Gartner

# Prove Cybersecurity Investment Impact at Scale

## Build and evolve a resilient and agile cybersecurity program.

# Build and evolve a resilient and agile cybersecurity program

Chief information security officers (CISOs) must build a resilient cybersecurity program with robust governance, practical strategy, clear metrics and full visibility, ensuring business agility through prevention, detection, response and recovery from cybersecurity incidents.

**62%** of organizations have experienced at least one deepfake attack that included some form of social engineering or exploited existing automated processes.

CISOs who do not build a resilient and agile cybersecurity program will fail to secure board confidence in investments and leave the business exposed to emerging threats.

The Gartner position is clear:

- **Enabling AI** requires net-new cyber investment. Managing new exposures safely demands robust governance frameworks**.**
- **Mitigation and recovery planning** now beats prevention. Architect processes for operational continuity to achieve true agility.
- **Human vulnerability** to misinformation will be as impactful as traditional technology vulnerabilities.

This eBook provides a step-by-step approach to build a resilient program, linking practical strategy to metrics that prove impact.

# Your roadmap to success

In an era of rapid technology evolution and emerging AI threats, CISOs face mounting pressure to ensure business agility while managing new risk exposures and closing a critical board confidence gap. To be effective, they must build a resilient cybersecurity program founded on robust governance, practical strategy and transparent, business-aligned communication.

Gartner equips CISOs with continuous assessment tools, outcome-driven metrics and structured guidance to systematically baseline controls maturity, optimize resource allocation and communicate investment impact to stakeholders — supporting resilient operations and securing essential board support.

1. **Define program scope, governance and accountability structure.**
2. Prioritize resource allocation for critical security processes and capabilities.
3. Architect processes, services and technologies that support resilience.
4. Measure performance using clear, outcome-driven security metrics.
5. Communicate cybersecurity and identity and access management (IAM) investment impact to senior stakeholders.

## One key outcome to consider in Step 1

**Set clear strategy, boundaries and governance structures** to drive program resilience, agility and accountability across cybersecurity and IAM initiatives.

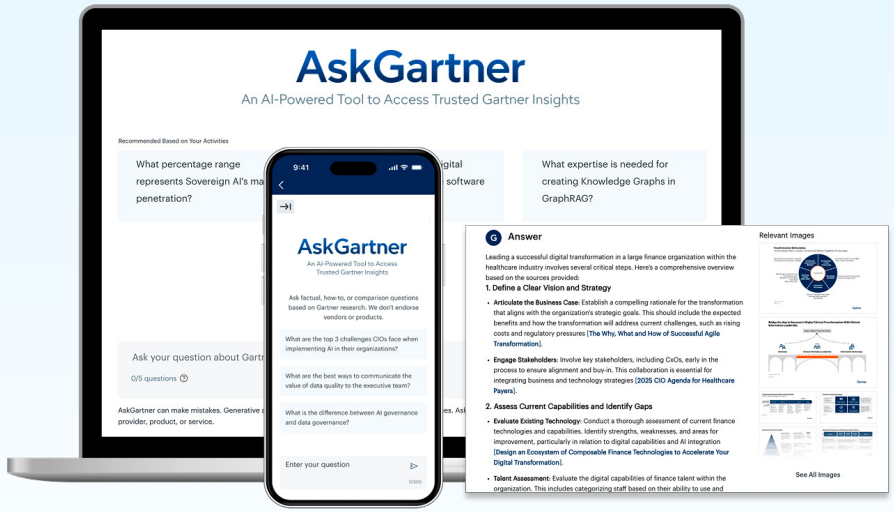
# Key questions to ask

Gartner clients can ask questions like these directly using AskGartner.

**Gartner clients can click to explore answers.**

| | |
|---|---|
| How do I build a cybersecurity program and strategy that delivers and enables adaptive organizational resilience and growth? | Explore answer ↗ |
| How can IAM be integrated into cybersecurity strategies to strengthen security and enable business outcomes? | Explore answer ↗ |
| How do I build an effective third-party cybersecurity risk management capability? | Explore answer ↗ |
| How do I improve the quality of my cybersecurity risk management decision making? | Explore answer ↗ |
| How can I benchmark our cybersecurity program and prioritize investments in my strategy and roadmap? | Explore answer ↗ |

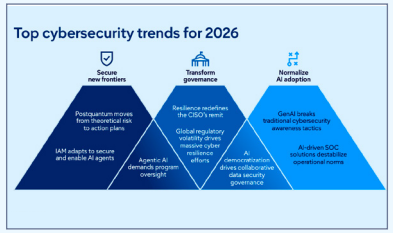
## Your peers use AskGartner to answer these questions in minutes.




Learn More

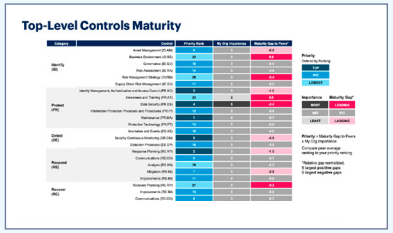
# Gartner resources turn your priorities into plans and actions

## 1. Define program scope, governance and accountability structure.



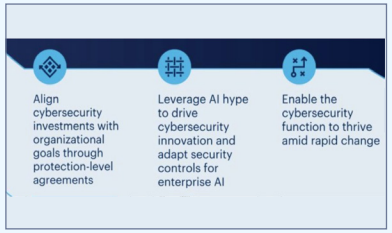

Top Cybersecurity Trends CISOs Must Act on in 2026 ↗

## 2. Prioritize resource allocation for critical security processes and capabilities.



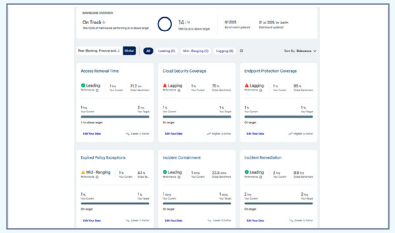

Cybersecurity Controls Assessment ↗

## 3. Architect processes, services and technologies that support resilience.




Cybersecurity's Top Projects for 2026: What CISOs Must Deliver Next↗

## 4. Measure performance using clear, outcome-driven security metrics.



Cybersecurity Business Value Benchmark ↗

## 5. Communicate cybersecurity and IAM investment impact to senior stakeholders.


Gartner CISO Effectiveness Diagnostic ↗

## Engage with Gartner

- Baseline your controls maturity with Gartner Controls Assessment tools.
- Leverage the Gartner Outcome-Driven Metric/Protection Level Agreement approach to communicate cybersecurity value.
- Use Gartner frameworks to track progress and validate and demonstrate success.

## Expected outcomes

- Prioritize control gaps for remediation to maximize investment impact.
- Improve board engagement leading to increased funding and support.
- Prepare adequately for new roles and job functions as a result of AI.

# Who needs to be involved?

The most successful organizations establish cross-functional teams for their cyber resilience initiatives. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.



### CIO/head of technology ↗

Sets a clear enterprisewide cybersecurity ambition, identifies use cases, quantifies benefits and risks, aligns teams and competencies and drives innovation across the organization.

### Head of AI ↗

Develops, champions and executes the organization's AI strategy through thinking of cyber resilience by overseeing AI use case selection, scaling and risk, establishing governance and literacy, implementing solutions, monitoring market trends, building a world-class team and reporting on business impact.

### Chief data and analytics officer and team ↗

Lead the organization's cybersecurity data strategy by identifying use cases, establishing governance, developing new data value and ensuring data readiness for cybersecurity technologies.

### Head of enterprise architecture and team ↗

Align cybersecurity structure and design with organizational value by guiding use cases and requirements, governing architecture investments, leading adoption decisions and architecting cybersecurity solutions.

### Software engineering leader and team ↗

Drive cybersecurity integration by clarifying desired outcomes, establishing engineering best practices, transforming services with a cybersecurity-first approach and architecting software development to support cybersecurity objectives.

Client Story

# HUGO BOSS Enhances Cybersecurity Transparency and Agility

### Mission-critical priority

Stefan Baldus, Chief Information Security Officer at HUGO BOSS, sought to establish a resilient cybersecurity program that enhanced transparency and integration across the enterprise. His core priority was ensuring business agility and driving faster organizational performance by building a practical strategy with full visibility.

### How HUGO BOSS leveraged Gartner resources

To evaluate the maturity of the company's cybersecurity controls, the CISO leveraged the Gartner Cybersecurity Controls Assessment to prioritize key initiatives and areas for improvement. Additionally, they partnered with Gartner analysts to interpret these assessment results, gather insights on incorporating agility, and develop a strategic roadmap for highly effective board presentations.

### Mission accomplished

With guidance from Gartner, HUGO BOSS successfully integrated agility into their cybersecurity program, transforming their organizational structure to enhance both transparency and efficiency. The CISO was able to effectively communicate the critical importance of cybersecurity to leadership, which directly resulted in securing the necessary funding to move forward. Furthermore, the CISO was able to network with a community of like-minded peers at the Gartner Security and Risk Management Summit to continue their program's evolution.

**Watch the full story ↗**

# Address your other mission-critical priorities

## Build and evolve a resilient and agile cybersecurity program

Only **14%** of nonexecutive directors are very or extremely confident in the effectiveness of current cyber risk assessments.

## Adapt cybersecurity strategies for AI

**91%** of senior business leaders see AI as a value driver, making AI cybersecurity governance essential.

## Optimize cybersecurity technology and architecture effectiveness

**75%** of CISOs identify budget or resource constraints as a challenge to meet their strategic objectives in the next six months.

# Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

**U.S.:** 1 855 322 5484

**International:** +44 (0) 3300 296 946

Become a Client

Interested in becoming a client?

**Learn more about Gartner for CISOs**
https://www.gartner.com/en/cybersecurity

**Stay connected to the latest insights**



Gartner®