Gartner

Mitigate AI Cybersecurity Risks: A Public Sector Leader's Roadmap

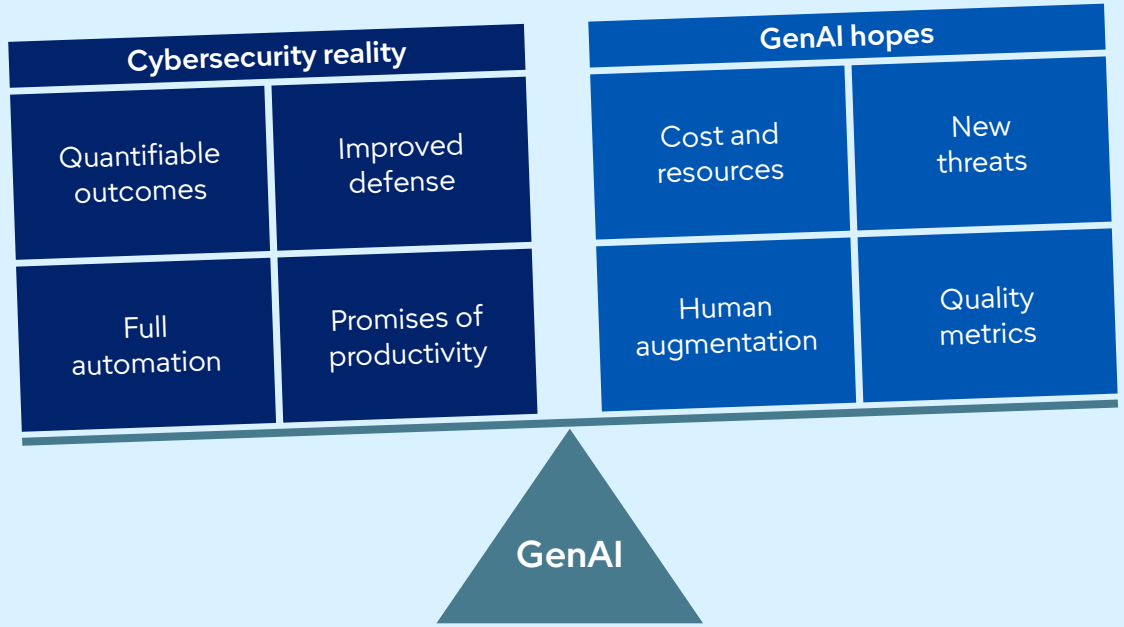
Minimize disruption, manage risk and harness the value of AI.

Mitigate cybersecurity threats before applying AI solutions to government services

Government technology leaders and CISOs need a comprehensive AI cybersecurity strategy. However, AI cybersecurity strategies are likely to fail with a potentially catastrophic impact on mission outcomes if they are not differentiated from responsibility frameworks. While responsibility frameworks address things like transparency, value, human in the loop and other priorities, they do not provide guidance for **mitigating threats that target AI-based systems.**

With **77% of government technology leaders reporting plans to increase AI investments in 2026,** having a plan to implement AI trust, risk and security management (TRiSM) and mitigate threats targeting AI systems will be essential to securing mission outcomes and citizen trust.

Balancing cybersecurity reality with GenAI hopes



Source: Gartner

Some of the top questions your peers are asking about AI in cybersecurity:

1. How can we rightsize AI's impact to ensure responsible and ethical use in public sector operations?

2. In what ways can we maximize AI's value to improve service delivery, streamline operations and enhance threat detection across our organization?

3. How can we anticipate and prepare for future changes in regulations, technology and the evolving threat landscape to stay ahead of emerging risks?

What are the key stages?

This roadmap will equip public sector CIOs and CISOs with practical guidance to responsibly adopt AI, prioritize and manage cybersecurity risks, maximize the value of AI in government operations and proactively prepare for future regulatory and technological changes.

Minimize disruption: Rightsize AI impact

Pivoting to AI in the public sector will require new or adapted governance principles, along with a well-defined cyber roadmap that integrates robust, AI-focused considerations.

Actions to take:

- ☐ **Adapt application security strategy to AI.** Leverage privacy-enhancing technologies to protect sensitive citizen data.
- ☐ **Integrate new AI technologies into cybersecurity,** ensuring alignment with policy mandates and mission operations.
- ☐ **Update risk management frameworks** to address evolving AI skills, fostering improvement and protecting public trust in government digital services.

Sample of Gartner client resources include:

Insights
- Top Trends in Cybersecurity for 2026
- 2026 Cybersecurity Leaders' Priority: Adapt Cybersecurity Strategies for AI

Tool
- Monitor the AI Solution Deployed for AI-Assisted Reference Architecture Generation

77%

of government technology executives reported their enterprises would increase AI investments in 2026.

Source: Gartner

→ Fast-track government priorities with our **Accelerators for public sector leaders.**

Manage risk: Prioritize securing AI applications

This checklist ensures your organization looks beyond responsibility frameworks and concentrates on emerging threats that will target your AI-based systems.

Actions to take:

- ☐ **Form a cross-functional team/ dedicated unit** to oversee and coordinate AI TRiSM efforts across your government organization.
- ☐ **Collaborate across departments** to select, integrate and maintain best-in-class tools that support a comprehensive, government-aligned AI TRiSM program.
- ☐ **Regularly monitor AI usage** against defined objectives and compliance requirements.

Sample of Gartner client resources include:

Insights
- Emerging Tech: The Future of AI Security Is in Securing Agent Actions, Not Prompts
- Adapt IAM to Secure AI Agents
- Apply Crime Prevention Principles to Secure Agentic AI
- How to Secure Custom-Built AI Agents
- Best Practices to Mitigate Security Risks With Agentic Coding Tools

Tool
- Build an Adaptive Roadmap to Secure and Enable the Use of AI
- AI Cybersecurity Strategy and Roadmap on a Page

By 2028, at least

80%

of governments will deploy AI agents to automate routine decision making, enhancing efficiency and service delivery.

Source: Gartner

→ Watch the on-demand webinar: **The Gartner Framework to Manage AI Governance, Trust, Risk and Security**

Manage risk

Focus on 3 key areas of risk

AI offers significant benefits for government organizations, including improved efficiency and service delivery. However, it also introduces three critical categories of risk that public sector organizations must address:

Content anomaly detection

- Develop "guardian agents" to monitor data and models across all stages of development and deployment for flagging of suspicious activities.
- Monitor for unacceptable or malicious use of GenAI.
- Identify and mitigate hallucinations, misinformation or outputs that may be inaccurate, illegal or infringe on copyright.
- Ensure GenAI-generated content aligns with policy standards, legal requirements and ethical guidelines.

Data protection

- Adapt IAM to secure AI agents.
- Prevent data leakage and protect sensitive citizen and government information.
- Safeguard content and user data from compromise during GenAI processing.
- Enforce privacy and data protection policies, conduct privacy impact assessments and ensure compliance with regional and national regulations.
- Promote data management and AI sovereignty by selecting a national provider that hosts data locally.

Application security

- Secure custom-built AI agents.
- Defend against adversarial prompting attacks and other GenAI-specific threats.
- Protect vector databases and application endpoints from unauthorized access or manipulation.
- Continuously monitor for and respond to hacking attempts targeting GenAI-enabled systems.

Harness AI to maximize potential

Government IT leaders are under growing pressure to embed AI into decision-making capabilities. To harness AI's benefits while managing risks, government organizations require a model that integrates data-driven insights, human judgment and ethical safeguards.

Actions to take:

- ☐ **Evaluate AI technologies** and decide what "good" looks like for your organization, considering mission objectives, legal requirements and public trust.
- ☐ **Maintain and improve** your organization's ability to detect, assess and respond to uncertain or ambiguous threats arising from AI adoption.
- ☐ **Allocate resources** to proactively identify, monitor and address the most relevant risks to your organization.

Sample of Gartner client resources include:

Insights
- Top Trend in Government: AI for Decision Intelligence

Guide
- Hype Cycle for AI and Cybersecurity, 2025

Tool
- AI Cybersecurity Strategy and Roadmap on a Page

By 2029,

70%

of government agencies will require explainable AI and human-in-the-loop mechanisms for all automated decisions that impact citizen service delivery.

Source: Gartner

Discover 1,000+ proven AI use cases and real-world case studies with Gartner AI Use Case Insights for faster, stronger results.

Harness AI

GenAI promises to transform a wide range of security and business processes

To maximize value and uphold public trust, CIOs and CISOs should prioritize the following:

CIO checklist

- ☐ **Check inventory and monitor and manage AI consumption** of third-party GenAI applications and features.
- ☐ **Update provider and technology selection requirements** to address privacy, copyright, traceability and explainability, AI sovereignty, citizen data and ensuring accountability.
- ☐ **Enhance AI application and data security practices** by integrating protections against new attack surfaces.
- ☐ **Conduct proof of concept before deploying GenAI into cybersecurity programs,** aiming to augment staff capabilities rather than replace them.
- ☐ **Monitor changes in the threat landscape.** Ensure access to timely intelligence on emerging threats, while recognizing that scenario planning for future GenAI.

CISO checklist

- ☐ **Assess AI technologies** for risks to sensitive government data, just as with any other tool.
- ☐ **Define clear success criteria** to measure how AI enhances existing security metrics without introducing unnecessary complexity.
- ☐ **Pilot new GenAI features** from security vendors in focused, high-priority areas like security operations and application security.
- ☐ **Apply the AI TRiSM framework** when developing or adopting GenAI and LLM applications, ensuring transparency, accountability and compliance.
- ☐ **Train teams** to address both direct risks (privacy, IP, AI security) and indirect impacts from GenAI use across departments such as HR, finance and procurement.

Critical leadership roles to successfully set a strategy and implementation plan for AI

CIO/Head of Technology/AI Leader

Government CIOs are relied upon by organizational leaders, lawmakers, oversight groups, peers and other government stakeholders to develop a formal AI strategy that enables you to:

- Set an AI ambition that aligns with your mission objectives, identify use cases and quantify both benefits and risks.
- Align operations and technology teams and evolve organizational competencies to support AI adoption.

CISO/Security Leader and Team

Cybersecurity leaders must ensure that cybersecurity and data privacy are an integral part of AI strategy and successfully:

- Provide overall program oversight on security and risk.
- Anticipate and take actions against unforeseen consequences such as data breaches.
- Continuously update skills and readiness against new threats.

CDAO/Data and Analytics Leader and Team

D&A leaders are expected to lead their organizations in setting the data for AI strategy and must successfully:

- Identify AI use cases for augmented analytics and data management.
- Leverage existing D&A practices and establish D&A governance policies for AI.
- Develop new sources of value from data leveraging AI.
- Be AI-data ready.

Enterprise Architecture Leader and Team

EA leaders are expected to drive tangible improvements to mission outcomes from AI and must successfully:

- Own the full AI infrastructure roadmap.
- Govern AI technology architecture investment decisions.
- Lead decision making about adopting AI solutions to drive mission outcomes.

Software Engineering Leader and Team

Software engineering leaders must understand the implications of AI technology in depth and successfully:

- Clarify the desired benefits for AI integration.
- Establish AI engineering best practices across the organization.
- Transform products, services and experiences and build an AI-first approach into roadmaps.

Client Story

Environmental Protection Agency (EPA) Ireland Enhances Cybersecurity and Strategic Planning

Mission-critical priority

The CIO sought Gartner expertise to enhance cybersecurity. They needed to streamline ICT strategy and align operations with strategic goals. They also aimed to address sustainability and disaster recovery challenges.

How Gartner helped

Gartner analysis helped EPA Ireland elevate the ISO role and establish a dedicated cybersecurity team, enhancing their security framework with a specific budget. The Gartner strategic models enabled EPA Ireland to create a concise, two-page ICT strategy, aligning technological vision with board expectations.

Outcome

By collaborating with Gartner, EPA Ireland **improved its security and reduced threats by 40%,** gained clear strategic direction and executive approval and proactively addressed challenges such as sustainability and disaster recovery.

Watch the Full Story ↗

Actionable, objective decision intelligence

Explore these additional complimentary resources and tools for public sector leaders:

eBook

Safeguard Public Trust: A Roadmap to Cybersecurity Readiness

Get actionable steps and resources to develop an effective cybersecurity strategy.

Download Now

eBook

Unlocking AI Value: 5 Steps for Public Sector Leaders

Lead your organization's AI journey and achieve sustainable, mission-driven results.

Learn More

eBook

Improve Government Efficiency and Effectiveness With AI, Data and Analytics

Overcome modernization barriers and unlock AI value in your government organization.

Download Now

Tool

Accelerators for Government CIOs

Explore our step-by-step tools and diagnostics tailored specifically for government CIOs.

Learn More

Already a client? Get access to even more resources in your client portal. Log In ↗

Connect with us

Get actionable, objective decision intelligence to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance.

U.S.: 1 855 322 5484
International: +44 (0) 3300 296 946

Become a Client

Learn more about Gartner for Government IT Leaders
gartner.com/en/industries/government-public-sector

Stay connected to the latest insights

Gartner®