Executive Office of the Governor
Office of the Chief Inspector General

Artificial Intelligence and Cybersecurity

The Honorable Ron DeSantis
Governor of Florida

Melinda M. Miguel
Chief Inspector General

What is the State of Cybersecurity?

Source: ISACA's State of Cybersecurity 2025 Global Report. Infographic. Released on September 29, 205.

GOVERNMENT & POLITICS

Cyber attack headaches linger at state patrol, other Ga. agencies

BY: **BEAU EVANS** - SEPTEMBER 9, 2019 8:40 AM

Over the course of a month starting in late June, three separate ransomware attacks struck the state's courts, emergency management and the Georgia Department of Public Safety. Pixa photo.

Cyber attacks that hit some state agencies in Georgia earlier this summer continue to ripple through the system, particularly for law enforcement and the courts.

Meanwhile, security officials work to boost software safeguards and train thousands of employees to avoid

lerk
ack online

THE CLERKS AUTHORITY
Georgia Superior Court Clerks' Cooperative Authority

glossary login

FILE SEARCH LEARN MANAGE FINES & FEES CLERKS NOTARY & APOSTILLES

SYSTEM MAINTENANCE IN PROGRESS

Due to a credible and ongoing cybersecurity threat, the Clerks' Authority activated its defensive security protocols, which include temporarily restricting access its website and related services. We are committed to ensuring that our systems will be operational as soon as possible. However, out of an abundance of caution, we continue to test and analyze our systems before they are made accessible to ensure maximum safety. We apologize for the inconvenience, and w appreciate your patience.

Recent ransomware attacks and nudging from national associations have prompted the governor to mandate all state employees undergo twice-yearly training.

BY BENJAMIN FREED • AUGUST 15, 2019

orgia SNAP call center berattack tied to incidents in tes: USDA

Published August 15, 2025 6:37am EDT | Georgia | FOX 5 Atlanta |

and state authorities are investigating a cyberattack that shut down 's SNAP call center for over a week.

ng to officials, they've received reports of similar incidents in Delaware, , Iowa, Oklahoma, and Virginia.

orgia Department of Human Services urges anyone with an EBT card to their pin as soon as possible to ensure funds are secure.

n Greig
2025

Cybercrime

e insights with the corded Future ligence Cloud. earn more.

Hackers launch 'serious' attacks agair school district, New Mexico university

Multiple school districts and a university in New Mexico are currently cyberattacks causing operational issues for thousands of students.

In a statement on Sunday, Georgia's Coweta County School System s cyberattack on Friday evening that will impact its 23,000 students ac

"Some school system network processes will be hampered in the co system employees have been advised not to access desktop devices being investigated," the school district said.

School system official Dean Jackson called the attack "serious" and reported to the Georgia Emergency Management Authority and Hom

Cyber Incidents/Events in Georgia

SECTION 2. RISK LEVELS

Exhibit 1. North America – Highest Risks

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 271 for North America.

Source: IIA Global Risk in Focus (2026)

SECTION 3. AUDIT PRIORITIES

Exhibit 5: North America – Highest Audit Priorities

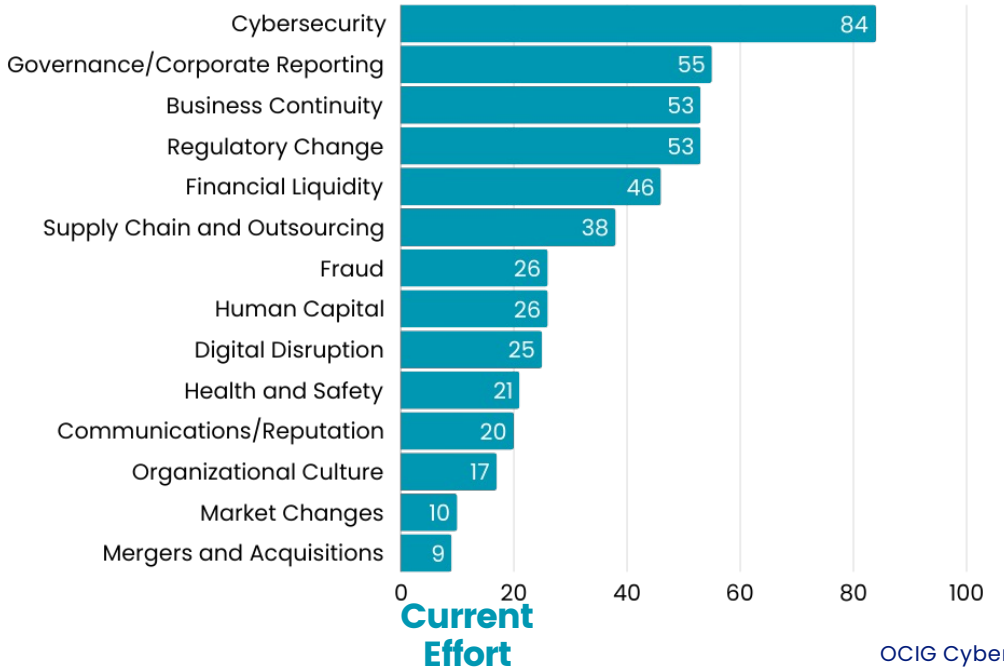
Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

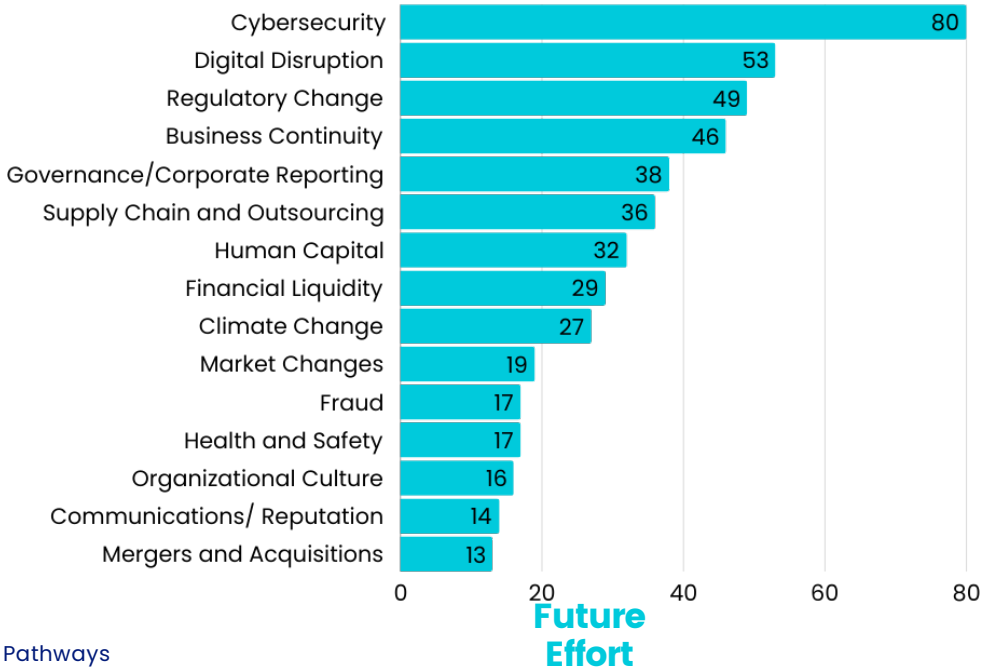
Current Audit Effort vs. Future Audit Effort (North America)

What are the top five risk on which audit spends the most time and effort?

What are the top five risk you expect internal audit to spend the most time and effort addressing three years from now?

- Overwhelmingly, CAEs chose cyber security as a top five area for internal audit effort (84%)
- Second place is held by governance/corporate reporting, but this area is expected to decrease in the future.





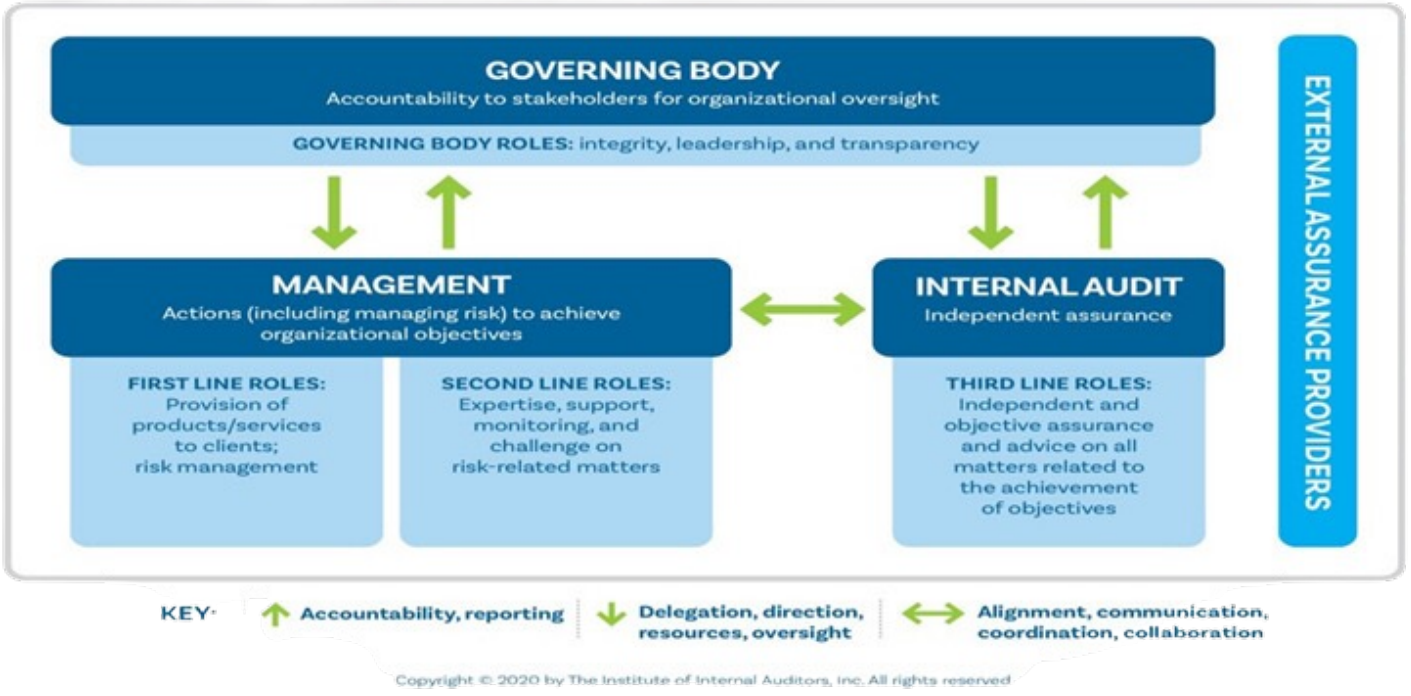
OCIG Cyber Pathways

The Florida IG Act of 1994

Section 20.055, F.S. requires Inspectors General to:

- Conduct audits, investigations, inspections, reviews
  - **Fraud, waste, abuse, economy & efficiency of government operations**
- Develop annual and long-term internal audit plans
  - Including a *specific cybersecurity audit plan (HB 1297 in 2021)*
  - Based on periodic **risk assessments** (of agency programs, operations, funding, etc.)
  - Conducted in accordance with **professional standards** (IIA's Red Book, AIG Green Book, Yellow Book)
- Have staff with IT auditing experience
- Report results to appropriate parties
- Make recommendations for improvement
- Refer criminal matters to law enforcement

The IIA's Three Lines Model



$1M Annual Budget for CIG Cyber Pathways Program

Florida Offices of Inspectors General adopted a multi-featured cyber resilience pathways program supported by the Office of the Chief Inspector General. This program created "pathways" to cyber competency and to fulfill expectations associated with amendments to the Florida IG Act in 2021 (HB 1297) that requires an annual specific cyber audit plan.

The Cyber Pathways Program equips State Agency Offices of Inspectors General staff with the fundamentals required to audit, investigate, inspect, and review cybersecurity risk management and cybersecurity operations, and assess agency compliance with government requirements such as NIST while following professional auditing standards.

The Cyber Pathways Program includes the following:

1. Training on Auditing or Investigating Cybersecurity Issues
2. Tools to Improve the Process
3. Audit Enablement through Subject Matter Expert Advisory Services

Benefits of the Cyber Pathway Program

More effective cybersecurity auditing	Reduced need for staff augmentation to perform cybersecurity audits
More Effective Investigations	More strategic awareness of agency's IT operations and enterprise security governance
Enhanced skillset, better ability to assess risk, evaluate internal control, and abiliy to add value to	Better ability to identify fraud, waste, and abuse throughout the enterprise
Ability to assess threats and vulnerabilities to state information technology resources	Building a culture of security within state agencies
Increased compliance with cybersecurity rules, regulations, and governing directives	Enhanced technological defenses against cyber threats
Better governance, increased value to state agencies, more secure continuity of operations	Ensure the integrity of state resources and mitigating the risk of leaks and breaches throughout the organization

Enhanced compliance with required professional auditing standards (Standards 3.1 (Competency), 7.2 CAE Qualifications), 8.2 (Resources), 10.2 (HR Management), 13.4, 9.4, 13.2, 13.6, 14.6) requiring consideration of cybersecurity risks in planning and performing audit engagements.

Florida OCIG Enterprise Cybersecurity Audits Completed

The Florida Cybersecurity Standards are based on the NIST Cybersecurity Framework (CSF) and is in sync with the CSF version 1.1 . These are being updated to 2.0.

Function Identifier		Category Identifier	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Enviroment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PE.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

FY 24/25 ID.AM - Asset Management

FY 22/23 PR.AC – Identity and Access Controls

FY 25/26 PR.DS – Data Protection and Security

FY 21/22 DE. CM – Security Continuous Monitoring

FY 23/24 VARIOUS – Incident Response, Recovery, and Reporting

Updated as of FY 24/25 OCIG Cyber Pathways

Highlights from Cybers Pathways Training Sessions

- The OCIG has trained over 736 Unique Attendees – included over 100 unique attendees thus far in FY 25/26
- Attendees have included those not only from Executive Agency OIG staff (Management, Admin Staff, Auditors, Investigators), but also all Agency OIG staff, Local IG Offices, University IG Staff, Water Management Districts, Clerks of Courts IG Offices, Agency CIOs, Agency ISMs, Other IT Staff.
- 22,480.25 Hours of Training provided since program inception in FY 21-22
- 56 training session provided thus far. Courses have included Cyber Fundamentals (2-Day), Risk Management Framework Introduction, FBI Bootcamp, Cyber Investigations, Auditing the Cybersecurity Program, Privileged Account Management, and certification courses (CISA, CGEIT, etc.)

OCIG Cyber Pathways Metrics as of November 2025


TENNESSEE
"GEORGIA ON MY MIND"
CHATTAHOOCHEE NATIONAL FOREST
ALABAMA
DALTON
GALHOUN
ROME
CARTERSVILLE
KENNESAW
CANTON
WOODSTOCK
MILTON
PEACHTREE CORNERS
MARIETTA
ROSWELL
JOHNS CREEK
SANDY SPRINGS
SMYRNA
ALPHARETTA
ATHENS
DECATUR
SOUTH CAROLINA
VILLA RICA
DOUGLASVILLE
ATLANTA
OCONEE NATIONAL FOREST
EAST POINT
FAIRBURN
UNION CITY
RIVERDALE
FAYETTEVILLE
LOVEJOY
CARROLLTON
FOREST PARK
STOCKBRIDGE
COVINGTON
NEWNAN
PEACHTREE CITY
MCDONOUGH
GRANTVILLE
HOGANSVILLE
GRIFFIN
SAVANNAH RIVER
LA GRANGE
EVANS
AUGUSTA
GROVETOWN
MANCHESTER
PINE MOUNTAIN
HAMILTON
MACON
MILLEDGEVILLE
WAYNESBORO
COLUMBUS
WARNER ROBINS
PERRY
DUBLIN
"WISDOM JUSTICE AND AMERICUS MODERATION"
STATESBORO
SYLVANIA
GREEN CITY
ESTABLISHED
RINGON
EDEN
POOLER
SAVANNAH
PLAINS
1778
BLOOMINGDALE
DAWSON
HINESVILLE
EDISON
MORGAN
ALBANY
FLEMING
MIDWAY
RICHMOND HILL
KELLER
RICEBORO
FANCY HALL
OSSABAW ISLAND
CAMILLA
ASHBURN
TIFTON
TY TY
BACONTON
THE PEACH STATE
HOBOKEN
NAHUNTA
BRUNSWICK
159
SYLVESTER
MOULTRIE
HAHIRA
WAYCROSS
COUNTIES
VALDOSTA
THOMASVILLE
OKEFENOKEE NATIONAL WILDLIFE REFUGE
LAKE PARK
CAIRO
BOSTON
KINGSLAND
ST MARYS
FLORIDA
ATLANTIC OCEAN
N
W
E
S
GEORGIA

GTA Office of Information Security

We aim to enhance security on state networks, develop a cyber-ready workforce, and build enduring partnerships. GTA OIS is available to assist state and local government entities with questions related to cybersecurity.

REPORT A CYBER INCIDENT

Cyber Dawg Live-Fire Exercise

September 22 - 26, 2025

Cyber Dawg 2025 was a successful live-fire exercise with a record 129 players from 33 organizations, focusing on detection and analysis. Blue teams, mostly new talent, defended against simulated nation-state threats, enhancing inter-agency collaboration and improving Georgia's defensive posture.

LEARN MORE

State and Local Cybersecurity Grant Program

On September 16, 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind

Governance, Risk, and Compliance

GTA OIS works collaboratively with information security organizations at all levels of state government. We offer assistance and subject matter expertise to help build, manage, and mature cybersecurity programs as well as provide support to identify and manage IT-related risk.

What happens?

Cyber Dawg is a multi-day, live-action exercise where
against advanced attackers. The exercise is designed
threats in real time, react to simulated breaches, and
operations.

The event uses a complex sandbox environment with
including captured IP blocks from U.S. adversaries, su
Korea, providing a real-world cyber threat landscape.

Exercise roles

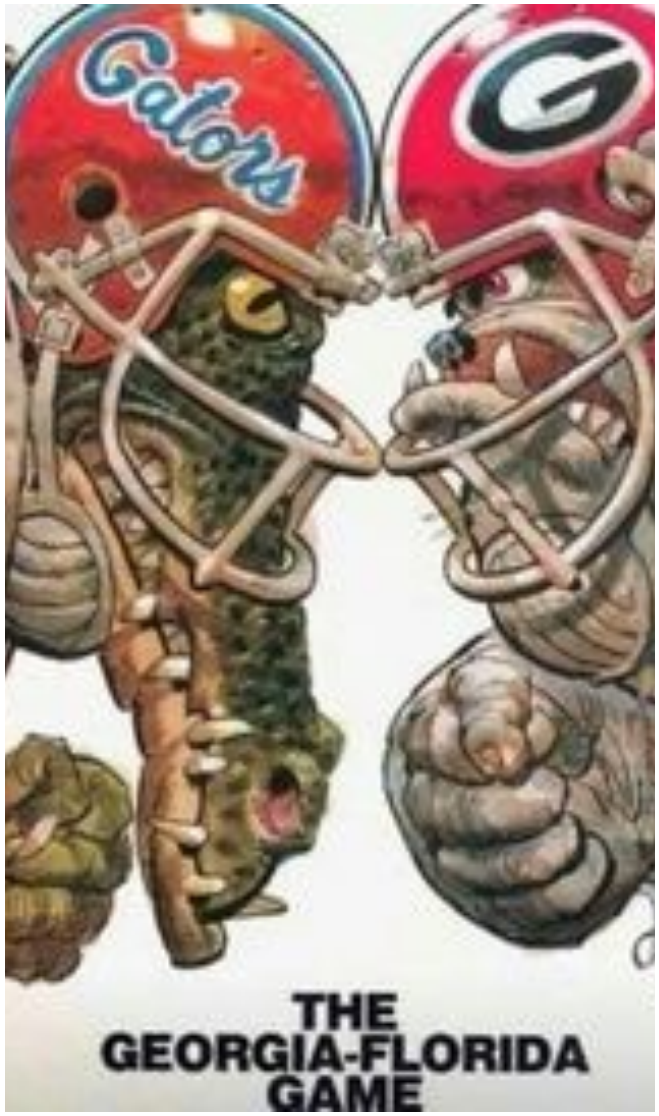
RED TEAM: Attackers - The red team is offensiv
attacks on simulated agency infrastructure, leverag
and challenge the defending blue team.

BLUE TEAM: Defenders - The blue teams (there
attacks. They are the cybersecurity professionals fr
organizations.

WHITE CELL: The white cell, comprised of leade
smooth execution of the Cyber Dawg exercise

FUSION CELL: The fusion cell, comprised of cyb
intelligence for the exercise.

GOLD TEAM: The gold team is incident response



Cyber Dawg Live-Fi

Event ended September 26, 2025

on training exercise at the Georgia Cyber Innovation and Training Center
a cyber-attack in a controlled environment. Cybersecurity professionals
kills. It's a high-pressure scenario without the real-world risks.

Georgia's cyber readiness

ith the Georgia
se, successfully
025, a live-fire
held September 22
ber Innovation and

a record 129
organizations,
increase over 2024.
ne was composed of
ate agency
across 11 simulated
s. Under continuous
isticated red team
documented nation-state threat actor, they were tasked with
and escalating suspicious activity.

he blue team members were first-time participants, underscoring
developing new talent. The red team's multi-phase campaign,
ngineering and exploitation to lateral movement and controlled

Executive Office of the Governor
Office of the Chief Inspector General

Artificial Intelligence for Offices of Inspector General

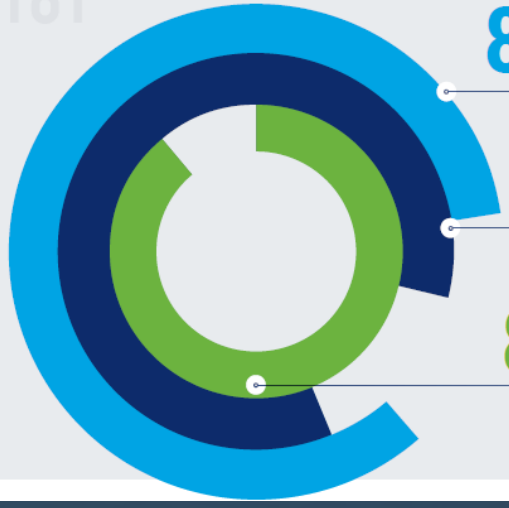
AI Knowledge and Skills In Demand

31%

of organizations are increasing jobs for AI-related functions **IN THE NEXT 12 MONTHS.**

72%

believe that **AI SKILLS ARE VERY OR EXTREMELY IMPORTANT** for professionals in their field right now.



84% consider themselves to currently have just a beginner or intermediate level of expertise in AI.

85% agree or strongly agree that many jobs will be modified due to AI.

89% of digital trust professionals say they will need AI training within the next two years to advance their careers or even keep their current roles. 45% say it is needed within the next six months.

AI Policies and Training Still Lacking

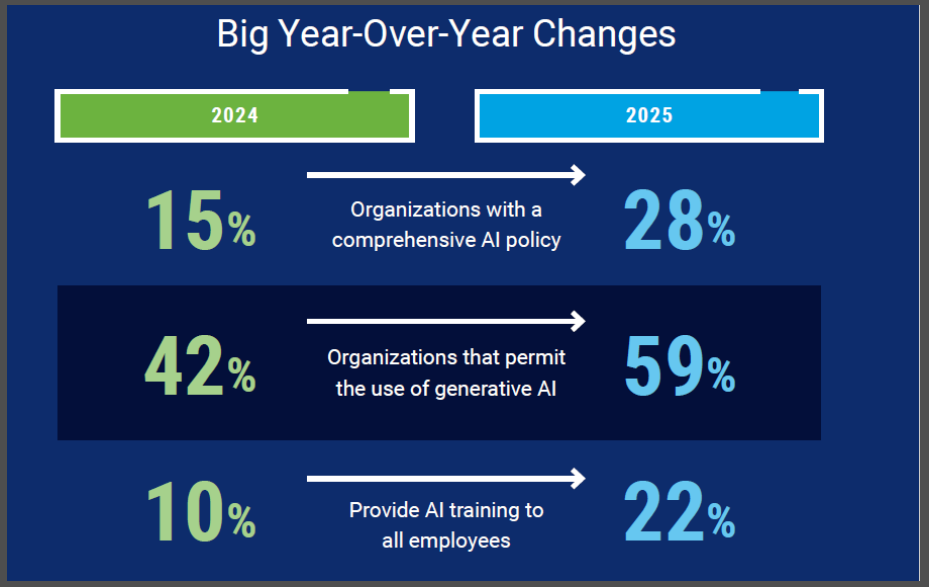
81%

believe employees within their organization use AI, **WHETHER OR NOT IT IS PERMITTED.**

YET ONLY 28%

of organizations have a **FORMAL, COMPREHENSIVE POLICY** in place for AI.

Big Year-Over-Year Changes



Standard 10.3 Technological Resources

Requirements

The chief audit executive must strive to ensure that the internal audit function has technology to support the internal audit process. The chief audit executive must regularly evaluate the technology used by the internal audit function and pursue opportunities to improve effectiveness and efficiency.

When implementing new technology, the chief audit executive must implement appropriate training for internal auditors in the effective use of technological resources. The chief audit executive must collaborate with the organization's information technology and information security functions to implement technological resources properly.

The chief audit executive must communicate the impact of technology limitations on the effectiveness or efficiency of the internal audit function to the board and senior management.

Considerations for Implementation

The internal audit function should use technology to improve its effectiveness and efficiency. Examples of such technology include:

- Audit management systems.
- Governance, risk management, and control process mapping applications.
- Tools that assist with data science and analytics.
- Tools that assist with communication and collaboration.

To evaluate whether the internal audit function has technological resources to perform its responsibilities, the chief audit executive should:

- Assess the feasibility of acquiring and implementing technology-enabled enhancements across the internal audit function's processes.
- Collaborate with other departments on shared governance, risk, and control management systems.
- Present sufficiently supported technology funding requests to the board and senior management for approval.
- Develop and implement plans to introduce approved technologies. Plans should include training internal auditors and demonstrating the realized benefits to the board and senior management.
- Identify and respond to the risks that arise from technology use, including those related to information security and privacy of individual data.

Technology's Impact on Internal Audit

The Foundation's Internal Audit Vision 2035: Creating Our Future Together report offers a valuable look into the attitudes and use of technology among internal audit practitioners around the world. Research participants clearly recognize the value and importance of technology in shaping the profession's future. Indeed, this group of more than 7,000 internal audit practitioners and stakeholders from across the globe identified technology as the single driver that will have the greatest impact on internal audit in the next 10 years. This involves not only using new technology, but also understanding its associated risks and having the skills necessary to assess technology transformations.

Research participants envisioned several technology-driven changes that will contribute to internal audit's transformation, including:

- Increasing volumes of complex data to manage/analyze.
- Enhancing internal auditors' skills to remain relevant.
- Developing better insights for recommendations.
- Requiring an elevated skill set for entry level internal auditors.[2]

Further, 92% of Vision 2035 survey participants report that new technology is key to helping internal audit add more value in the future.

"According to survey respondents, who were asked to share their perspectives on AI in internal audit, AI will add value by enabling the analysis of more information and the development of more in-depth insights. With these efficiencies, the profession should anticipate a transformation in how audits are conducted in the future, along with enhanced assurance opportunities and expanded advisory services."[3]

2 "Internal Audit: Vision 2035 Creating Our Future Together," The Internal Audit Foundation, 2024.
3 Ibid

Source: The Foundation's Vision 2035 Survey. Q38. Please indicate your level of agreement with the following statements about new technology (such as AI, machine learning, and automation) and its impact on internal audit in the future. (n=6,506).

AUDITBOARD Internal Audit FOUNDATION

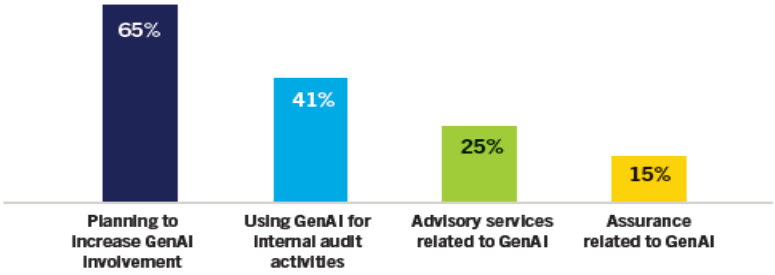
GenAI Integration

4 in 10 respondents are using GenAI for internal audit activities

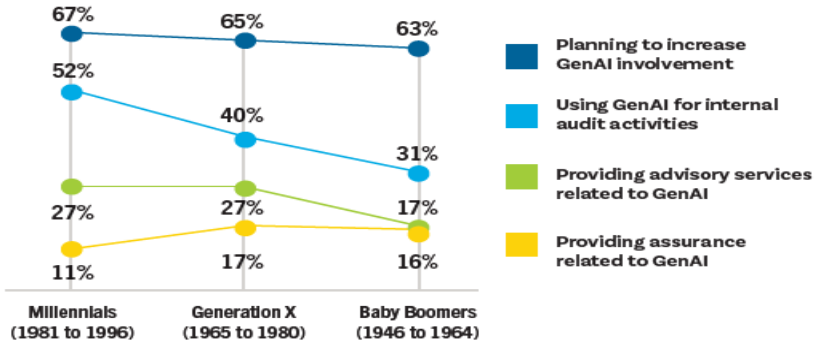
While 41% are using GenAI for internal audit activities, assurance and advisory activities are substantially lower, with 15% providing assurance for their organization's use of GenAI and 25% providing advisory services, including support for GenAI implementation.

Generational differences stand out in the use of GenAI for internal audit activities, with Millennials most active (52%), followed by Generation X (40%), and Baby Boomers (31%).

Internal Audit Involvement with GenAI



Internal Audit Involvement with GenAI (Compared to Generation)

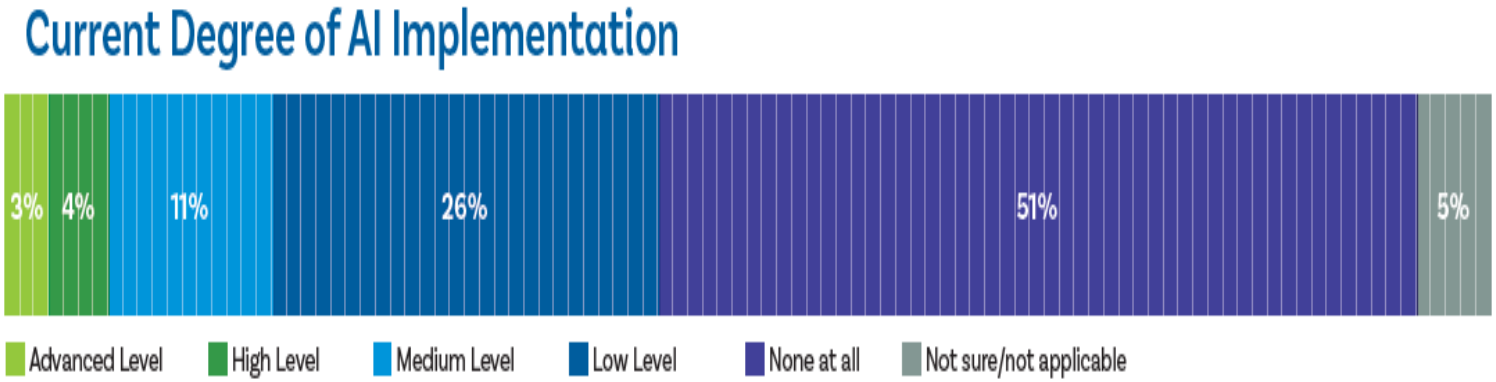


Note: The IIA's North American Pulse of Internal Audit Survey, Oct. 10 to Nov. 14, 2024. Q27: In what ways is your internal audit function involved with GenAI (generative artificial intelligence) at your organization? (Choose all that apply.) Q28: Do you plan to increase or decrease internal audit use of GenAI in the next year? Q29: Please indicate to what extent your internal audit function is using GenAI to support the following internal audit activities. *n* = 405.

IIA Foundation, Current Degree of AI Implementation and 4 Use Cases

- Internal Audit Foundation Publication ***Demystifying AI*** details 4 internal audit use cases for applying new technology:

  - Enthusiast
  - Protector
  - Explorer
  - Sage



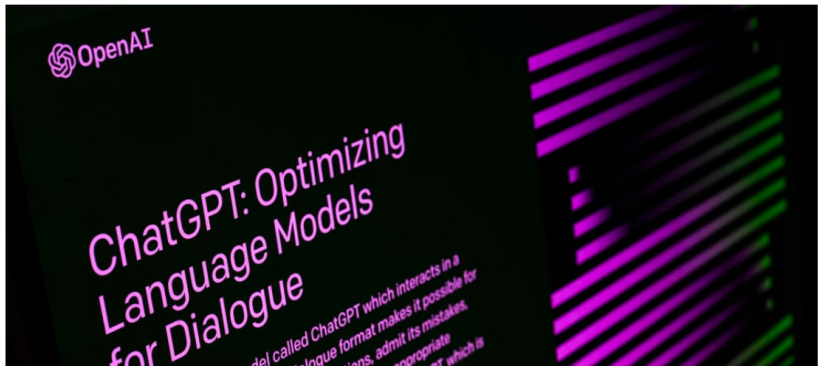
AI Governance and Environment

CULTURE & SOCIETY | ENVIRONMENT | FLORIDA GOVERNMENT | POLITICS & LAW | WORKING & THE ECONOMY

‘Age of darkness and deceit’: DeSantis proposes ‘AI bill of rights’ in crack down

Governor offers legislative proposals to regulate artificial intelligence.

BY: **LIV CAPUTO** - DECEMBER 4, 2025 1:09 PM



AI protection part of Gov. DeSantis’ legislative priorities for January session

Central Florida Public Media | By **Danielle Prieur**

Published January 5, 2026 at 4:34 PM EST

Georgia’s 2026 Tech Philosophy: ‘AI Governance Is Security’

CIO Shawnzia Thomas decodes why "cyber discipline" drives AI, modernization, and trust in Georgia’s 2026 tech agenda, and how cyber resilience is achievable through digital literacy and upskilling.

January 08, 2026 • Ashley Silver

Shawnzia Thomas Government Technology/David Kidd

As technology becomes more visible in how government works, the state of Georgia is paying closer attention to what sits behind it.

That’s because whether the topic is AI, modernization, data or workforce readiness, security is showing up early — and often — in the conversation.

In a recent interview, the state’s CIO Shawnzia Thomas, executive director of the Georgia Technology Authority (GTA), made it clear that nearly every major technology decision now hinges on this question: Is it secure enough to scale? From AI pilots to workforce development and citizen-facing services, what she calls “cyber discipline” has become the foundation for how Georgia plans to move forward in 2026.

ARTIFICIAL INTELLIGENCE

Georgia's AI Lab Cooks Up Tech Ideas in New Test Kitchen

The state’s technology department officially opened its Innovation Lab this week — a dedicated space for ethical AI experimentation aimed at advancing public service.

July 18, 2025 - Ashley Silver

An official website of the State of Georgia. How you know

gta | Office of Artificial Intelligence

Program | AI Guidance | Innovation Lab | Training

AI Guidance > Guidance for State Organizations > 5 Guiding Principles

- AI Guidance
- Guidance for State Organizations
  - 5 Guiding Principles
  - How to Properly Cite AI-Generated Content
- Guidance for Select Tools
- Ethics Framework
- Blog
- Common AI Terminology

5 Guiding Principles

To safeguard the welfare of and enhance the services provided to Georgians, GTA has established five guiding principles governing the design, implementation, and utilization of automated systems. Informed by industry research and experts, these principles are intended to guide state agencies as they integrate protective measures into their policies and operational procedures. These principles serve as a framework whenever automated systems have significant implications on the rights of Georgians or their access to essential services.

Implement Responsible Systems

- User-centered Design and Development +
- Comprehensive Testing +
- Ongoing Monitoring and Improvement +

Strengthening IG Operations with AI and the Center of Excellence Model

Center of Excellence (CoE) Model:

- Centralizes best practices, training, and innovation across agencies
- Promotes collaboration and standardization in audit and investigative functions
- Supports continuous improvement through shared expertise and resources

AI-Enabled Tools in Action:

Microsoft Copilot

- Integrated into Microsoft 365 (Word, Excel, Teams)
- Assists IG staff with drafting reports, analyzing data, summarizing findings
- Reduces time spent on repetitive tasks, enabling focus on high-risk areas
- Enhances audit documentation and investigative case management

Google Gemini

- Deployed in pilot programs across 18 state agencies
- Used for summarizing evidence, drafting communications, and automating workflows

Integrating AI & Cyber Training to Meet Evolving Oversight Demands

Why It Matters:

- Cyber threats are growing in complexity and frequency.
- Florida statutes 20.055(6)(i) and 282.318, require annual cybersecurity audits aligned with NIST and Rule 60GG-2
- AI tools and cyber training are essential to modernize IG audit and investigative functions.

Opportunities for Integration:

AI in Audit & Investigations

- Automate data analysis, risk detection, and report generation
- Use tools like Microsoft Copilot and Google Gemini to streamline workflows
- Enhance fraud detection and pattern recognition in large datasets

Cybersecurity Training

- Upskill IG staff in NIST-aligned frameworks
- Leverage micro-trainings and simulations for incident response
- Align training with Florida's Rule 60GG-2 cybersecurity standards

Strategic Benefits:

- Improves audit quality and investigative accuracy
- Builds internal capacity to meet statutory mandates
- Enhances readiness for emerging cyber risks and compliance reviews

OCIG AI Prompt Library

TITLE	TYPE	USE CASE/DEFINTION	TESTED?	PROMPT
Root Cause Analysis	Audit Work Activities	Conduct a root cause analysis of any report findings to determine the underlying root cause. (See Standard 14.3 and 14.4)	No	As part of the internal audit process and as required by Global Internal Audit Standard 14.3 and Global Internal Audit Standard 14.4, internal auditors are required to conduct a root cause analysis of any issues, findings, or deficiencies identified during the audit and determine the underlying roo cases. Utilizing established root cause analysis methodologies and the attached relevant audit finding, I would like to systemically investigate the identified issues. I would like to identify the fundamental reasons for the issues, analyze contributing factors, and provide insights into the root cause to enable the development of well-crafted and effective internal audit recommendations and corrective actions. This analysis should aim to uncover the underlying reasons for the identified deficiency and support the implementation of targeted solutions and recommendations to address these issues.
Developing Scoping Questions and Risk Hyphotheses	Audit Planning	Draft risk hyphotheses for a auit.	No	Act as an experienced, internal audit. We are planning an audit of XX. Suggest a list of potential inherent risks, relevant regulations, and 10 preliminary survey scoping questions to help define the audit scope.
Interview and Walkthrough Prep	Preliminary Survey Activities	Prep internal audit stadd for walkthrough and provide depth of inquiry and more confidence in client interactions.	No	I am interviewing the XXX to validate controls with respect to XXX. Generate a list of 10 open-ended questions that assess system access, exception handling, and fraud risk.
Summarizing Audit Evidence	Audit Fieldwork Analysis	Digest complex control test results and help the senior auditor draft initial audit findings	No	Summarize the following testing evidence across the relevant internal control activities. Highlight recurring deficiences, trends, and any compliance implications. I would like the output to be provided in bullet points suitable for a working paper.
Drafting Audit Findings and Recommendations	Report Drafting	Providing a consistent tone and structure that aligns with the company's reporting standards.	No	Draft a management-level audit finding for the following issue: XXX. Include condition, root cause, impact, and recommendation. Use professional and neutral language, appropriate for reporting to senior management.
				I'm planning to [decision/plan] because [reasoning] and with a goal of [objective]. Play

Executive Office of the Governor
Office of the Chief Inspector General

Thank you!

Steven Henry, Director of Auditing

(850) 717-9264