Scrut Automation

eBook

Top 10 GRC and AI predictions for 2025

Scrut Automation

Top 10 GRC and AI predictions for 2025

Introduction

As we head into 2025, governance, risk, and compliance (GRC) are on the brink of some major changes, thanks to the rapid progress of artificial intelligence (AI). Over the past few years, AI has gone from being a buzzword to becoming a core driver of efficiency and smarter decision-making across industries. It's no longer a "nice to have" or a future possibility—integrating AI into compliance and risk management is now an absolute must.

The numbers speak for themselves. Gartner estimates that by 2028, a whopping 15% of daily work decisions will be made autonomously by AI—up from literally zero today. On top of that, the global GRC platform market is projected to skyrocket from $49.2 billion in 2024 to $127.7 billion by 2033, growing at a solid annual rate of 11.18%. And let's not forget the big picture: IDC forecasts that the worldwide spending on AI-supporting technologies will surpass $749 billion by 2028.

In this fast-moving world, keeping up with these trends isn't just a good idea—it's essential for survival. So, let's dive into our top 10 predictions for how GRC and AI will intersect in 2025 and explore how organizations can ride the wave of innovation to stay ahead of the curve.

Prediction 1: ISO 42001 is approved as "harmonised standard" under the EU AI Act

With the European Union (EU) AI Act published in the summer of 2024, full enforcement is just around the corner. With that said, the EU's Joint Technical Committee (JTC) responsible for certifying "harmonized standards" under the act has said they won't release these until the end of 2025. This leaves less than a year before full enforcement of the new regulation rolls out, leaving firms very little time to prepare and get into compliance.

As a result, we are pretty sure the existing ISO/IEC 42001:2023 standard will be adopted as a harmonized standard despite the European Commission casting doubt on whether it would cover all of the AI Act's requirements in mid-2023. We suspect there will be some sort of compromise whereby certain Annex A controls from the standard become required for AI Act compliance (rather than being optional, as they are for ISO 42001 by themselves).

To stay ahead, organizations should begin aligning their practices with ISO 42001 now rather than waiting for the harmonized standard to be finalized. Conducting internal audits, leveraging automated compliance solutions, and fostering cross-departmental collaboration can help bridge potential gaps before the regulations hit full force. On the contrary, non-compliance could result in heavy penalties, as outlined in the AI Act.

How to prepare for ISO 42001 compliance

a. **Conduct a gap analysis:** Identify how your current AI systems measure up to ISO 42001.
b. **Develop a compliance roadmap:** Prioritize addressing high-risk gaps, and establish clear timelines.
c. **Leverage automation:** Use AI-specific compliance tools to streamline monitoring and reporting.
d. **Train your team:** Ensure employees understand the requirements and their role in maintaining compliance.
e. **Engage experts:** Collaborate with consultants or certification bodies familiar with ISO 42001 to validate your approach.

Download an ISO/IEC 42001 Readiness Checklist for ISO 42001 for compliance managers and start-up founders on the Scrut website.

Prediction 2: SOC 2 gets a shake up

While the System and Organization Controls (SOC) 2 report has become a staple of cybersecurity due diligence, this won't necessarily last forever. Most audit firms apply the necessary scrutiny to their assessments but there is a growing consensus in the GRC field that a small subset are turning into "report mills." These firms do the bare minimum required to issue a report, without digging deeply. This commoditization of audit reports hurts everyone in the industry and cannot continue unabated.

In 2025, we'll likely see the American Institute of Certified Public Accountants (AICPA) tighten standards and enforce discipline among audit firms issuing SOC 2 reports.

New changes coming up in SOC 2

Based on industry trends & anticipated updates, here are some of the changes that businesses can expect in SOC2:

Area of change	Expected updates
Enhanced auditor oversight	Stricter enforcement of auditing standards to ensure high-quality, in-depth assessments by audit firms.
Integration of AI controls	Inclusion of criteria for evaluating controls over AI systems and algorithms used in critical processes.
Greater focus on data privacy	Alignment with global data privacy laws like GDPR and CCPA, incorporating more rigorous privacy controls.
Cloud security enhancements	Updated guidelines to address security risks associated with evolving cloud technologies and services.
Third-party risk management	Increased emphasis on assessing and reporting risks related to vendors and supply chains.
Continuous monitoring requirements	Encouragement for organizations to adopt continuous controls monitoring instead of periodic reviews.

Organizations will need to ensure they partner with reputable audit firms that uphold rigorous standards. Embracing advanced audit readiness platforms can help companies streamline their preparation process while maintaining the integrity of their security practices. This proactive approach will not only prepare businesses for tighter regulations but also foster trust with stakeholders seeking reliable compliance assurances.

Prediction 3: The Federal Trade Commission (FTC) takes fewer enforcement actions on data privacy issues

As we wrote previously, the FTC has been very aggressive in data privacy and AI governance-related enforcement actions under Chair Lina Khan. That is almost certainly going to change when President-elect Trump takes over in January 2025. His pick for the head of the FTC, Andrew Ferguson, is likely to be more business-friendly in his approach.

While this will likely result in fewer fines and suits against companies for mishandling data, that doesn't mean companies can ease up on their governance and compliance efforts. In fact, businesses may need to work harder to establish self-regulation practices that demonstrate their commitment to ethical AI and data privacy.

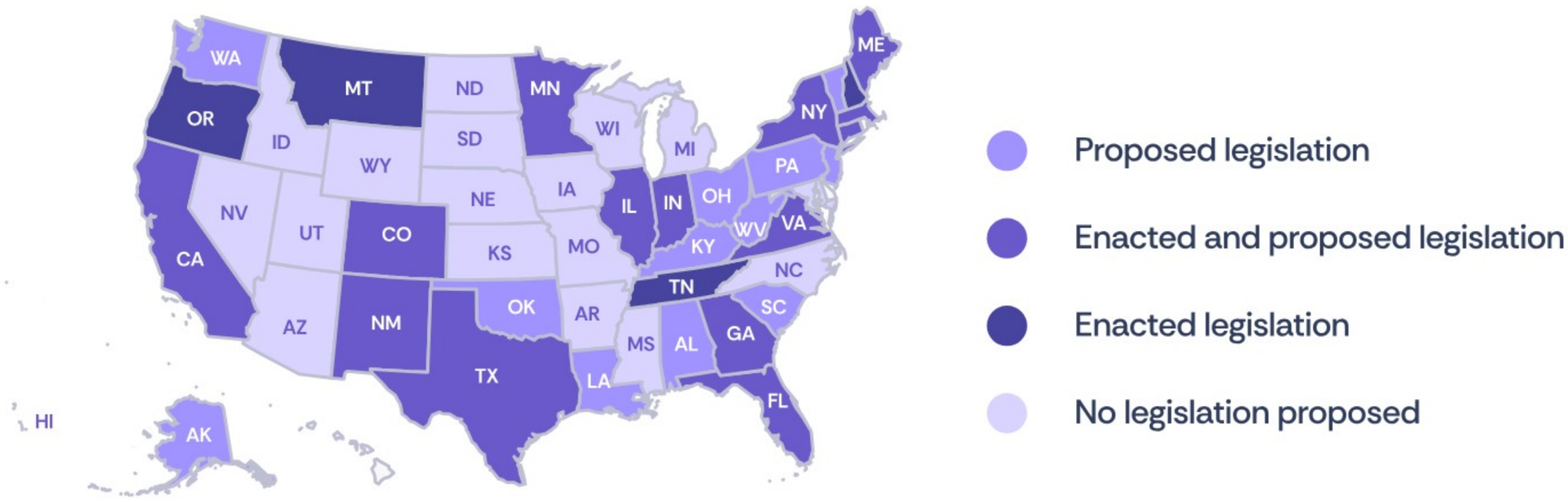
Building trust with customers and partners through transparent policies and proactive compliance measures will be more critical than ever. That's because of the state and local-level AI governance laws, as discussed in the next section.

Prediction 4: State- and local-level AI governance laws proliferate, just like data privacy ones did

States like Colorado and even individual cities like New York have already passed AI-specific regulations called the Colorado Privacy Act (CPA) and Local Law 144, respectively. Big states like Texas and California are likely to follow in 2025. California has been actively expanding its privacy regulation under the California Privacy Rights Act (CPRA) which could move in an AI-specific direction focusing on transparency and consumer rights. Just like the jumble of privacy and data breach notification laws that grew over the past two decades, AI governance is likely to be no different.

With a consolidated federal data privacy or AI governance law unlikely to be a top priority of the new administration, we can expect states and other jurisdictions to fill in the gaps.

The following map shows state-by-state AI legislation information as of June 7, 2024 (source: BCLP):



To navigate this patchwork effectively, organizations will need scalable compliance frameworks and tools capable of adapting to diverse regulations. Establishing a clear, centralized strategy for AI governance will help minimize the operational complexity of adhering to multiple laws.

Recommendations on navigating state and local compliance

To effectively navigate the evolving state and local compliance landscape, businesses should:

a. **Adopt a flexible compliance framework:** Use adaptive tools that can incorporate changing requirements across multiple jurisdictions.

b. **Monitor regulatory updates:** Stay informed about new and amended laws, particularly in key states like California and Texas, where innovation often shapes legislation.

c. **Standardize policies:** Develop a core set of compliance policies that can be customized for specific state-level nuances.

d. **Engage local expertise:** Collaborate with legal or compliance experts familiar with state-level regulations to minimize oversight risks.

e. **Automate reporting:** Implement compliance automation solutions, like Scrut, that simplify tracking and reporting for state-specific requirements.

Prediction 5: Dedicated AI governance professionals become the norm

As AI becomes central to how every business operates - just like cloud computing did beforehand - managing its risks will become a full-time job. While responsibilities are often split between security, privacy, legal, and data science teams, the AI governance professional will likely become a dedicated role.

We are already seeing certifications - like the AI Governance Professional (AIGP) from the International Association of Privacy Professionals (IAPP) - that are shaping the career progression for this new breed of compliance professional.

The demand for AI governance solutions is projected to grow significantly. According to Grand View Research, the global AI governance market size was estimated at USD 227.6 million in 2024 and is projected to grow at a compound annual growth rate (CAGR) of 35.7% from 2025 to 2030.

Organizations that prioritize hiring or upskilling AI governance professionals now will position themselves as leaders in responsible AI usage. These professionals will not only address compliance risks but also drive innovation by ensuring AI initiatives are ethical, transparent, and aligned with business goals.

AI governance market

Size, by component, 2020-2030 (USD million)

35.7%

Global market CAGR 2025 - 2030

Recommended AI certification courses to upgrade your team

a. **Artificial Intelligence Governance Professional (AIGP):** Offered by the International Association of Privacy Professionals (IAPP), this certification equips professionals with the knowledge to develop, integrate, and deploy trustworthy AI systems in line with emerging laws and policies.

b. **Certified AI Governance Professional (AIGP) Course:** Provided by QA, this training presents an awareness of unforeseen concerns with AI and knowledge of debated issues surrounding AI governance, preparing professionals for the AIGP certification exam.

c. **AI Security & Governance Certification:** This comprehensive training by AI Tech & Privacy Academy focuses on AI ethics, compliance, and regulation, covering the latest developments in the field.

d. **AI Governance Training:** This comprehensive training by AI Tech & Privacy Academy focuses on AI ethics, compliance, and regulation, covering the latest developments in the field.

e. **Certificate in AI Governance & Compliance:** Offered by Georgetown University, this program equips professionals with the knowledge & skills to navigate the complexities of AI and generative AI systems.

Prediction 6: The European Union AI Liability Directive is passed

On top of the AI Act, the EU has been considering a separate AI Liability Directive (AILD) that creates strict standards for companies using or deploying AI systems. This proposed rule lets consumers sue companies even if the individual in question didn't buy the company's product (Kennedy's Law). EU legislators introduced the rule because they thought national liability rules didn't sufficiently address damage caused by AI-based products and services because of their lack of transparency.

We expect the AILD to be passed in 2025.

With the combined risks of government fines under the AI Act as well as private action under the AILD, technology-enabled companies operating in Europe will need to be extremely careful as they release products.

To ensure readiness for the EU AI Act's compliance requirements, businesses should follow the above. Also, explore the key focus areas to confidently navigate the EU AI Act in our comprehensive guide—download it now.

Prediction 7: GRC professionals merge with security engineers

As almost every employee in a modern company becomes "technical" to some degree, GRC pros won't be any different. With the emergence of the GRC engineering discipline, simply mastering spreadsheets won't be enough for security and compliance pros to stay competitive in the job market.

To deliver value, these employees will need to understand compliance automation platforms and practices, working from the beginning to help product teams deliver value while protecting data confidentiality, integrity, and availability.

This trend will also push organizations to redefine traditional compliance roles, blending them with technical expertise to meet evolving demands. For GRC professionals, learning to collaborate seamlessly with security engineers will not just enhance their career prospects but also enable teams to build more resilient systems. Ultimately, this fusion of skills will ensure that compliance is baked into every layer of product development, from design to deployment.

Skills and tools needed to thrive in hybrid roles

To excel in these emerging hybrid roles, professionals will need a blend of technical and strategic skills.

Key skills include:

a. Proficiency in programming languages like Python or SQL for compliance data analysis.

b. Knowledge of DevSecOps practices to integrate security and compliance into the software development lifecycle.

c. Strong understanding of frameworks like SOC 2, ISO 27001, and ISO 42001 to guide regulatory adherence.

Essential tools include:

a. Compliance automation platforms, such as Scrut, for real-time risk tracking and reporting.

b. AI-based analytics tools to identify compliance gaps and optimize resource allocation.

c. Collaborative project management software to align cross-functional teams effectively.

By fostering these skills and leveraging the right tools, GRC professionals can seamlessly bridge the gap between governance and technical execution, making themselves indispensable in this evolving landscape.

Read also: Creating a DevSecOps Culture for Your Company

Prediction 8: Companies figure out how to integrate cryptocurrency into operations

While it experienced a "winter" following the collapse of the FTX exchange in 2022, cryptocurrency - especially Bitcoin - has come roaring back. Because of a friendly incoming Presidential administration, the risk of bank collapses like that of SVB in 2023, and the need to keep reserves on hand in case of a ransomware attack, companies of all sizes will increasingly integrate cryptocurrency into their operations.

Preventing theft by insider threats, securing it from outside attacks, and complying with emerging regulations will become priorities for GRC teams in 2025.

The global cryptocurrency market has seen significant growth, with its total value reaching approximately $3.4 trillion as of January 2025 (and counting). This expansion underscores the increasing integration of digital assets into mainstream financial systems.

As companies integrate crypto into their operations, they'll also need to establish robust governance practices around its use. This includes clear policies for crypto custody, regular audits of blockchain transactions, and collaboration with regulators to address evolving compliance requirements.

Integrating cryptocurrency can provide resilience and innovation, but careful planning and adherence to best practices are critical to mitigate risks and meet compliance requirements.

Risks to address:

a. **Volatility:** Crypto's value fluctuations can impact financial stability; companies should establish clear limits on holdings.

b. **Regulatory uncertainty:** Lack of uniform global laws can expose organizations to legal risks if they operate across jurisdictions.

c. **Cybersecurity threats:** Cryptocurrencies are a prime target for hackers, making robust security measures essential.

Best practices to follow:

a. **Build secure custody systems:** Use multi-signature wallets or custodial services with a proven track record of compliance.

b. **Adopt blockchain analytics tools:** These tools help monitor transactions, detect anomalies, and prevent money laundering risks.

c. **Ensure internal accountability:** Create clear policies for crypto transactions, including roles and responsibilities for employees handling digital assets.

d. **Stay informed on regulations:** Regularly review compliance frameworks such as the Financial Action Task Force (FATF) guidelines and local cryptocurrency laws.

Prediction 9: AI safety takes center stage

With the explosion in the power of AI systems, national governments have already taken - like the EU - or promised they will take - like the United Kingdom - action. On top of the cybersecurity and privacy implications, 2025 is likely to see a push by regulators to address the large-scale and even existential risks posed by AI. Self-regulation efforts, like through OpenAI's Preparedness Framework, will be important supplements, but not replacements for, these official moves.

The integration of AI into business operations is accelerating. A recent McKinsey survey indicates that 65% of organizations are now regularly using generative AI in at least one business function, nearly double the percentage from the previous year. This rapid adoption underscores AI's expanding role in decision-making processes across various industries.

Our expert underscores how organizations are optimizing returns on AI investments by embedding GRC into their AI workflows.

Businesses will also need to invest in third-party evaluations of their AI systems to ensure they are free from bias and vulnerabilities. Regular testing and validation processes will become essential to build trust and minimize risks as AI takes on increasingly critical roles in decision-making.

5 Pillars of AI safety

1 Transparency

- Ensure that AI systems are explainable and decisions are interpretable by humans.
- Provide clear documentation for datasets, algorithms, and decision-making processes.

2 Accountability

- Establish clear ownership of AI systems to monitor and address any issues.
- Assign roles and responsibilities for oversight and regulatory compliance.

3 Fairness

- Prevent biases in AI models by auditing training data and decision-making processes.
- Regularly test systems for equitable treatment of all user groups.

4 Robustness

- Build systems resistant to adversarial attacks and ensure resilience to unexpected inputs.
- Continuously monitor AI models to detect and address anomalies.

5 Ethical Alignment

- Align AI behavior with organizational values and societal norms.
- Regularly evaluate systems against ethical standards and emerging best practices.

Prediction 10: Quantitative risk management becomes the standard

While they have been a hallmark of cyber risk management practice for decades, qualitative assessment measures are likely to wane in 2025.

Especially as companies feel increasing pressure on their margins due to competitive pressures - in part driven by AI - security teams will need to more effectively describe the value they provide the business.

Tools like Factor Analysis of Information Risk (FAIR) methodology and the Hubbard-Seiersen method will thus see increasing adoption in the coming year.

Integrating these methodologies with AI-driven analytics can provide real-time risk insights, enabling companies to prioritize investments more strategically. This shift will not only improve decision-making but also empower security teams to demonstrate their contributions in terms that resonate with executive leadership.

Process flow: Steps in quantitative risk assessment

Conclusion

If you thought 2024 was a whirlwind, buckle up—2025 promises to be just as action-packed.

The political and technological landscapes are undergoing seismic shifts. From a major change in the U.S. Presidential Administration to landmark regulations rolling out across Europe, the scene is as dynamic as ever. On the technological front, AI is rapidly becoming central to nearly every business, pushing security and compliance teams to upskill with advanced tools like GRC engineering and risk quantification to stay ahead.

In short, the next 365 days promise to be transformative for AI and GRC. The good news? Scrut Automation is leading the charge, staying ahead of these developments to help you navigate them seamlessly. Need support with your compliance program? We're here to help— reach out today!