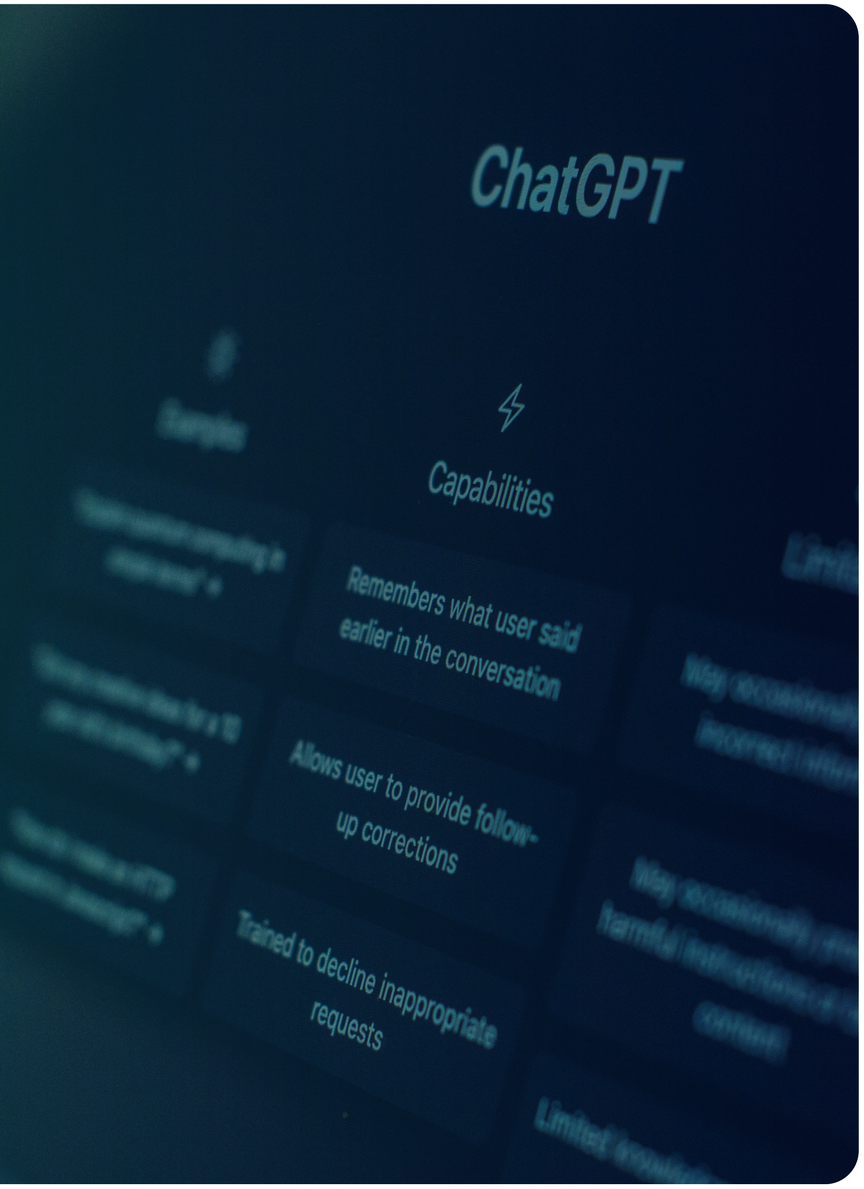
PONDURANCE



Navigating the AI Frontier

Strategy, Security & Compliance



PONDURANCE

TABLE OF CONTENTS

Chapter 1: Explore Your AI Options and Weigh Risk With a Phased Approach 3

Chapter 2: Ensuring Cyber Resilience in the Age of AI 8

Chapter 3: Maintaining Regulatory Compliance in the Gen AI World 16

©2025 Pondurance LLC. All Rights Reserved.

CHAPTER 1:

Explore Your AI Options and Weigh Risk With a Phased Approach

Artificial intelligence (AI) solutions are being rapidly adopted by U.S. businesses, including midmarket organizations, across a wide range of industries. As much as 78% of respondents in the March 2025 McKinsey survey reported that their organizations use AI in at least one business function, up from 55% in 2023.

AI tools provide attractive business opportunities, such as productivity gains, improved content for marketing and sales, and faster customer service, and there are plenty of options for organizations to choose from. Employees are eager to test the performance of AI tools, often before organizations have had a chance to fully implement best practices, draft new policies, and address regulatory compliance issues.

So how do organizations explore the many AI options available and still stay safe from risk? It's a balancing act. Pondurance suggests that midmarket organizations explore the benefits of the AI tools on the market, weigh the risks of using them, and take a phased approach to AI adoption.

78%

of respondents eported that their organizations use AI in at least one business function.

Source: *McKinsey Survey*

©2025 Pondurance LLC. All Rights Reserved.



PONDURANCE

Exploring AI solutions

The AI revolution is here, and global spending on AI, including applications, infrastructure, and services, is expected to more than double over the next few years, reaching $632 billion by 2028. Organizations in every industry know they need to determine how AI can drive efficiencies for their businesses to avoid falling behind. However, there are abundant AI technologies on the market, and choosing the AI tools that work best for your midmarket organization can seem overwhelming.

As a first step in considering how AI can help your organization, you can conduct an in-depth analysis of your workflow to identify the pain points for your business. Then contemplate how AI can possibly address those pain points to move you closer to your overall business goals. Also think about how the tools will work within your unique organization. Ask yourself: *How do the tools integrate with my existing technology and workflows? Can the tools grow as the business grows? Can the technology handle and process my data? What are the costs to set up, use, and maintain the tools?*

©2025 Pondurance LLC. All Rights Reserved.



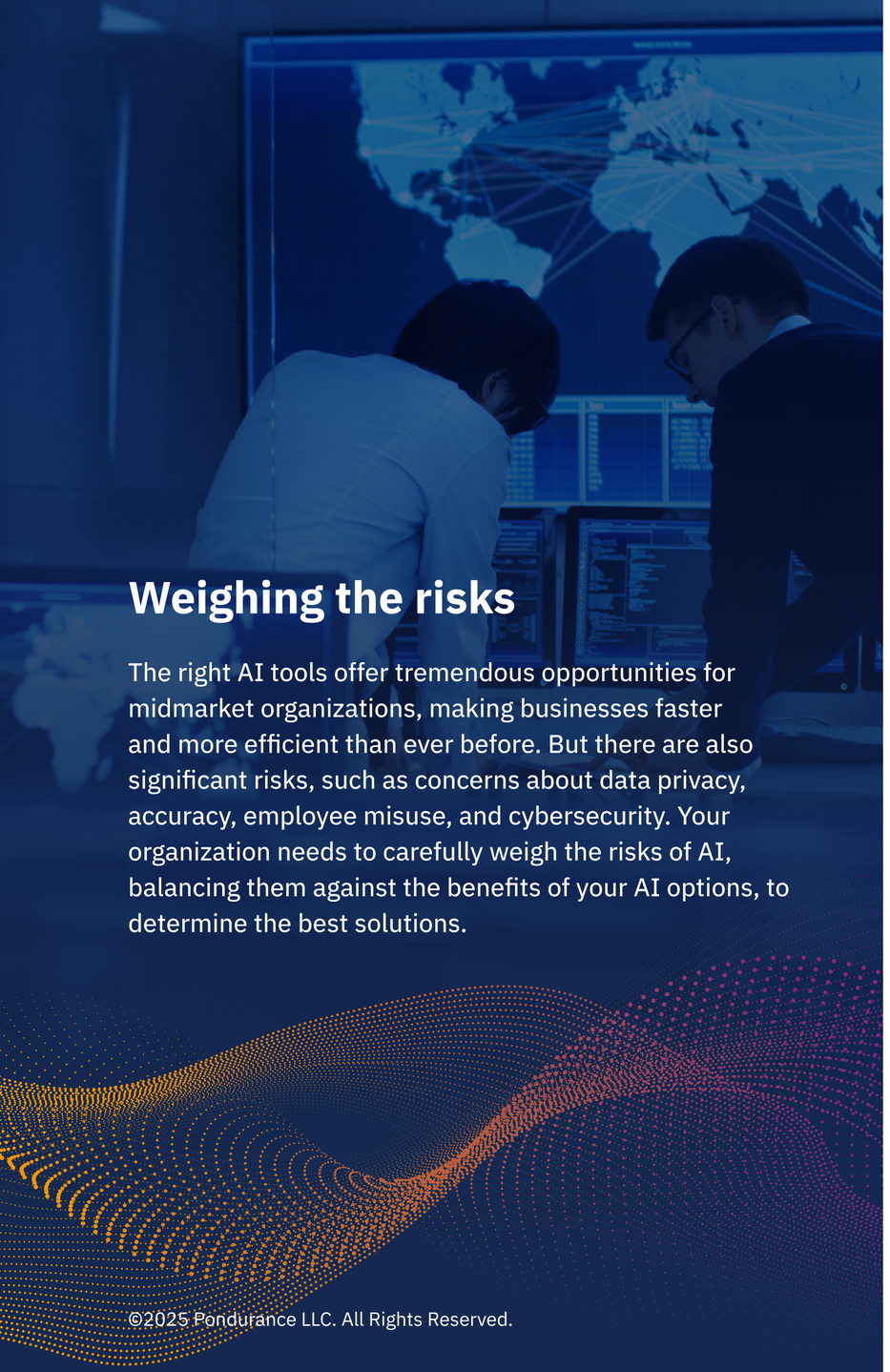
PONDURANCE

You'll want to consider every department in your analysis, not just IT. AI solutions can address pain points for teams across your organization, and it's important that you explore your options.

- **Marketing.** Content generation tools, such as Microsoft Copilot and Jasper, use text prompts to generate drafts of written content for emails, blogs, and creative inspiration. AI solutions can also check grammar, edit videos, generate images, manage social media posts, and create presentations.
- **Sales.** AI tools can help your sales team identify customer trends, generate predictive analytics to anticipate customer needs, recognize upselling and cross-selling opportunities, write better emails, and generate leads.
- **Customer service.** Chatbots, such as ChatGPT and Claude, allow your business to communicate with customers in real time to improve their online experiences. Many AI solutions can also retrieve data analytics from emails, logs, social media posts, and product reviews.
- **Human resources.** AI tools can assist in recruiting candidates, onboarding, managing employee records and benefits, and upskilling workers to effectively use AI.
- **Cybersecurity.** AI can proactively help teams with enhanced security monitoring, authentication, threat detection, and incident response. However, AI also can pose security risks as it adds to the organization's attack surface.
- **Finance.** Teams can use AI tools to detect fraud, automate compliance checks, assist with budgeting, analyze data, and more.

Before letting employees experiment with these AI options, your organization should consider executing a pilot program where teams can safely use the AI tools in a controlled setting. Your organization can gather information from the pilot program teams and use their keen insights to narrow down the options that best address your pain points and further your business goals.

©2025 Pondurance LLC. All Rights Reserved.



Weighing the risks

The right AI tools offer tremendous opportunities for midmarket organizations, making businesses faster and more efficient than ever before. But there are also significant risks, such as concerns about data privacy, accuracy, employee misuse, and cybersecurity. Your organization needs to carefully weigh the risks of AI, balancing them against the benefits of your AI options, to determine the best solutions.

©2025 Pondurance LLC. All Rights Reserved.

PONDURANCE

Data privacy. AI tools collect and analyze large amounts of data to train algorithms, make predictions, and improve performance. Businesses need to safeguard the data from threat actors (or even unwitting employees) to protect intellectual property and avoid data leaks that can cause ethical or reputational damage. In addition, organizations in regulated industries must protect their sensitive customer data to meet the compliance requirements of federal and state privacy laws.

Accuracy. AI tools are designed to provide a correct answer to prompts. Unfortunately, when AI doesn't know the answer, it may invent one, known as an AI hallucination. For example, Microsoft's Bing AI Chat provided inaccurate figures about a Gap earnings report and Lululemon financial data. Also, ChatGPT fabricated six court cases for two attorneys to use as legal precedents in a brief submitted to a judge, and the judge subsequently fined the attorneys for using the fake citations. AI tools always require human oversight. Employees should verify all information generated by AI tools to confirm accuracy.

Employee misuse. Sharing sensitive company or customer information on AI systems can create serious confidentiality issues, data privacy violations, and exposure of company trade secrets. The risk is real. In a recent survey, 47% of employees reported they have uploaded sensitive information into public AI tools, and 44% admits using AI at work in violation of company policies. Organizations need to set up safeguards, conduct ongoing training, and create safe workplace cultures to mitigate the risks.

Cybersecurity. AI technology can detect patterns in your network traffic for a quicker response to cyber threats. But AI tools also expand the attack surface and provide new vulnerabilities for threat actors to exploit. In addition, threat actors are using their own AI tools to generate deepfakes, execute phishing scams, and create malware that is more convincing than victims have seen in prior attempts.

Using a phased approach

Once you've decided which AI solutions work best for your organization, you need to figure out how to implement them — and that implementation requires considerable preparation and planning. Your organization needs to determine the process or approach for the rollout, the usage policy, employee training, risk management, and many other important decisions.

Phased approach. For most midmarket organizations, Pondurance recommends using a phased approach to AI adoption. In a phased approach, your organization takes small steps to implement AI, focusing on your pain points and business objectives in determining the phases. Your organization may want to start with the AI solutions that make the biggest impact for your employees but have a low level of risk, such as onboarding new talent, generating sales leads, or creating content for a new website. Or your team may have a high-risk priority that AI tools can address, and you want to tackle that first. No matter how you do it, the important thing is to concentrate only on specific areas or functions at a time — always with risk in mind — and set clear time frames to keep the process on schedule and on budget.

Usage policy. For cybersecurity, your organization most likely compiled a comprehensive incident response plan. A similar plan is critical for AI, getting all employees and stakeholders on the same page. With the fast pace of AI adoption, your organization may not have the opportunity to draft a thorough usage policy before adopting AI. But at a minimum, your organization needs to specify the roles and tasks for using AI, the ongoing monitoring and auditing required, the training and awareness programs needed, and the controls and assessments required to protect sensitive customer data and company secrets.

Employee training. AI tools are meant to help humans rather than replace them, so your organization should clearly communicate the positive benefits of AI to your employees. Your organization should offer ongoing training to every employee, teaching them how to responsibly use AI tools and stay current on the risks of AI. Your organization will also want to upskill employees, or prepare them for job changes as AI performs mundane tasks while employee work becomes more strategic.

Risk management. The phased approach allows your midmarket organization to consider risk at every stage — and there are plenty of risks. Employees can misuse AI tools, resulting in the public release of confidential information or intellectual property, the use of false AI-generated information in content, or the exposure of sensitive customer data in violation of compliance laws. Threat actors pose a risk as AI expands the attack surface, leaving your network vulnerable to exploit, and they also use AI tools for deepfakes, phishing attacks, and social engineering scams. For all these reasons, it's important to build in periodic risk monitoring and assessments during your AI launch period and after AI has become the norm to keep your organization safe and protected.

CONCLUSION

AI tools can provide productivity gains and efficiencies for your midmarket organization, but your teams must do the hard work of exploring the options, weighing the risks, and implementing AI with a phased approach. It takes preparation and planning. When you do it right, AI solutions can ease your pain points and align with your business goals to get your business running more productively and efficiently with reduced risk.

©2025 Pondurance LLC. All Rights Reserved.



90%

of organizations are using or exploring the use of AI

Source: *Cybersecurity Information Sheet*

PONDURANCE

CHAPTER 2:

Ensuring Cyber Resilience in the Age of AI

Midmarket organizations are quickly adopting generative artificial intelligence (gen AI) tools to improve efficiency and enhance quality. Whether the need is content generation, well-written sales emails, improved online customer service, more efficient onboarding of new employees, or research for new technical and business initiatives, AI can help. Today, more than 90% of organizations are using or exploring the use of AI, and 92% of organizations intend to increase their AI investments over the next three years, according to Exploding Topics.

With gen AI use in the early stages for most organizations, concerns about data security and client privacy are widespread. Organizations in every industry want to know how to ensure data privacy and integrity when using AI tools. Pondurance suggests that all organizations use best practices from the Cybersecurity Information Sheet (CSI) as the 10 steps for how to secure data used to train and operate AI systems. The CSI was developed by the U.S. National Security Agency's Artificial Intelligence Security Center, the Cybersecurity & Infrastructure Security Agency, the FBI, and several non-U.S. security agencies.

©2025 Pondurance LLC. All Rights Reserved.



The Pondurance team encourages everyone to read the entire CSI, and this article will briefly discuss the 10 steps to jump-start your efforts to ensure cybersecurity and data privacy in the emerging AI world. Throughout these steps, the term “AI” will be used to include gen AI, agentic AI, and traditional AI tools and systems.

1. Source reliable data and track data provenance

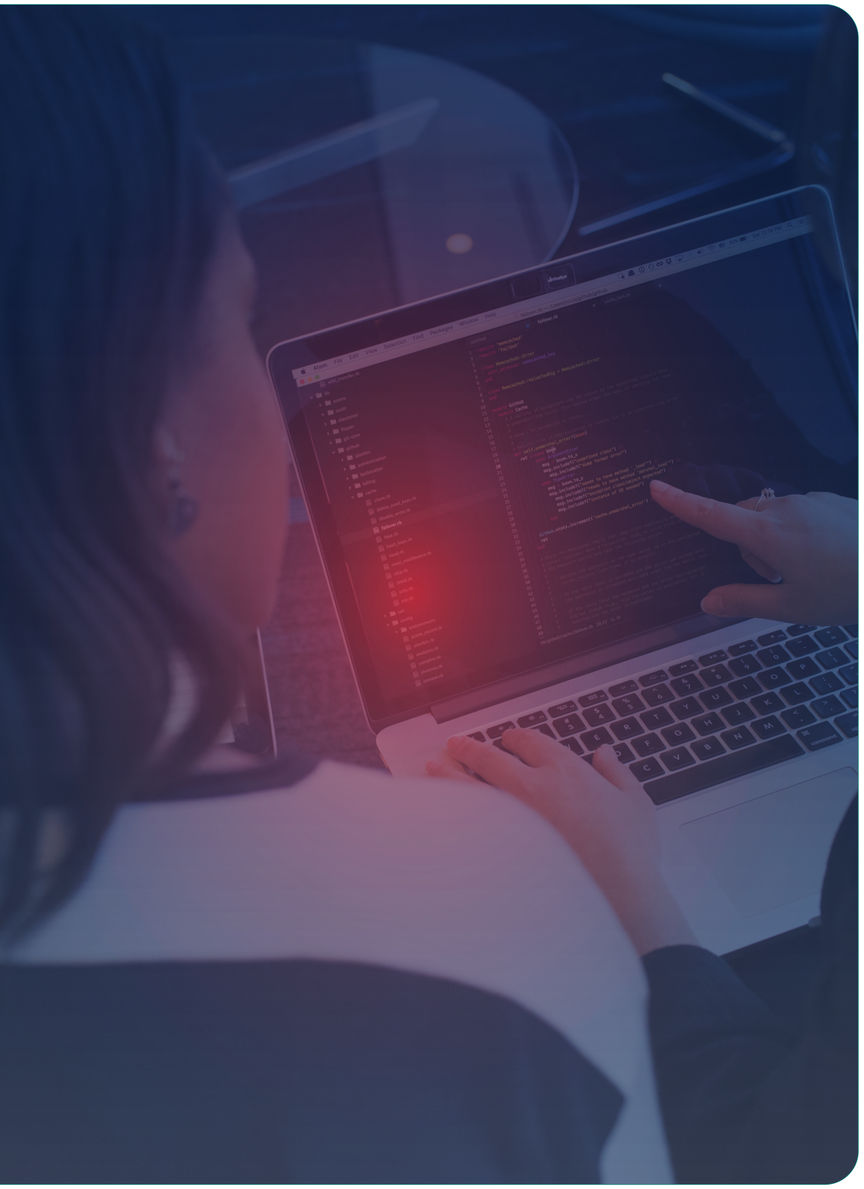
AI algorithms require an abundance of reliable data, so where your organization gets its data and the quality of that data are important. Quality in, quality out. Your organization can use in-house data only, third-party data providers, public databases, web scraping, crowdsourcing, or data marketplaces to source your data. But no matter how the data is obtained, it must be verified as trusted, reliable, and accurate data from an authoritative source.

To ensure the reliability of the data, your organization needs to track the data provenance, or the origin and history of the data, using metadata. Data provenance tells your team where the data came from, how it was created, who created it, and any updates or changes that have been made to it. Best practices also suggest that the database should be cryptographically signed and should include an unchangeable, append-only ledger so that no one can manipulate the data without detection.

2. Verify and maintain data integrity

Once your organization has sourced accurate, reliable, and trustworthy AI data, the data’s integrity must be maintained over time. The data must remain in its original state with no unauthorized modifications during storage and transport. To ensure data integrity, your team should use checksums — small blocks of data derived from other blocks of data to detect errors introduced during storage and transport — and cryptographic hashes to verify that the data has not been altered.

©2025 Pondurance LLC. All Rights Reserved.



3. Use digital signatures

Using digital signatures is another way to ensure data integrity. In particular, your organization should require quantum-resistant digital signatures for data used during AI model training, alignment, fine-tuning, and reinforcement learning from human feedback. Quantum-resistant digital signatures use cryptographic algorithms that are designed to stay protected into the future because the algorithms are based on mathematical problems that even a quantum computer cannot easily crack. Cryptographic signatures should be used on all original versions, and any later modifications should be signed by the individual making the changes.

In addition, your organization should use trusted certificate authorities throughout the verification process. These entities validate the digital identity of websites, email addresses, organizations, and individuals and issue digital certificates to prove authenticity.

4. Leverage trusted infrastructure

The use of AI can add vulnerability to your network. For added protection, your organization should leverage zero-trust architecture to keep sensitive data safe and unaltered. This security framework is based on three principles: verify, use least privilege access, and assume a breach. With zero-trust architecture, your team must always assume a breach is imminent and verify every request as if it were a potential threat. The “never trust, always verify” approach reinforces data integrity processes and reduces risk to data for a more capable, transparent AI system.

©2025 Pondurance LLC. All Rights Reserved.



5. Classify data and use access controls

Data classification helps organizations identify and categorize data to apply proper security measures, such as stringent encryption and access controls, to different types of data. Classifying data can help your organization better understand what type of data it has, how sensitive the data is, and who should have access to it. Overall, the input data and output of AI systems should be classified at the same level.

Best practices suggest that organizations classify data based on sensitivity and protection requirements. Safeguarding sensitive data is required for compliance with federal and state privacy laws. Sensitive information can include:

- Personally identifiable information - names, addresses, and social security numbers
- Protected health information - medical records, health insurance information, and patient histories
- Financial data - credit card numbers, bank account numbers, credit histories, and tax information
- Intellectual property - trade secrets, patents, and copyrights
- Biometrics - fingerprints, voiceprints, facial recognition data, and retinal scans

6. Encrypt data

To secure data at rest, in transit, and during processing, your organization should implement advanced encryption protocols that are comparable to your overall data protection level. Advanced Encryption Standard with a 256-bit key (AES-256) is the industry gold standard for securing data, as its number of possible key combinations makes it nearly impenetrable in a brute force attack. In particular, as a best practice for securing data in transit, your team should use protocols such as transport layer security, a cryptographic protocol used to provide security to applications transmitting data over a network, along with AES-256 or postquantum encryption.

©2025 Pondurance LLC. All Rights Reserved.



7. Securely store data

When your organization stores sensitive data for AI, it must be secured in certified storage devices that enforce National Institute of Standards and Technology (NIST) compliance to provide a high level of security against an attack. This data storage requirement covers areas related to the design and implementation of the cryptographic module, which is the hardware and software that support security functions.

Four levels of storage are defined in the NIST standards. Best practices single out Level 3 for robust protection but acknowledge that the security level should be based on an organization's needs and risk assessments.

- **Level 1** – Offers basic security that does not require specific physical security mechanisms and allows the cryptographic module to be executed on an unevaluated operating system.
- **Level 2** – Adds a requirement for tamper evidence, such as coatings, seals, or pick-resistance locks, and requires role-based authentication.
- **Level 3** – Requires physical security mechanisms that provide a high probability of detection and response if a threat actor attempts to access the cryptographic module. This level includes identity-based authentication and requires that organizations perform the entry or output of plaintext critical security parameters using physically separated ports or interfaces.
- **Level 4** – Provides complete protection of the cryptographic module to detect and respond to all unauthorized attempts for access.

©2025 Pondurance LLC. All Rights Reserved.

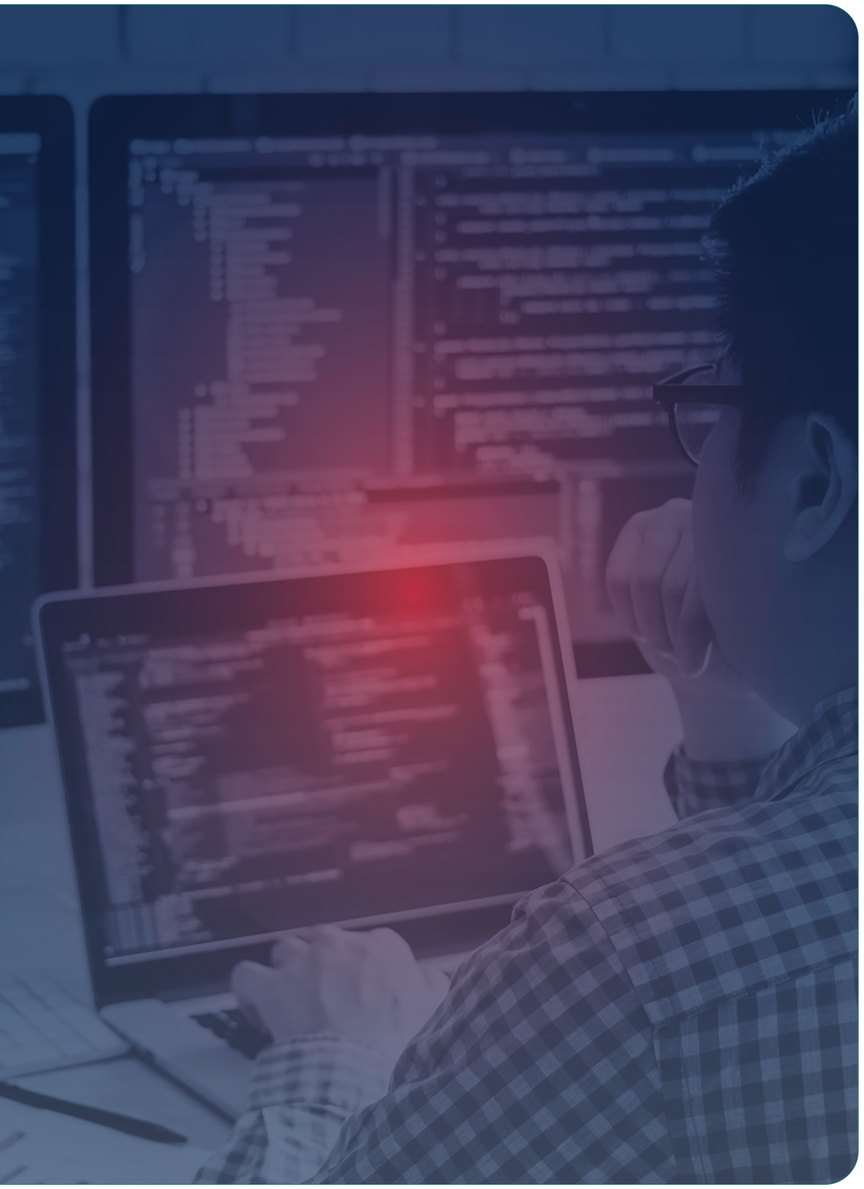


8. Leverage privacy-preserving techniques

AI data privacy can ensure compliance, reduce legal risks, and build trust with clients. Your organization can leverage privacy-preserving techniques to increase data security. Best practices list three specific techniques to consider:

- Data depersonalization techniques, such as data masking, are processes where sensitive data is replaced or altered with plausible but false data to protect the sensitive data while AI tools use it for training, testing, and analysis. For instance, customer names can be replaced with fake names or date fields can be altered by adding or subtracting a random number of days. Best practices specifically recommend using data masking during AI model training and development to safeguard sensitive data.
- Differential privacy is a quantifiable way to balance privacy and usefulness in a dataset. The technique adds random noise to the data before storing it in the AI system, making it difficult for threat actors to identify individual data points within the data. Differential privacy allows organizations to analyze and transfer data while still protecting sensitive data and maintaining compliance with privacy laws.
- Decentralized learning techniques, such as federated learning, allow multiple local devices to train a single shared AI model without directly sharing their own data. Instead, only the AI model updates are centrally aggregated. This machine learning approach ensures data privacy and security because the sensitive data never leaves the local devices. Best practices recommend using secure multiparty computation for training and inferencing processes.

©2025 Pondurance LLC. All Rights Reserved.

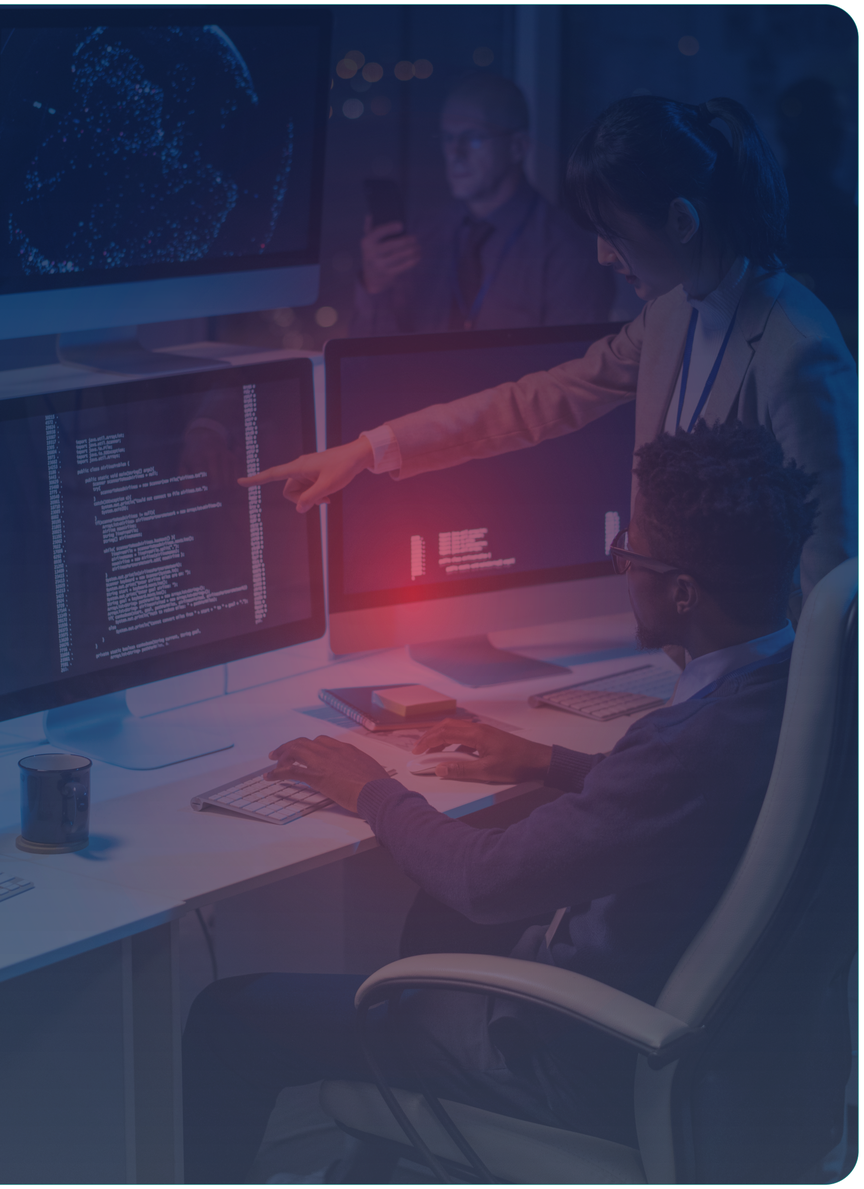


9. Securely delete data

Organizations must maintain appropriate controls over their AI data even when deleting it. Before disposing of data or reusing drives used for AI data storage, your organization should erase the existing data using a secure deletion method. Best practices note three secure deletion methods:

- **Cryptographic erase**. This method sanitizes the cryptographic keys that encrypt the data, leaving only the ciphertext on the storage device. With the encryption ability gone, the remaining encrypted data is unrecoverable. Cryptographic erase is fast and highly reliable for deletion of data, but it should only be used for data that was encrypted on the device prior to storage.
- **Block erase**. This deletion method erases a block of data by applying a high voltage level to all NAND cells on a solid-state drive or by using device-specific commands to wipe a flash memory device.
- **Data overwrite**. This method replaces the existing data on a storage device by writing over it with insignificant data or patterns. The process is time-consuming as it requires multiple passes to assure that the sensitive data is no longer recoverable.

©2025 Pondurance LLC. All Rights Reserved.



PONDURANCE

10. Conduct risk assessments

Before using AI, organizations need to understand the risks of the technology, including AI hallucinations, bias, denial-of-service attacks, privacy and data security risks, and compliance violations. A risk assessment enables your organization to evaluate your cyber landscape, identify potential risks and vulnerabilities, and prioritize the actions needed to keep your data safe while using AI. Assessments must be ongoing and adhere to industry-standard frameworks to help your organization continuously improve its data security measures. Pondurance recommends that every organization conduct a risk assessment to evaluate changes to the network due to the adoption of AI tools.

CONCLUSION

Midmarket organizations in every industry are adopting gen AI tools and exploring the use of agentic AI, and concerns about data integrity, data privacy, and data security are commonly part of the transition. Fortunately, AI best practices from the CSI are available to help organizations take the necessary steps to keep data unaltered, private, and secure. Managed detection and response solutions like the one provided by Pondurance are working hard to stay ahead of the associated threats of using AI.

©2025 Pondurance LLC. All Rights Reserved.

CHAPTER 3:

Maintaining Regulatory Compliance in the Gen AI World

Generative artificial intelligence (gen AI) uses deep learning models and large datasets to recognize patterns within the data and learn from them. Once a gen AI tool is trained, it can create new data, similar to the data it was trained on, to generate content such as text, images, designs, music, and computer codes. As much as 91% of midmarket organizations use AI in their business practices, according to RSM Middle Market AI Survey 2025. That's a marked increase from 78% reported in 2024.

With such rapid adoption of gen AI, midmarket organizations are legitimately concerned about balancing the innovation benefits of gen AI and the potential risks that come with its use. Data privacy, security, and integrity top the list of concerns and are a primary focus for regulatory compliance. Keeping data safe can help organizations build trust with customers, sustain a good company reputation, and avoid costly penalties from compliance violations.

Organizations can take a few substantial steps toward achieving gen AI compliance by knowing the applicable laws, making a written plan, monitoring and conducting risk assessments, and providing training to all employees.



©2025 Pondurance LLC. All Rights Reserved.

Know the law

Organizations have had to follow cybersecurity rules to stay in compliance, and adding gen AI rules heightens the risk of possible compliance violations. Staying in compliance means following all state, federal, and even international laws that may apply.

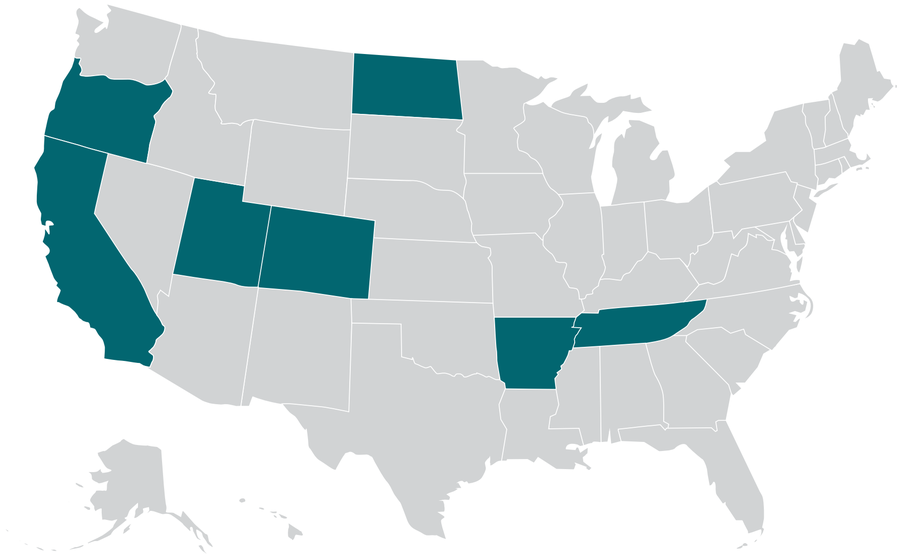
Currently, there's no overarching federal law that regulates gen AI for U.S. companies. In a January 2025 executive order, President Donald Trump revoked "existing AI policies and directives that act as barriers to American AI innovation." Then, in the One Big Beautiful Bill, the Trump administration attempted to place a 10-year moratorium on state governments' abilities to enforce and enact legislation on AI; however, the moratorium provision was removed by the Senate prior to passage. Proponents of the moratorium argued that the restriction would keep states from passing a mishmash of rules that would discourage AI innovation, while those in opposition to the moratorium argued that AI technology needs rules in place to ensure fairness and protect citizens from possible misuse.



©2025 Pondurance LLC. All Rights Reserved.

All 50 states introduced legislation on AI in 2025, and as of July, 38 states have adopted or enacted laws covering a wide range of AI topics. A few examples of new and existing AI legislation for various states include:

- **Arkansas.** The statute sets out who owns AI-generated content and makes clear that the content cannot violate intellectual property rights or copyrights.
- **California.** The law requires a disclosure when election-related advertisements use AI-generated content, and a separate law requires AI services with over 1 million users to disclose AI-generated content.
- **Colorado.** The statute requires developers and deployers of high-risk AI systems to use reasonable care to protect against algorithmic bias and disclose the use of AI to customers.
- **North Dakota.** The legislation expands existing law, mandating that an individual must not use an AI robot to stalk or harass.
- **Oregon.** The law mandates that a nonhuman, including an AI robot, is prohibited from using the title "nurse."
- **Tennessee.** The Ensuring Likeness, Voice, and Image Security Act, known as the ELVIS Act, prohibits the use of gen AI to mimic the voice of a songwriter, performer, or celebrity without the individual's permission.
- **Utah.** The legislation mandates that a mental health chatbot must disclose to the user that it is not a human being but is gen AI technology.



The diverse collection of state gen AI regulations poses a challenge for organizations doing business in all or multiple states across the country. Organizations should become familiar with the enacted and pending AI laws in the 50 states — or whatever states they do business in — to make sure they are in compliance. In addition, organizations that conduct business globally should comply with the European Union AI Act and other regulatory measures drafted or enacted in countries such as China, Japan, Singapore, India, and Brazil.

©2025 Pondurance LLC. All Rights Reserved.



Make a written plan

For years, midmarket organizations have implemented incident response plans for cybersecurity — and written plans for gen AI are just as important, particularly for regulated industries like healthcare and financial services. Only 43% of organizations are currently developing ethical AI guidelines aligned with regulations, according to RSM Middle Market AI Survey 2025. The need for such plans may rise as future legal battles over gen AI increase in number and more companies adopt gen AI tools.

The provisions needed in a written plan depend on the company size, which gen AI tools are implemented, how the gen AI tools are used, and other company-specific considerations. In general, a few crucial topics to consider in a written plan are:

- Proper uses for gen AI. Organizations need to define when employees should use gen AI and when it should be prohibited. The plan's rules should define who can use gen AI, under what conditions, and for what purposes.
- Data privacy. Gen AI tools collect and analyze large amounts of data, including sensitive and confidential information, to train algorithms, make predictions, and improve performance. Organizations need to protect the data from possible employee misuse, threat actor exploits, intellectual property infringement, and data leaks that can lead to consumer privacy violations and cause ethical or reputational damage to the company.
- Verification of data. AI tools require human oversight, and employees should regularly verify all information generated by AI tools to confirm accuracy, remove bias, ensure privacy, and protect intellectual property rights. The plan should provide a clear understanding of when corrective action is needed.
- AI use disclosure. Some state laws now require that AI-generated output must be disclosed, and experts agree. In a 2024 MIT Sloan Management Review survey, 84% of participants either agreed or strongly agreed that organizations should make disclosures about AI use in their consumer products and offerings. The plan should spell out any mandatory AI use disclosure language and requirements.

©2025 Pondurance LLC. All Rights Reserved.

Monitor and conduct risk assessments

Midmarket organizations must understand the possible compliance risks of using gen AI technology, including privacy and data security breaches, exposure of confidential information and trade secrets, and exploitation by bad actors. The organization's cybersecurity team or provider should constantly monitor the environment to protect against threats and conduct a risk assessment on an annual basis and whenever the organization adds a new gen AI tool to the network.

A risk assessment enables an organization to assess the cyber landscape, identify potential risks and vulnerabilities, and prioritize the actions needed to stay safe while using gen AI. A written plan should provide provisions for ongoing monitoring and scheduled risk assessments to evaluate and protect the network.



©2025 Pondurance LLC. All Rights Reserved.



©2025 Pondurance LLC. All Rights Reserved.

PONDURANCE

Provide training

A single employee using a gen AI tool can be the epicenter for a regulatory compliance violation. Employee misuse, such as sharing sensitive customer information using gen AI tools, can create data privacy breaches and confidentiality issues. Also, the use of gen AI tools, such as ChatGPT or Microsoft Copilot, is making phishing emails harder for employees to detect primarily due to more convincing language and correct grammar.

To reduce the risk of a compliance violation, midmarket organizations should provide user awareness training to all employees. Currently, 45% of organizations are training employees on compliance requirements to reinforce the safe, ethical, and responsible use of gen AI, according to RSM Middle Market AI Survey 2025. Ongoing training can reduce risk as employees learn how to properly use gen AI tools and stay up to date on the evolving risks of their use. Organizations should designate a specific contact person who employees can report to and should outline the reporting process for any possible gen AI-related compliance issues.

CONCLUSION

The fast adoption of gen AI has left midmarket organizations concerned about balancing innovation and the potential risks of gen AI. But knowing the laws, making a written plan, monitoring and conducting risk assessments, and providing training to employees can be the basic steps an organization needs to stay compliant.