EINPRESSWIRE

4 Practical Ways AI Is Being Used in Cyber GRC Today

How CISOs are applying artificial intelligence to governance, risk, and compliance, and what it takes to make it work in practice

LONDON, UNITED KINGDOM, February 2, 2026 /EINPresswire.com/ -- As artificial intelligence becomes embedded across security operations, one question is coming up repeatedly among CISOs, risk leaders, and compliance teams:

How can AI actually be used in GRC — beyond experimentation and hype?

Governance, Risk, and Compliance (GRC) has no shortage of complexity. Security teams are expected to manage more frameworks, assess more vendors, mitigate more vulnerabilities, and communicate risk more clearly — all without additional headcount. While AI promises efficiency, most organizations struggle to translate that promise into day-to-day Cyber GRC execution.

In practice, AI delivers value in GRC only when it is embedded directly into existing workflows, aligned with regulatory requirements, and built for auditability and trust. Based on real-world enterprise use, four practical AI applications are emerging as the most impactful in Cyber GRC today — all now operationalized within platforms like Commugen’s AI-powered Cyber GRC platform.

1. Automating Vendor Evidence Reviews with AI

Third-party and supply chain risk has become one of the most resource-intensive areas of Cyber GRC. Vendor questionnaires often contain hundreds of questions, multiple document formats, and inconsistent answers. Reviewing them manually is slow, repetitive, and prone to human error.

AI is now being used to automatically analyze vendor responses and supporting evidence, identifying gaps, inconsistencies, and outdated information such as expired ISO or SOC 2 certificates. More importantly, AI can explain why a finding matters by mapping it back to internal controls and compliance requirements.

In mature implementations, this process is no longer a document check — it becomes AI-driven evidence analysis, producing consistent, auditable risk insights at scale. Platforms like

Commugen embed this capability directly into vendor risk workflows via an Automate Third-Party Security Reviews AI Agent, enabling teams to review hundreds of vendors weekly without sacrificing rigor or traceability.

2. Using AI to Generate Audit-Ready Security Policies

Every compliance framework — ISO 27001, SOC 2, NIST, GDPR, and others — requires policies. Writing and maintaining those policies is one of the biggest time sinks in GRC, often resulting in documents that are outdated, disconnected from controls, and difficult to audit.

AI is now being applied to turn approved controls, mitigations, and frameworks into clear, enforceable security policies automatically. Instead of writing policies from scratch, teams can generate consistent, audit-ready documents in minutes, complete with versioning and traceability back to the originating controls.

This approach fundamentally changes policy management: policies evolve alongside controls and regulations, rather than becoming static documents rewritten before every audit. Commugen's AI Policy Generator exemplifies this shift by embedding policy creation directly into the Cyber GRC lifecycle.

3. Transforming Vulnerabilities into Actionable Mitigation Plans

Vulnerability management often breaks down at the "last mile." Security tools identify CVEs and findings, but remediation stalls due to unclear ownership, lack of prioritization, or poor alignment with business risk.

AI is now being used to convert raw vulnerability data into structured, step-by-step mitigation plans. These plans include task breakdowns, ownership mapping, prioritization based on business impact, and links back to the risk register and compliance controls.

Instead of static vulnerability lists, organizations gain AI-generated mitigation playbooks that are actionable, trackable, and audit-ready. Within platforms like Commugen, this capability connects vulnerability data directly to Cyber GRC processes. Commugen's AI mitigation Advisor ensures that remediation progress is visible and defensible during audits, and that it takes only minutes to get a mitigation plan.

4. Rewriting Technical Risk Content for Any Audience

One of the least discussed — but most critical — challenges in GRC is communication. The same risk often needs to be explained differently to engineers, compliance teams, executives, and the board.

AI is increasingly being used to rewrite technical risk content for different audiences without changing the underlying facts. With a single action, technical findings can be translated into compliance-aligned narratives or business-focused summaries that highlight financial and operational impact.

This use of AI dramatically improves consistency, reduces reporting time, and ensures that stakeholders actually understand the risks being presented. Commugen's AI GRC Assistant embeds this capability directly into Cyber GRC workflows, enabling clearer communication across the organization.

What Makes AI in GRC Actually Work

While these four use cases show where AI adds real value, they also highlight an important reality: AI only works in GRC when it is enterprise-ready.

Effective AI-powered GRC platforms must ensure:

Full auditability and explainability of AI outputs

Alignment with SOC 2, ISO 27001, GDPR, and other regulatory requirements

No use of customer data for AI model training

Secure, private deployment options

Commugen's approach to AI in Cyber GRC is built around these principles, ensuring that automation strengthens — rather than undermines — governance and compliance.

AI Built on a No-Code Foundation

Underlying these AI capabilities is Commugen's no-code platform philosophy, which shapes how AI is actually used in Cyber GRC. Rather than requiring custom development or data science expertise, Commugen's AI is designed to be easy to configure, easy to use, and easy to adapt. Security and GRC teams can create and tailor AI agents directly within the platform to support virtually any GRC task — from vendor risk assessments and policy generation to mitigation planning and executive reporting. This no-code approach ensures that AI fits existing workflows instead of forcing teams to change how they work, enabling organizations to evolve their AI-driven GRC capabilities as requirements, regulations, and risks change.

The Bottom Line

AI is no longer a future concept in GRC. It is already reshaping how organizations review vendors, manage policies, remediate vulnerabilities, and communicate risk.

The difference between success and disappointment lies in how AI is applied. When embedded directly into Cyber GRC workflows — as it is within the Commugen platform — AI becomes a force multiplier for security, compliance, and risk teams.

For CISOs and GRC leaders asking how to actually use AI in governance, risk, and compliance, these four use cases represent where AI is delivering measurable impact today.

Adam Babayoff
Commugen
+44 20 4591 9206
adam.babayoff@commugen.com

This press release can be viewed online at: https://www.einpresswire.com/article/888677723

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.