

Gartner®

How General Counsel Can Enhance Board Effectiveness

5 critical areas to become a better strategic partner





1. Communicate AI regulatory updates and manage AI governance



2. Monitor cybersecurity risks and manage disclosures



3. Report misconduct



4. Improve information governance



5. Build and maintain an ESG program

Rapid changes in the technological, political and social fabric are challenging today's general counsel (GC) to guide their board, executive team and department through changing expectations, heightened risks and overall complexity. Now more than ever, boards need timely risk information that is easy to digest and puts the company's risks in perspective.

GC must establish an effective system to support the board. Doing so will enhance the consistency and quality of board oversight while reducing the GC decision-making burden. The best GC turn to Gartner for timely and reliable insight on emerging risks and leverage our experts, research and tools to effectively communicate and take action.

This guide outlines how Gartner has helped GC understand and structure board presentations for, and take action on a series of key emerging risks. Learn how Gartner can help you stay ahead and guide your organization through the inevitable changes in law, geopolitics and technology.



What you need to know

Communicate AI regulatory updates and manage AI governance

The rapid expansion and deployment of artificial intelligence (AI) throughout organizations has resulted in a broad global push to regulate AI. President Biden issued an executive order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence that directed federal agencies to advance key policy objectives surrounding the development of use of AI. Additionally, the EU AI Act and China's AI laws place even greater demands on global enterprises to develop strong AI governance and risk mitigation strategies.

Timeline of key AI regulatory updates

The NYC Automated Employment Decision Tool (AEDT) and other U.S. State laws introduce clauses that regulate AI in areas such as hiring.

President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence is released, directing federal agencies to advance key policy objectives surrounding AI.



China's Interim Measures for the Administration of Generative AI Services, among other new Chinese laws, is administered to ensure that training and AI-generated content are "true and accurate."

The EU AI Act is agreed upon by European Council and Parliament, further harmonizing global governance and risk mitigation rules of AI systems.

Source: Gartner

Recommended action

Communicate AI regulatory updates and manage AI governance

Legal and compliance leaders should ensure their board understands that the AI landscape is rapidly evolving. For this reason, it is crucial to establish a strong AI governance foundation, to accommodate for new and expanding AI regulations as they develop.

Take action with this complimentary resource: [Board Briefing: AI Regulatory Updates](#)



Governance should align with 5 key principles

01 Transparency

Clarify for stakeholders when, whether and how AI is used, including how it makes decisions and arrives at outcomes.



02 Fairness

Ensure AI output and decisions are free from bias and discrimination.



03 Human Oversight

Include human review in relevant steps in AI processes to minimize negative impact on individuals, employees, stakeholders or society.



04 Risk Management

Certify that AI risks are properly understood and assessed, and that decisions related to AI balance the risks and benefits of AI use.



05 Privacy

Minimize the potential for personal data to be processed or stored in a way that increases the chances of privacy harm to a data subject.



Source: Gartner

2

What you need to know

Monitor cybersecurity risks and manage disclosures

In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted cybersecurity disclosure rules related to governance, risk management, and strategy and material cybersecurity incidents. The latest rules require public companies to provide more transparency to investors regarding their governance, oversight and risk management of cybersecurity, and any “material” cybersecurity incidents. This builds on previously issued guidance on disclosure obligations for communicating cybersecurity risks and incidents.

Actions for general counsel to prepare for SEC cybersecurity rules

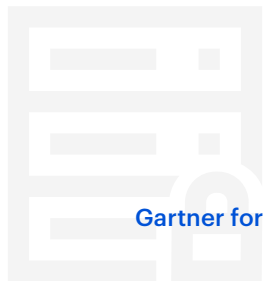
- Evaluate risk management documentation
- Set risk tolerance levels
- Conduct risk assessments
- Establish risk management processes
- Assess monitoring and detection processes



- Verify the effectiveness of reporting and information controls and systems
- Evaluate disclosure controls and procedures
- Review insurance coverages

- Establish incident and crisis response plans
- Establish a process to determine the materiality of cybersecurity incidents
- Prepare for disclosure obligations

SEC = Securities and Exchange Commission
Source: Gartner




2

Recommended action

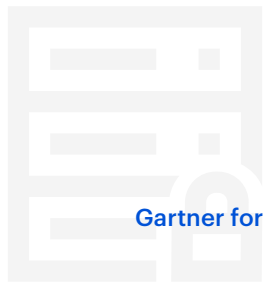
Monitor cybersecurity risks and manage disclosures

Legal, compliance and risk leaders must educate their board on the SEC’s cybersecurity disclosure rules and the impact of the rules on the board’s duty of oversight and responsibility to oversee risk management and strategy.

Take action with this complimentary resource: [Board Briefing on the SEC’s Cybersecurity Disclosure Rules](#) 

<p>What’s the board’s duty of oversight?</p>	<p>Directors must (1) make a good faith effort to establish reporting and information controls and systems to monitor and oversee risks and (2) monitor those systems for indications that implicate</p>
<p>How can the board ensure reporting and information controls and systems are established and effective?</p>	<p>Increase the frequency and type of cybersecurity information presented at board meetings by:</p> <ul style="list-style-type: none"> • Establishing increased time on the agenda for cybersecurity • Encouraging CISO/cybersecurity leader to report on KPIs that they use to monitor risk • Requiring reports on tabletop exercises <p>Encourage senior leadership to reexamine information controls and systems throughout organization by:</p> <ul style="list-style-type: none"> • Reviewing how and when cybersecurity information is shared throughout the organization, including to the board, officers and disclosure committee • Reviewing disclosure committee membership and considering if the CISO/cybersecurity leader should be added • Establishing an incident documentation policy to (1) memorialize the steps taken by the organization in response to an incident and the materiality determinations and (2) track aggregation of minor cybersecurity incidents • Adopting a framework to escalate incidents within the organization (including elevating to the board) • Conducting due diligence and assessments on third parties to determine contract notification provisions and other vulnerabilities • Developing a regulatory notification chart to track different incident reporting obligations

Source: Gartner



3

What you need to know

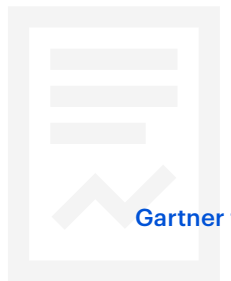
Reporting misconduct

Misconduct reporting has declined for many companies in the past two years, reducing compliance's visibility into organizational misconduct. Among employees who said they did not report observed misconduct, a common reason was their concern that the company wouldn't act on their report. In a hybrid world, several environmental changes deter employees from reporting misconduct. These include distrust in the company due to increasing social polarization, fear of losing jobs amid pandemic-led attrition, competing mental concerns or time commitments and more. Consequently, reporting rates have steadily fallen in recent years, meaning compliance is now learning about 30% fewer misconduct instances.

4 false employee assumptions about the investigation process



n = 901
Source: 2022 Gartner Employee Misconduct Reporting Survey




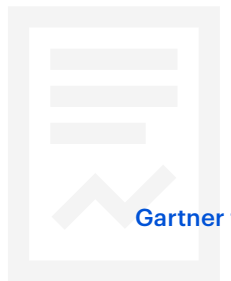
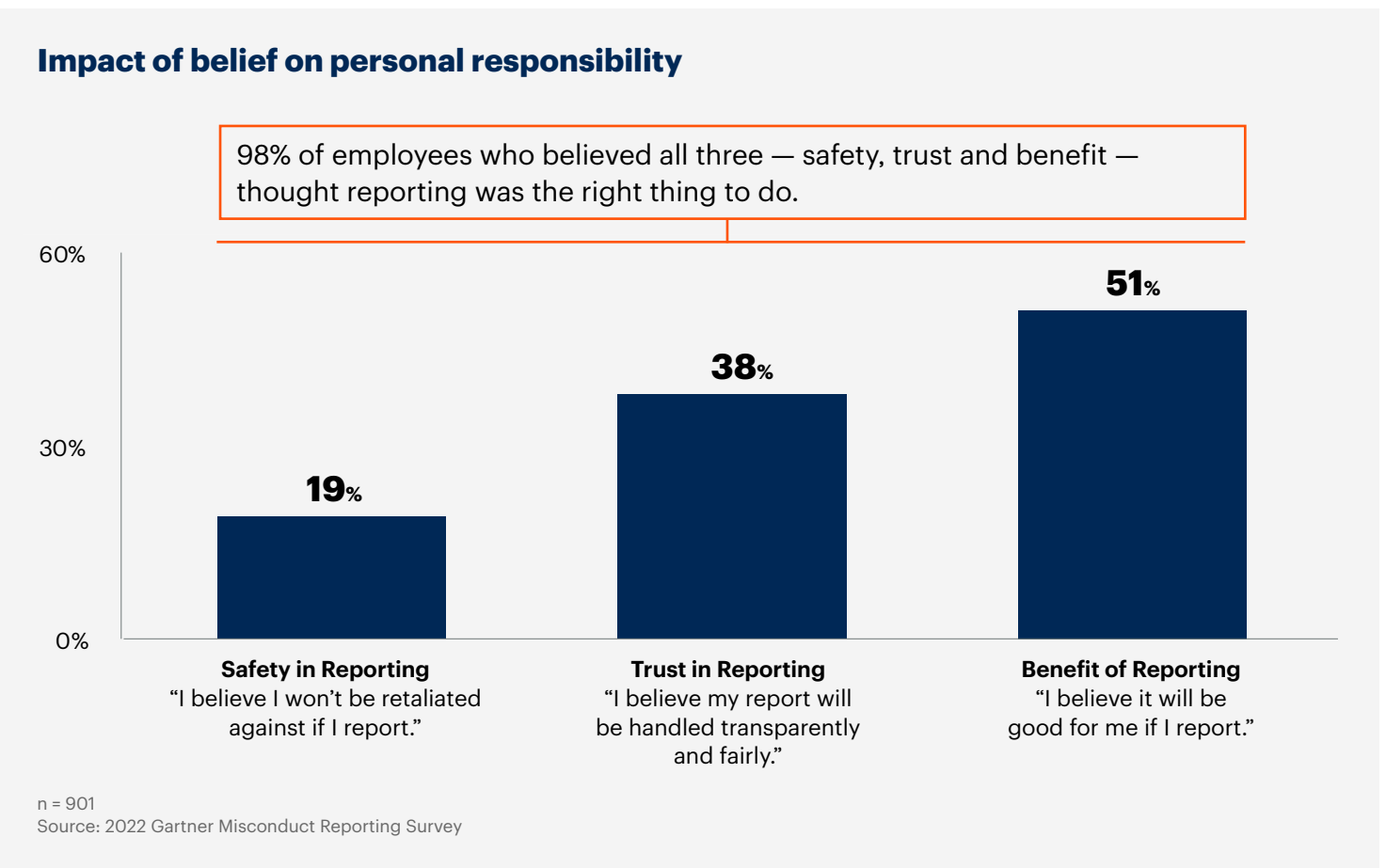
3

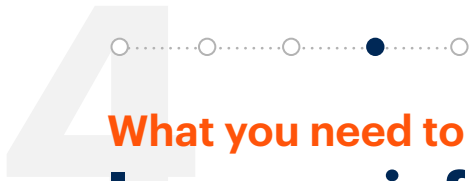
Recommended action

Reporting misconduct

When it comes to employees' perception of culture, general counsel can help their board understand that communication is key. To convince all employees that reporting is the right thing to do despite competing pressures, CCOs must provide them with a new reporting value proposition based on the three drivers proven to have tangible impacts on personal responsibility to report: safety, trust and benefit.

Take action with this complimentary resource: [3 Strategies to Improve Employees' Trust in Reporting Misconduct](#) 



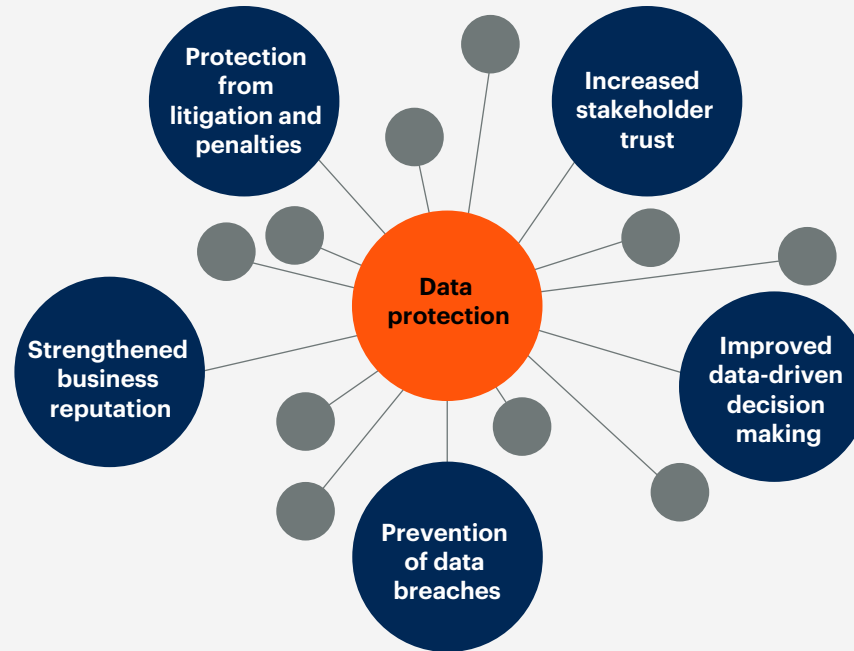


What you need to know

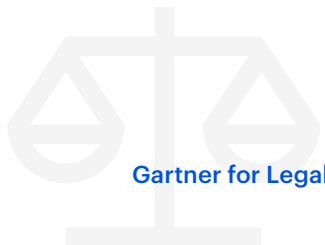
Improve information governance

Operationalizing information governance within the business is essential to driving risk-informed behavior in the valuation, creation, usage, storage, deletion and protection of information. However, business partners often lack basic awareness of what information governance is, how effective information governance benefits their part of the business and what role they play in operationalizing the information governance framework.

Business benefits of information governance




Source: Gartner






Recommended action

Improve information governance

Take action with this complimentary resource: [Driving Business Buy-in for Operationalizing Information Governance](#) 

Legal and compliance leaders must communicate to their board the importance of information governance to develop a policy roadmap and train business partners on roles and responsibilities.

Components of an information governance framework

Key Elements	1. Processes	2. Policies	3. Roles and Responsibilities	4. Metrics
<p>Sample questions that guide information governance framework scoping decisions</p> <p></p>	<ul style="list-style-type: none"> What are our practices and standards (e.g., stewardship) around information life cycle management? Do we have risk assessment and approval processes for collecting, managing and storing information? 	<ul style="list-style-type: none"> How do we choose between a centralized or an integrated framework when outlining the scope of the information governance framework? What data should be within the scope of an information governance framework? 	<ul style="list-style-type: none"> Which stakeholders must be involved in activities like data classification, setting data quality standards, data inventorying and mapping, retention, etc.? Who should handle escalations if a data incident or a data breach occurs? 	<ul style="list-style-type: none"> What is the percentage of company employees who have completed information governance training? What are the results of internal information governance audits? How many privacy incidents and privacy breaches do we encounter in a year? What is the percentage of documents that are marked/unmarked with a classification designation, etc.?

Source: Gartner





What you need to know

Build and maintain an ESG program

Amid rising stakeholder demands, effective environmental, social and governance (ESG) reporting is a corporate imperative. General counsel are often tasked with leading or reviewing ESG reporting. Successful ESG programs require the support of all stakeholders involved, including the board of directors. Organizations must prepare now and have a long-term plan to meet consistently increasing ESG expectations.

Increasing stakeholder interest in ESG

Employees

74%

of employees and consumers expect companies take a public stance on societal issues, regardless of the issue's relevance to corporate objectives

n = 30,284 employees and members of the general public
Source: Gartner Optimizing Communications for Changing Stakeholder Expectations Survey

Consumers

86%

of consumers believe companies should address ESG issues

Source: Gartner Optimizing Communications for Changing Stakeholder Expectations Survey

Investors

2x

increase in investment in ESG funds in 2020

Source: Money Invested in ESG Funds More Than Doubles in a Year, CNBC.




5

Recommended action

Build and maintain an ESG program


General counsel can advise the board on how leading organizations are formalizing their approach to ESG reporting by developing a comprehensive ESG program. Effective ESG programs ensure organizations consistently meet shifting stakeholder expectations; they comprise four key components: understand stakeholder expectations, set ESG strategy and goals, establish program governance and communicate your ESG narrative.

Take action with this complimentary resource: [Board Briefing for Building an ESG Program](#) 




Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for general counsel:




Webinar
Join a Virtual Event
Hear the latest insights from Gartner experts.

[Watch Now](#)




eBook
Define the Leadership Vision for Your Role
Achieve success with data-driven actionable insights.

[Download eBook](#)



Template
Strategic Planning for Your Function
Turn your strategy into action with these tools and templates.

[Download Now](#)



How We Help
Gartner for Legal, Risk & Compliance Leaders
Discover how we can help you tackle your mission-critical priorities.

[Learn More](#)

Already a client?
Get access to even more resources in your client portal. [Log In](#)

Everything you need in a single solution to:

Accelerate technology investments • Increase functional productivity • Modernize risk management approaches



Expert Insights and Interactions

- Tap into latest insights on functional improvement and personal effectiveness, as well as emerging topics like generative AI.
- Get direct access to our global team of research and advisory experts.



Service Delivery Support

- Available in the self-directed delivery model with the support of a service associate.



Peer Experiences

- Quickly solve urgent challenges. Connect with a community of business and tech peers.
- Engage in forums, 1:1 chats, polls, and product ratings and reviews from verified peers.



Must-Attend Events

- In-person and virtual events arm you with actionable plans.
- Be inspired by world-class speakers, thought leaders, experts, demos and peers.



Workflow and Benchmark Tools

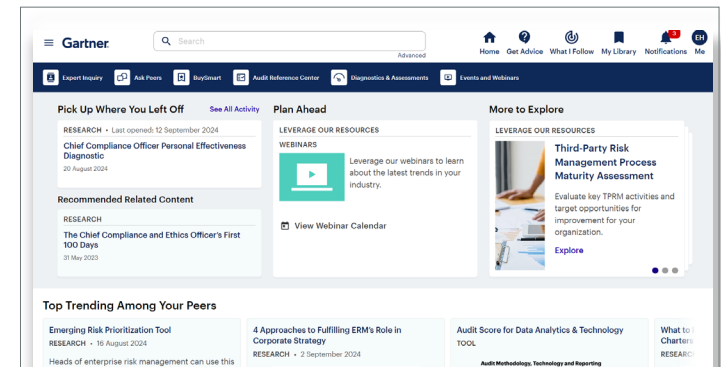
Practical tools and benchmarks to turn strategy into action by helping accelerate key initiatives and drive better business outcomes, including:

- Functional maturity assessments
- Risk assessments
- Budget and efficiency benchmarking



Gartner.com Experience

A customized gartner.com experience that gives you access to the most relevant insights and tools for your role.



Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

[Become a Client](#)

Learn more about Gartner for Legal, Risk & Compliance Leaders

gartner.com/en/legal-compliance

Stay connected to the latest insight

