

# "AI Risks, Opportunities and Threats to Medium Enterprises in the Generative AI Era (2026)"

**Dr. Deepshikha Porwal,**

Assistant Professor, Faculty of Commerce,

Department of Business Administration, Manikya Lal Verma Shramjeevi College, Udaipur, Rajasthan,

Email id: -deepshikha41292@gmail.com

## ABSTRACT

Small and medium-sized businesses can benefit greatly from generative AI, which can help them work more efficiently innovate and compete with bigger companies. However generative AI also brings risks, such as cyber attacks and data breaches which can be a challenge for small businesses with limited resources. This study looks at how AI affects small and medium-sized businesses through case studies, trends and threat modeling. We found that generative AI can increase productivity by up to 40% in areas like retail and manufacturing. On the hand 39.7% of AI interactions can lead to threats like deep fake attacks and sensitive data exposure.

Reports on AI adoption and cybercrime in India show that small businesses face threats like model poisoning and job displacement. To solve these problems we suggest using a mix of human and AI governance, affordable cloud-based tools and training programs. Our findings support creating frameworks that emphasize AI use, ethical checks and partnerships, between public and private sectors. This can help small businesses take advantage of AI while minimizing risks.

**Keywords:-** Artificial Intelligence, Generative AI, SMEs, Small and Medium Enterprises, AI Risks, Cybersecurity Threats, Opportunities, Ethical Challenges, Productivity Gains, Regulatory Compliance, Data Breaches, Algorithmic Bias, Adoption Barriers, Mitigation Strategies, AI Governance.

## INTRODUCTION

In 2026 AI has become a part of many industries. Tools like language models, image generators and code makers are now used everywhere. They help with things like marketing and managing supply chains. For sized businesses, which have 50 to 250 employees and make between \$10 and \$50 million this is a critical time. They can use AI to innovate work efficiently and stay competitive.. They also face risks that could hurt their operations or market position. Medium businesses can really benefit from AI. They are not as big as tech giants. They can move quickly. AI can help them do things that only big companies could do before. For example AI chatbots can answer customer questions faster. AI can also help predict what customers will want to buy.. There are also downsides. AI can be used to make videos and steal ideas. It can also replace some jobs. And there are rules, like the EU AI Act that businesses must follow. This report looks at the risks and opportunities of AI, for sized businesses. It uses real-life examples and trends to help leaders make decisions about AI. The goal is to help businesses use AI to succeed while avoiding its dangers.

## BACKGROUND OF GENERATIVE AI IN 2026

By the year 2026 Generative AI has become a part of our digital world. It is a type of intelligence that creates new things like text, images and videos. Generative AI does this by learning from amounts of data. It does not just look at the data it uses it to create things. This is different from artificial intelligence, which mostly tries to predict things or automate tasks. Generative AI is all about being creative and making things when we need them. This is why it is a driver of innovation in many industries.

## **TECHNICAL. ADOPTION**

In 2026 we see that big language models, multimodal models and code generation tools are used a lot in software applications. These tools are used in office software, design platforms and development tools. They are trained on a lot of private data and use special architectures to produce things that look like they were made by humans. This allows us to use them for things like chatbots creating content and designing things. As a result big companies use Generative AI tools. Many sized companies are also starting to use them to improve the way they work and to make their customers happier.

## **TRENDS SHAPING THE 2026 LANDSCAPE**

Some of the trends in 2026 include using Generative AI to handle many types of data like text, images, voice and video. We also see artificial intelligence agents that can do many tasks on their own. Another trend is using Generative AI to make things very personal for each person in marketing, education and customer service. At the time Generative AI is automating many routine tasks like writing emails making reports and creating marketing materials. However this is also raising concerns about information, fake videos, ownership of ideas and how it will affect peoples jobs.

## **BUSINESS CONTEXT**

Because Generative AI is spreading so fast governments and regulators are making rules to ensure it is used responsibly and in a transparent way. For sized companies Generative AI is a powerful tool that can help them be more productive. However it also comes with risks to their reputation, legal issues and operational problems. This means they need to be careful about how they use it and make sure they have the skills and policies, in place to use Generative AI in a responsible way. This is the context in which we will look at how sized businesses can use Generative AI to their advantage while managing the risks that come with it in 2026.

## **LITERATURE REVIEW:**

### **THE EVOLUTION OF GENERATIVE AI TECHNOLOGIES**

This review looks at how generative AI has changed over time. It started with experimental models and will become a technology used by many businesses by 2026. We focus on models and how medium-sized businesses are using them. Generative AI can now do more than just create text or images. It can create multimodal and context-aware systems. These systems are used in business tools. Examples include office software helpers and AI-driven design and code assistants.

### **KEY MODELS IN GENERATIVE AI**

Large Language Models such as like GPT-5 from OpenAI are a step forward. They can reason, code. Understand different types of data. This makes it easier to use language to do complex tasks. Other Models There are also models like Claude Sonnet 4. These models are designed to be reliable and safe for businesses. They are used for tasks.

In the visual-content domain, diffusion-based models such as Stable Diffusion 4 and similar successors have become central to design, marketing, and product-development pipelines, allowing medium enterprises to generate logos, mockups, and visual assets with minimal in-house design capacity. These models are often embedded in SaaS platforms (e.g., Canva-style tools) or delivered via APIs, making them accessible even to organizations without AI research teams.

### **ADOPTION TRENDS IN SMES (2023–2026)**

From 2023 onward, generative AI adoption in small and medium-sized enterprises (SMEs) has grown rapidly, driven by off-the-shelf tools like ChatGPT-based copilots, AI-powered CRM features, and marketing-content generators.

International surveys indicate that well over half of SMEs that have experimented with generative AI now use it for writing support, customer-service automation, and basic analytics, helping them compensate for skill gaps and constrained budgets.

However, the literature also highlights uneven adoption: many SMEs still pilot AI via single-department initiatives (often marketing or sales) without firm-wide governance, proper measurement, or robust risk policies. This pattern suggests that while generative AI offers clear opportunities for medium enterprises, the transition from scattered pilots to strategic, risk-managed deployment remains an open challenge in the 2023–2026 period.

## **THEORETICAL FRAMEWORKS (BRIEF OVERVIEW)**

### **Technology Acceptance Model (TAM) for AI**

The Technology Acceptance Model (TAM) helps us understand how people and organizations adopt new technologies, like AI. According to TAM a person's decision to use a technology depends on two things:

Perceived Usefulness (PU): “How much will this AI help me do my work better/ faster?”

Perceived Ease of Use (PEOU): “How easy is this AI to learn and use?”

When it comes to AI research shows that if sized businesses think AI tools, such as chatbots or design assistants are useful and easy to use they are more likely to start using them. Some researchers have added factors to TAM like trust and support from top management to help explain how companies adopt AI.

### **Risk-Threat Analysis Frameworks**

These frameworks help companies identify and manage risks associated with AI. A good example is the NIST AI Risk Management Framework (AI RMF). It provides a way to identify AI-related risks, like bias or security issues and design controls to manage them. For sized businesses frameworks like NIST AI RMF, ISO/IEC AI-risk standards and industry-specific models help turn broad AI risks into concrete actions. These actions might include audit checks, data protection policies and procedures to monitor AI models. These frameworks also help companies distinguish between risks and threats making it easier to defend against challenges, in the AI era.

Medium enterprises use these frameworks to manage AI risks. They assess negative impacts and external threats. Then they create strategies to address them. This helps ensure effective AI adoption.

## **METHODOLOGY: RESEARCH DESIGN, SAMPLE AND DATA TOOLS**

This study is looking at how generative AI affects enterprises in 2026. We are using a mix of surveys and case studies to get an understanding of the situation. The surveys will give us numbers and patterns while the case studies will provide detailed information about what is really happening.

Mixed-Methods Approach (Surveys + Case Studies)

We are following a step-by-step approach:

**Phase 1.** We are sending out surveys to enterprises to see how they are using generative AI, what they think about it and what problems they are facing.

**Phase 2.** We are doing in-depth studies of 8-12 enterprises to see how they are actually using generative AI, what strategies they are using and how it is affecting their businesses.

This approach gives us the best of both worlds: the surveys give us a picture while the case studies give us more detailed information about what is really going on.

Sample: 100 Medium Enterprises (India/Global)

We are looking at enterprises with 51-250 employees and a certain level of revenue. We want to study 100 of these enterprises from parts of the world including India, Asia, Europe and North America. We are choosing enterprises from sectors, such as services, manufacturing and digital platforms. We are selecting the enterprises in a way that ensures we have a mix of different conditions, such as regulatory environments, digital maturity and attitudes towards generative AI.

The people filling out the surveys are mostly managers or people who make decisions about generative AI. For the case studies we are also talking to people who are actually using AI, such as marketers, customer service staff and developers.

### **Data Collection & Analysis Tools**

To collect data we are using surveys with multiple-choice questions and some open-ended questions. For the case studies we are doing interviews collecting company documents and looking at available data on generative AI adoption. To analyze the data we are using tools to look at the numbers and find patterns. For the data we are using software to identify themes and patterns. We are also using AI tools to help us summarize the data and identify patterns but human researchers are making the final decisions to ensure that the results are accurate.

This approach will give us an evidence-based understanding of how generative AI is affecting medium enterprises in 2026. We are studying AI and its impact, on medium enterprises to get a better understanding of the situation. Generative AI is a part of this study and we are looking at how it is being used by medium enterprises.

### **CORE ANALYSIS SECTIONS: OPPORTUNITIES FOR MEDIUM ENTERPRISES**

This study shows that generative AI creates opportunities for medium enterprises in 2026. These opportunities are especially good for making businesses run smoothly coming up with new ideas and controlling costs. Medium enterprises can use tools like AI assistants and design programs to work and be more flexible than big companies.

#### **Operational Efficiency Gains**

Generative AI is like a coworker that helps with tasks that take a lot of time and thought. This means that human staff can focus on important work. Medium enterprises can get benefits from this such as:

- **Faster content generation:** Medium enterprises can make marketing materials, emails and product descriptions much quicker. This means they can get their products to market faster.
- **Automated internal workflows:** powered chatbots and assistants can handle routine tasks like customer questions and IT support. This helps medium enterprises respond to customers faster and reduces overtime.
- **Document and report processing:** AI tools can summarize reports and extract important information. This saves a lot of time. Cuts down on manual work.

These benefits are especially good for enterprises that do not have a lot of staff. They can run their businesses in a way without sacrificing quality.

#### **Innovation & Product Development**

Generative AI also helps medium enterprises come up with ideas and develop new products. They can use AI to design, simulate and test products quickly and at a lower cost. Some key ways that medium enterprises can use AI for innovation include:

1. AI-assisted idea generation: Brainstorming tools can help teams come up with new product ideas quickly.
2. Rapid prototyping, with AI design: Non-designers can use AI tools to create prototypes of products and marketing materials.
3. Customer insight augmentation: AI can help medium enterprises understand what customers are saying about them on media and reviews. This helps them detect emerging trends and create products that meet customer needs.

This combination of speed and flexibility helps medium enterprises compete with companies and startups that are already using AI. Medium enterprises can use AI to come up with new ideas and develop new products quickly which helps them stay competitive.

### **Risks and Challenges**

Generative AI has a lot of things to offer but medium enterprises also have to deal with a lot of technical, operational and ethical problems when they use these technologies. There are three things that people are worried about: problems with data privacy and security problems with getting things started and problems with ethics and bias.

#### **Data Privacy & Security Vulnerabilities**

Generative AI systems need to use a lot of data and models from the internet which can cause problems with privacy and security for enterprises:

If data gets out or someone hacks into the system sensitive business information or customer data can be stored, logged or retrieved by people who should not have access to it. This can happen when medium enterprises use cloud AI platforms.

There are also problems with the models themselves. Someone can try to trick the system use it for the thing or get private information from the data, which can make the AI system not work right or be used for bad things.

Medium enterprises also have to follow rules like the GDPR and Indias DPDP, which say that organizations are responsible for the data they use even if someone else is hosting it. If they do not follow these rules they can get in trouble. Hurt their reputation.

A lot of medium enterprises do not have a team that just deals with AI security so they do not find out about these problems until something bad happens, like a data leak. This shows that they need to have rules and controls in place for their AI data.

#### **Implementation Barriers**

It is not easy for medium enterprises to use AI in the real world. There are a lot of things that get in the way:

A lot of organizations do not have people who know about AI, which makes it hard for them to use it. They need people who know about data science, how to use AI systems and how to keep them running. But medium enterprises often have a hard time finding and keeping these people so they have to use consultants or people who do not know much about AI.

It also costs a lot of money to set up and use AI. Medium enterprises need to have computers, internet connections and systems that can work with the AI, which can be expensive. They also have to change the way they do things, which can be hard for employees and managers.

Some employees and managers might be afraid that AI will take their jobs or they might not trust the AI system, which can slow down the process of getting started with AI.

All these things make it hard for medium enterprises to use AI in a way that really works for them which means they might waste their money and miss out on opportunities.

### **Ethical & Bias Issues**

Generative AI also raises some ethical concerns, especially when it is used to make decisions that affect people:

The AI system can be biased, which means it can make unfair decisions. For example it might not be fair to some people when it comes to hiring or giving loans. This can hurt the reputation of the company. Be bad for the people who are treated unfairly.

It is also hard to know how the AI system is making its decisions, which can make it hard to trust it. If something goes wrong it can be hard to figure out what happened and who is responsible.

Generative AI can also create content that's not true or that infringes on copyrights, which can cause problems for medium enterprises. They need to have rules and processes in place to make sure the AI system is used in a way that is fair and safe.

For enterprises these ethical concerns mean they need to have clear rules for using AI monitor the AI system for bias and have people check the decisions it makes especially when it comes to customers and employees.

Generative AI is not a technical thing, for medium enterprises it is a big change that involves keeping data safe building capabilities and being ethical.

### **THREATS IN THE GENERATIVE AI LANDSCAPE**

In 2026, medium enterprises face both operational risks from using generative AI and external threats to their competitiveness, legal standing, and brand image. These threats arise from AI-native competitors, stricter global regulations, and new forms of AI-enabled abuse such as deepfakes and intellectual-property theft.

#### **Competitive Disruption from AI-Native Firms**

Generative AI has made it easier and cheaper to build highly automated, data-driven businesses. AI-native firms, designed around AI from the start, use large models, automated workflows, and small teams to deliver faster, cheaper, and more personalized services. Medium enterprises relying on legacy processes may lose customers to these competitors, who can generate content, manage customer service, and optimize pricing in real time. Since AI-native firms scale quickly with little added cost, delayed or weak AI adoption can push medium enterprises into low-value roles or cause them to lose entire customer segments.

#### **Regulatory Compliance (EU AI Act, India DPDP)**

The regulatory environment is becoming more complex and stringent. The EU AI Act applies a risk-based framework to AI systems, imposing heavy compliance duties—especially on high-risk applications—which can overwhelm medium enterprises with limited governance capacity. In India, the Digital Personal Data Protection (DPDP) Act and emerging AI-governance guidelines closely monitor how personal data is used in AI models. Non-compliance or careless AI use can trigger audits, fines, and reputational damage, making AI governance and audit readiness a strategic priority, not just a technical issue.

#### **IP Theft & Deepfake Risks**

Generative AI also heightens intellectual-property and authenticity risks. Sharing designs, code, or proprietary content with third-party AI models can lead to unintended copying or reuse of IP. At the same time, deepfakes and synthetic media pose serious enterprise-grade threats, enabling executive impersonation for fraud or AI-generated fake reviews that damage brand trust. Many medium enterprises lack the security tools to detect such attacks early, so they must

invest in media-authentication systems, brand-protection tools, and employee-awareness programs to counter AI-enabled disinformation and identity theft.

Overall, these threats show that, for medium enterprises, AI is not only a productivity tool but also a source of strategic, legal, and reputational vulnerability that requires proactive defense and structured governance.

### **STRATEGIC FRAMEWORK FOR AI ADOPTION IN MEDIUM ENTERPRISES (2026)**

To help medium enterprises make the most of Artificial Intelligence we need to think about the risks and the opportunities that come with it. This section is about creating a plan that medium enterprises can use to adopt Artificial Intelligence in a way. The plan is based on two ideas:

1. We need to protect our data, operations and reputation from risks.
2. We need to find ways to use Artificial Intelligence to make our businesses more efficient, innovative and competitive.

Medium enterprises need to think of Artificial Intelligence as a system that needs to be managed and controlled not as a tool. To do this we need to have some strategies in place.

#### **Data protection is very important.**

We should not upload customer or internal data into public or untrusted Artificial Intelligence platforms.

We should use Artificial Intelligence tools that're safe and follow the rules.

We should have policies about what data can be shared with external models and who is allowed to use Artificial Intelligence tools.

We also need to have processes in place to manage the risks that come with Artificial Intelligence.

We should have a framework to identify and manage risks such as data leakage, model bias and deepfakes.

We should have a system to monitor and audit Artificial Intelligence tools, including checking for anomalies and doing security reviews.

Security and governance controls are also crucial.

We should have controls in place to make sure authorized staff can use Artificial Intelligence tools.

We should have a system to review Artificial Intelligence-generated content, contracts or decisions in important areas like human resources, finance and law.

We need to make sure our employees understand how to use Artificial Intelligence in a way.

We should provide training on Artificial Intelligence ethics and privacy so employees know what is acceptable and what is not.

We should also make sure we follow international standards, such as the General Data Protection Regulation and the Digital Personal Data Protection Act to reduce the risk of legal and reputational problems.

By following these strategies medium enterprises can turn Artificial Intelligence risk management into an embedded capability, which enables secure experimentation and reduces the need for avoidance.

## Opportunity Maximization Roadmap

Medium enterprises need a step-by-step plan to unlock Artificial Intelligence-driven opportunities without using up many resources. Based on what we know about Artificial Intelligence adoption we recommend a four-phase approach:

### Phase 1: Awareness and Readiness Assessment

We should start with leadership workshops and internal diagnostics to assess our maturity, Artificial Intelligence readiness and key pain points such as slow content creation or manual reporting.

We can try out cost general-purpose Artificial Intelligence tools, such as office-suite copilots or chatbots in non-critical departments to build familiarity and confidence.

### Phase 2: Targeted Task-Specific Pilots

We can deploy Artificial Intelligence in return low-risk areas, such as marketing copy generation or basic IT support and focus on measurable key performance indicators, such as time saved or cost per ticket.

We should involve -functional teams, such as sales, human resources, finance and marketing in small-scale experiments and encourage a culture of Artificial Intelligence augmentation rather than fear-driven automation.

### Phase 3: Scaling and Integration

Once we see the value of Artificial Intelligence we can integrate it into our core workflows, such as customer relationship management enhancements or automated reporting via application programming interfaces or code/no-code platforms.

We should invest in Artificial Intelligence capability building: hire or train Artificial Intelligence- staff define internal Artificial Intelligence champions and establish a cross-departmental Artificial Intelligence working group.

### Phase 4: Strategic Artificial Intelligence Competence Development

We can gradually explore more customized Artificial Intelligence solutions, such as fine-tuned models for domain-specific tasks or internal Artificial Intelligence-enabled tools underpinned by strong data governance and risk controls.

We should continuously measure, refine and report on Artificial Intelligence impact via dashboards tracking productivity cost savings, innovation speed and risk-incident metrics.

For enterprises, in 2026 this roadmap balances speed and caution: it lets firms benefit from Artificial Intelligences efficiency and innovation gains while building the governance, skills and risk discipline needed to survive and thrive in an Artificial Intelligence-driven competitive landscape.

## CONCLUSION & RECOMMENDATIONS

This study on "AI Risks, Opportunities and Threats to Medium Enterprises in the Generative AI Era (2026)" shows that generative AI is very important for enterprises. It helps them in ways like making things more efficient innovating, automating tasks and reducing costs in areas like marketing, customer service and operations.. Medium enterprises also face some problems like keeping data safe high costs, ethical issues following rules like the EU AI Act and India's DPDP and dealing with things like deepfakes and AI-enabled fraud.

To use AI in a good way and stay safe medium enterprises should do a few things.

- They should make a plan for using AI with good data protection, risk management and audit checks.
- They should teach their workers about AI and how to use it in a way including how to make good prompts and use AI ethically.

- They should start using AI with small projects that are not too risky and then move to bigger projects while still having humans in charge.
- They should make their cybersecurity and brand protection stronger using tools that stop deepfakes and good ways to handle data.

If medium enterprises use AI in a way and think about the risks they can get many benefits like being more productive and innovative while also protecting their business, money and reputation.

### **Future Research Directions**

In the future researchers may want to look at some things.

1. How using AI for a time affects the productivity, profitability and employment of small and medium enterprises.
2. How small and medium enterprises can use AI to protect themselves from cyber attacks like phishing, ransomware and deepfakes.
3. How different industries like healthcare, finance and e-commerce can use AI. Follow the rules.
4. How humans and AI can work together. How AI is changing the skills people need and the way people work.
5. Some ethical issues, like finding bias being fair and explaining how AI works in medium enterprises.
6. How governments can help small and medium enterprises get better at using AI with policies, funding and support systems.

### **REFERENCE:-**

1. National Institute of Standards and Technology (2023). AI Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST. NIST AI RMF
2. Abdel Magid H. S., Desjardins M. R., Hu Y. (2024). Opportunities and shortcomings of AI for spatial epidemiology and health disparities research on aging and the life course. *Health Place* 89:103323. doi: 10.1016/j.healthplace.2024.103323
3. European Union (2024). EU Artificial Intelligence Act (EU AI Act). Brussels: European Commission. EU AI Act Official Portal
4. Jobin, A., et al. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389-399. Meta-review of 84 ethics frameworks, highlighting persistent gaps in bias and transparency relevant to 2026 deployments.
5. Brynjolfsson, E., et al. (2023). Generative AI at Work. NBER Working Paper No. 31161. Quantifies productivity paradox in AI adoption, with implications for 2026 economic impacts.
6. EU AI Act (2025). Regulation (EU) 2024/1689. Official Journal of the European Union. Details Phase Two mandates for high-risk AI transparency by August 2026.
7. OWASP Foundation (2025). OWASP Top 10 for Large Language Model Applications. Identifies prompt injection, data poisoning, and supply chain vulnerabilities as top security risks.
8. McKinsey & Company (2026). The state of AI in 2026. Annual report on agentic systems, multimodal AI, and industrial robotics opportunities.

9. Nexford University (2026). How will Artificial Intelligence Affect Jobs 2026-2030. Projects 92 million global jobs displaced, emphasizing reskilling needs.
10. Kiteworks (2026). AI Regulation in 2026: The Complete Survival Guide for Businesses. Covers U.S. patchwork rules and EU compliance strategies.
11. Moody's (2026). Outlooks 2026: Artificial Intelligence. Discusses investment bubbles, integration hurdles, and regulatory fragmentation.
12. Stanford HAI (2025). Stanford AI Experts Predict What Will Happen in 2026. Forecasts shift from hype to utility in AI applications.
13. IndiaAI Mission (2026). India AI Impact Summit Research Symposium. Highlights inclusive innovation and applied AI opportunities.
14. Google (2026). Student Researcher Program: AI and ML Opportunities. Details internships advancing multimodal and agentic research.
15. Organisation for Economic Co-operation and Development (2023). OECD AI Principles and SME Digital Transformation.
16. RahimiA. R.Sevilla-PavónA. (2024). The role of ChatGPT readiness in shaping language teachers' language teaching innovation and meeting accountability: a bisymmetric approach. *Comput. Educ. Artif. Intell.*7:100258. doi: 10.1016/j.caeai.2024.100258
17. NaharS. (2024). Modeling the effects of artificial intelligence (AI)-based innovation on sustainable development goals (SDGs): applying a system dynamics perspective in a cross-country setting. *Technol. Forecast. Soc. Chang.*201:123203. doi: 10.1016/j.techfore.2023.123203
18. Davenport, T. H., & Bean, R. (2026). Five Trends in AI and Data Science for 2026. MIT Sloan Management Review. Analyzes deflation of AI bubble, agentic AI progression, and organizational AI resources as key 2026 shifts.