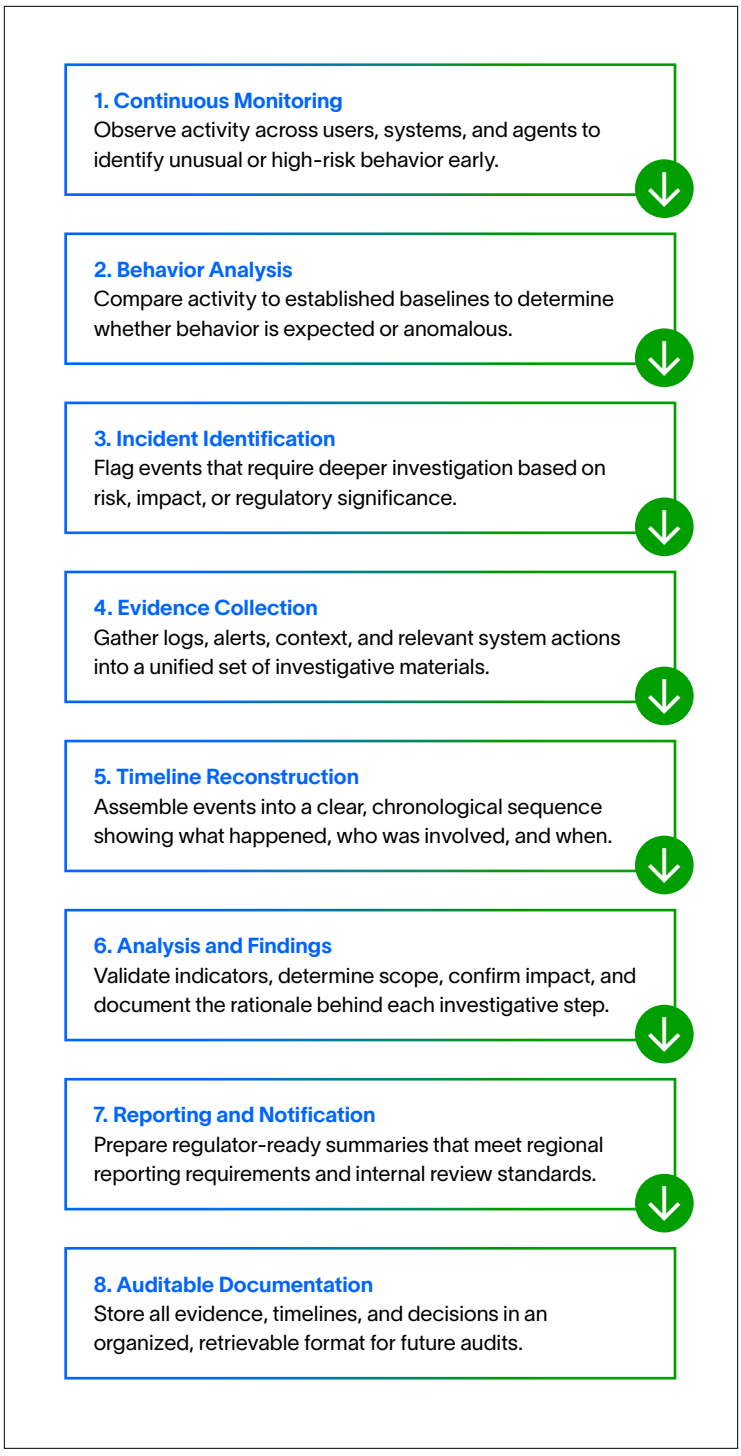

Figure 1.

How organizations collect, correlate, and document evidence from detection through reporting

Fast, Accurate Reporting

Most regulations now specify response or notification windows. Teams must be able to gather facts, confirm scope, and prepare required statements in a short timeframe.

Provable Control Effectiveness

Regulators look for evidence showing that controls were active and functioning both before and during an incident. This includes identity controls, data protections, monitoring rules, and escalation workflows.

How Exabeam Helps Organizations Meet Compliance Requirements

Exabeam supports organizations in meeting regulatory requirements by providing the behavioral visibility, investigation automation, and evidence collection capabilities needed for continuous compliance. These capabilities align with modern expectations for risk ownership and audit-ready response.

Behavioral Analytics for Users and Agents

Exabeam monitors activity from both human users and autonomous agents. It identifies when behavior falls outside expected patterns, supporting early detection of insider activity, policy drift, or agent misuse.

Automated Timelines for Auditable Investigations

Timelines automatically assemble all relevant events into a single, chronological view, enabling teams to understand incidents quickly and produce accurate reports for auditors and regulators.

Automated Investigation Workflows

Investigation tasks follow consistent, documented patterns. This produces reliable evidence trails that demonstrate compliance with required processes.

Data Protection Controls

Role-based access, data masking, and context-based visibility help ensure only authorized personnel view personal or sensitive data during an investigation.

Compliance-Ready Reporting

The platform generates reports aligned with common frameworks such as GDPR, ISO 27001, HIPAA, PCI DSS, and regional mandates. These reports help leaders demonstrate ongoing control effectiveness and prepare for audits.

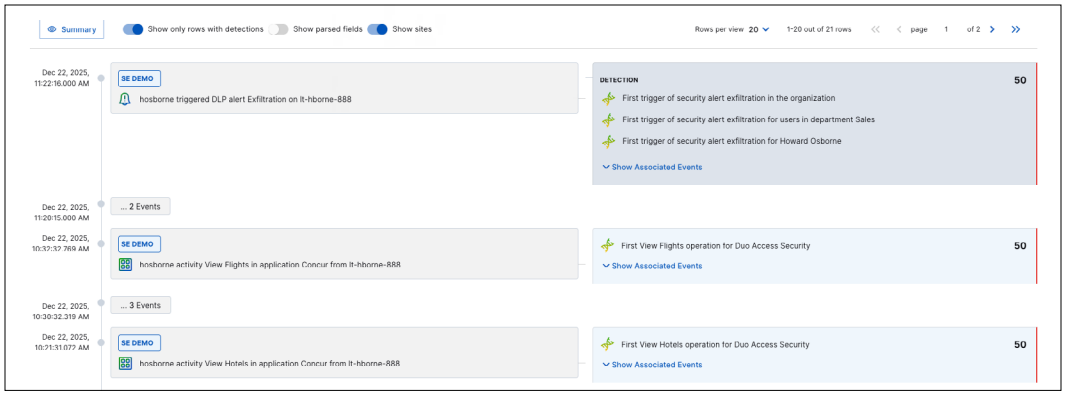

Figure 2.

Threat Timelines automatically reconstruct the sequence of events, giving you a clear, audit-ready view of activity, related detections, and investigation details.

Conclusion

Regulations continue to raise expectations for oversight, reporting, and documented investigations. Meeting these requirements calls for steady monitoring, clear ownership, and reliable evidence that shows how your team identified and handled each incident. By focusing on consistent processes and behavior awareness across both people and autonomous agents, your organization strengthens its ability to respond quickly and demonstrate that appropriate safeguards guided each step of the investigation.

If you're evaluating how well your organization meets growing regulatory expectations, now is the time to review your monitoring coverage, investigative workflows, and documentation practices. Confirm that you can identify unusual behavior quickly, reconstruct events accurately, and produce evidence that supports reporting requirements. Strengthening these areas helps you stay aligned with current mandates and prepares your team for new rules as they emerge.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

© 2026 Exabeam, LLC. All rights reserved.